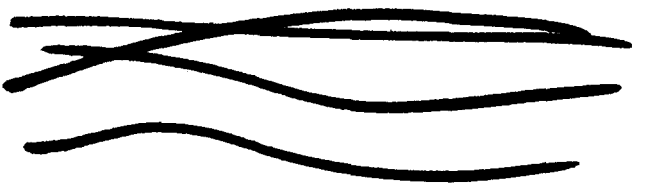
Simon Plouffe
le 5 mars 79

Théorie des nombres



A. 1. MARKOUCHEVITCH. — ***Fonctions d'une variable complexe. Problèmes contemporains*** (272 p.). Traduit par L. NICOLAS, 1962.

N. N. BOGOLIOUBOV et Y. A. MITROPOLSKI. — ***Les méthodes asymptotiques en théorie des oscillations non linéaires (520 p.).*** Traduit par G. JACOBI, 1962.

Y. V. LINNIK. — ***Décompositions des lois de probabilités*** (294 p.). Traduit par M. L. GRUEL, 1962.

J. MIKUSINSKI et R. SIKORSKI. — ***Théorie élémentaire des distributions*** (108 p.). Traduit par S. KLARSFELD, 1964.

1. M. GELFAND, D. A. RAIKOV et ***G. E.*** CHILOV. — ***Les anneaux normés commutatifs*** (259 p.). Traduit par M. et J.-L. VERLEY, 1964.

A. GELFOND et Y. LINNIK. — ***Méthodes élémentaires dans la théorie*** [illegible] Traduit par M. et J.-L. VERLEY, 1965.

Y. A. I. MITROPOLSKI. — ***Problèmes de la théorie asymptotique des oscillations non stationnaires*** (547 p.). Traduit par G. CARVALLO, 1966.

V. 1. ARNOLD et A. AVEZ. — ***Problèmes ergodiques de la mécanique classique (288*** p.), 1967.

MONOGRAPHIES INTERNATIONALES DE MATHÉMATIQUES MODERNES

Sous la direction de S. MANDELBROJT

Professeur au Collège de France

Théorie des nombres

par **Z. 1. BOREVITCH**

et **1. R. CHAFAREVITCH**

Traduit par

Myriam et **Jean-Luc VERLEY**

1967

GAUTHIER-VILLARS

PARIS

Traduction faite d'après
l'édition originale russe

ТЕОРИЯ ЧИСЕЛ

PRÉFACE

Ce livre s'adresse aux mathématiciens débutants; il constitue une introduction à la théorie des nombres, aux problèmes soulevés par cette théorie et aux méthodes utilisées.

Nous avons choisi une méthode d'exposition dans laquelle les problèmes et les techniques d'étude sont étroitement liés. En principe, nous partons de problèmes concrets relatif aux nombres entiers; les théories générales interviennent alors pour résoudre ces problèmes. En général, ces théories seront suffisamment développées pour en faire saisir la richesse et apprendre à les appliquer.

Les questions étudiées dans ce livre se rattachent principalement à la théorie des équations diophantiennes, i. e. à la théorie de la résolution en nombres entiers des équations à plusieurs inconnues. On considérera également des questions d'autre nature : par exemple, le théorème de Dirichlet sur les nombres premiers dans une progression arithmétique ou les théorèmes sur la variation du nombre de solutions d'une congruence.

Les méthodes qui interviennent ici sont surtout algébriques, principalement la théorie des extensions finies des corps et de leurs métriques. Cependant, on a accordé une place importante aux méthodes analytiques : le chapitre V leur est consacré et la méthode des fonctions analytiques p-adiques est exposée dans le chapitre IV. A plusieurs reprises interviennent également des considérations géométriques.

Ce livre n'exige pas de grandes connaissances de la part du lecteur. Deux années d'Université suffisent pour comprendre la presque totalité de l'ouvrage; c'est seulement dans le dernier chapitre qu'interviennent quelques résultats relatifs aux fonctions analytiques.

A la fin du livre, dans un « appendice algébrique » nous avons rappelé des définitions précises, des énoncés et parfois des démonstrations des résultats qui interviennent au cours de l'ouvrage et peuvent ne pas figurer dans certains cours d'algèbre.

Ce livre est tiré d'un cours fait par un des auteurs à l'Université de Moscou.

Nous remercions vivement A. G. Postnikov qui nous a communiqué les notes prises à ce cours.

Dimitri Konstantinovitch Faddeev a largement participé à cet ouvrage. Nous le remercions profondément pour les nombreuses et instructives conversations que nous avons eues avec lui et pour les précieuses remarques qu'il a bien voulu nous faire. Plusieurs démonstrations de ce livre lui sont dues, en particulier la nouvelle démonstration p-adique du théorème de Kummer sur le deuxième facteur du nombre de classes des corps cyclotomiques.

LES AUTEURS.

PRÉFACE
DE LA TRADUCTION FRANÇAISE

Une des particularités les plus frappantes de la théorie des nombres est la simplicité de formulation de ses problèmes ; beaucoup d'entre eux peuvent être compris par un étudiant. Mais, par ailleurs, la solution de ces problèmes fait intervenir d'autres notions que celles qui figurent dans leur énoncé ; cela exige l'élaboration de nouvelles méthodes, souvent très abstraites.

Cette manière de procéder conduit à des théories importantes, en partant de problèmes simples et élémentaires ; tel est l'objet de notre livre. Ce livre s'adresse à des mathématiciens débutants ; aussi ne demande-t-il que peu de connaissances préliminaires. Nous nous sommes limités à quelques questions qui sont étudiées à fond.

Dans la traduction française, on a effectué, avec l'accord des auteurs, quelques changements de notations ; ces modifications étaient nécessaires pour que l'ouvrage soit compréhensible par un lecteur français : par exemple, dans l'original russe, le corps des nombres rationnels est désigné par R et non par **Q** *!*

LES AUTEURS,
mai 1966.

CHAPITRE PREMIER

CONGRUENCES

Ce chapitre est consacré à la théorie des congruences et à ses applications aux équations. Remarquons que si l'équation

$$F(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

où F est un polynôme à coefficients entiers, a une solution en nombres entiers, alors la congruence

$$F(x_1, \ldots. x_n) \equiv 0 \pmod{m} \tag{2}$$

a une solution pour tout entier m. Pour chaque m, l'ensemble des classes résiduelles modulo m est fini et par suite la congruence (2) s'étudie directement. On obtient ainsi des conditions nécessaires pour que l'équation (1) soit résoluble en nombres entiers.

L'étude de la suffisance éventuelle de ces conditions est très difficile. L'affirmation : « une équation est résoluble si et seulement si pour chaque entier la congruence correspondante est résoluble » n'est pas vraie dans le cas général (cf. par exemple, exercice 4), mais est vraie pour plusieurs classes particulières d'équations. Dans ce chapitre, nous démontrerons ce résultat dans le cas où F est une forme quadratique, après avoir ajouté l'hypothèse supplémentaire (manifestement nécessaire) que l'équation (1) a une solution en nombres réels (si F est une forme, alors, par solution de F = 0, on entend solution non nulle).

La notion essentielle que nous étudierons tout d'abord dans ce chapitre est celle de nombre p-adique; nous appliquerons ensuite cette notion à la théorie des congruences. On sait, d'après la théorie éltmentaire des nombres, que, si $m = p_1^{k_1} \ldots p_r^{k_r}$ ($p_1, \ldots, p_r$ étant des facteurs premiers distincts), la résolution de la congruence (2) est équivalente à la résolution des congruences

$$F(x_1, \ldots, x_n) \equiv 0 \left(\mathrm{mod}\ p_i^{k_i}\right)$$

pour tout $i = 1, 2, \ldots, r$. Ainsi, la résolubilité de la congruence (2) pour tout entier m est équivalente à la résolubilité de ces congruences modulo toutes les puissances des nombres premiers. Dans la suite, nous fixerons le nombre premier p et nous étudierons les congruences

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{3}$$

pour toutes les valeurs entières de k. En liaison avec ce problème, Hensel a introduit, pour chaque nombre premier p, un nouveau type de nombres appelés par lui nombres p-adiques et a démontré que la résolubilité des congruences (3) pour tout entier k est équivalente à la résolubilité de l'équation (1) dans l'ensemble des nombres p-adiques. Par suite, la résolubilité des congruences (2) pour tout entier m est équivalente à la résolubilité de l'équation (1) dans les ensembles de nombres p-adiques pour les nombres p premiers.

En utilisant la notion de nombre p-adique, on peut donc donner la forme suivante au théorème mentionné ci-dessus (ce chapitre est consacré à la démonstration de ce résultat) : si $F(x_1, \ldots, x,)$ est une forme quadratique à coefficients entiers, l'équation (1) est résoluble en nombres entiers si et seulement si elle est résoluble en nombres réels et en nombres p-adiques, pour tout p.

Dans la formulation de ce théorème, appelé le théorème de Minkowski-Hasse, et dans beaucoup d'autres questions, les nombres p-adiques figurent sur le même plan que les nombres réels. De même que les nombres réels interviennent de manière naturelle dans l'étude des limites de nombres rationnels, les nombres p-adiques jouent un rôle analogue dans les questions liées à la division suivant les puissances successives du nombre premier p. Cette analogie entre les nombres p-adiques et les nombres réels sera précisée en montrant que les nombres p-adiques, tout comme les nombres réels, peuvent être obtenus par complétion à partir des nombres rationnels (pour d'autres métriques que la valeur absolue usuelle).

Faisons une dernière remarque : si F est une forme, la résolubilité en nombres entiers de l'équation (1) est bien entendu équivalente à l'existence d'une solution formée de nombres rationnels; ainsi, dans le théorème de Minkowski-Hasse, on peut parler de la résolubilité en nombres rationnels au lieu de la résolubilité en nombres entiers. Cette remarque évidente prend toute sa signification dans le résultat suivant : si F est un polynôme quelconque de degré 2, le théorème correspondant donne des conditions de résolubilité de l'équation (1) en nombres rationnels et non pas en nombres entiers. Par suite, dans l'étude des équations du deuxième degré nous ne nous limiterons pas à l'étude des solutions en nombres entiers mais examinerons également les solutions en nombres rationnels.

EXERCICES

1. Montrer que l'équation $15x^2 - 7y^2 = 9$ n'a pas de solutions en nombres entiers.

2. Montrer que l'équation $5x^3 + 11y^3 + 13z^3 = 0$ n'a pas d'autre solution en nombres entiers que la solution triviale x = 0, y = 0, $z = 0$.

3. Démontrer que les nombres entiers de la forme $8n + 7$ ne peuvent pas s'écrire comme somme de trois carrés de nombres entiers.

4. Utilisant les propriétés du symbole de Legendre, démontrer que la congruence

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \pmod{m}$$

est résoluble pour tout entier m. Remarquer cependant qu'il est évident que l'équation $(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0$ n'a pas de solution en nombres entiers.

5. Démontrer que l'équation linéaire $a_1x_1 + \ldots + a_nx_n = b$, où $a_1, \ldots, a_n, b$ sont des entiers, est résoluble en nombres entiers si et seulement si la congruence correspondante modulo m est résoluble pour tout entier m.

6. Démontrer le même résultat pour un système d'équations linéaires à coefficients entiers.

§ 1. — CONGRUENCES MODULO UN NOMBRE PREMIER

1) Équivalence des polynômes

Rappelons tout d'abord quelques propriétés des congruences modulo un nombre premier. Comme on le sait, les classes résiduelles modulo p forment un corps fini à p éléments qui sera constamment désigné dans la suite par $\mathbf{F}_p$; chaque congruence modulo p s'interprète comme une égalité dans ce corps. Tous les résultats de ce paragraphe et du suivant sont valables non seulement pour le corps $\mathbf{F}_p$, mais plus généralement pour tout corps fini; il suffit de remplacer à chaque fois le nombre p par le nombre $q = p^m$ d'éléments de ce corps. Nous nous limiterons cependant à l'étude des corps $\mathbf{F}_p$ et c'est seulement pour donner un contre-exemple après le théorème 3 que nous devrons faire appel à un corps fini qui ne soit pas de ce type.

Les corps résiduels modulo un nombre premier (et plus généralement tout corps fini) possèdent une série de propriétés qui les distinguent des corps usuels de l'algèbre élémentaire. Voici la plus importante d'entre elles, dont nous aurons souvent besoin : deux polynômes qui prennent des valeurs égales pour toutes les valeurs des variables n'ont pas nécessairement des coefficients égaux. Ainsi, d'après le petit théorème de Fermat, les polynômes x^p et x prennent des valeurs égales quand x parcourt tout le corps $\mathbf{F}_p$

mais leurs coefficients ne sont pas égaux (ce phénomène se produit dans tout corps fini : si $\alpha_1, \ldots, \alpha_q$ sont tous les éléments de ce corps, le polynôme $(x - \alpha_1) \ldots (x - \alpha_q)$ à coefficients non nuls prend seulement la valeur 0 quand x parcourt tout le corps fini considéré).

Nous écrirons

$$F(x_1, \ldots . x_n) \equiv G(x_1, \ldots, x_n) \pmod{p}$$

et nous dirons que les polynômes F et G sont congrus si leurs coefficients correspondants sont congrus modulo p. Si maintenant nous avons

$$F(c_1, \ldots, c_n) \equiv G(c_1, \ldots, c_n) \pmod{p}$$

pour tous les systèmes de valeurs $c_1, \ldots, c_n$, nous écrirons $F \sim G$ et nous dirons que les polynômes F et G sont ***équivalents.*** Il est clair que si $F \equiv G$, alors $F \sim G$, mais l'exemple des polynômes x et x^p montre que la réciproque n'est pas vraie en général.

Puisque les deux congruences $F \equiv 0 \pmod{p}$ et $G \equiv 0 \pmod{p}$ ont les mêmes solutions si $F \sim G$, il est naturel pour étudier une congruence de remplacer le polynôme considéré par un polynôme équivalent plus simple. Précisons cette question.

Si une inconnue x_i figure dans le polynôme F avec un exposant supérieur à p, alors, utilisant l'équivalence $x_i^p = x_i$ qui résulte du théorème de Fermat, nous pouvons remplacer x_i^p par x_i dans F. Puisque les équivalences s'additionnent et se multiplient terme à terme, on obtient facilement ainsi un polynôme équivalent à F et de degré en x_i strictement plus petit. On peut alors répéter ce processus jusqu'à obtention d'un polynôme équivalent à F dont le degré par rapport à chaque variable est strictement inférieur à p. Un tel polynôme sera dit ***réduit.*** Il est clair que par le remplacement de x_i^p par x_i le degré total de F (par rapport à l'ensemble des variables) diminue; nous obtenons ainsi le résultat suivant.

THÉORÈME 1. — ***Tout polynôme*** F ***est équivalent à un polynôme réduit*** F* ***dont le degré total est inférieur ou égal au degré total de*** F.

Montrons maintenant que le polynôme réduit équivalent à un polynôme donné est unique.

THÉORÈME *2.* — ***Deux polynômes réduits qui sont équivalents sont congrus.***

Ce théorème se démontre par récurrence sur le nombre de variables, exactement comme le théorème rappelé ci-dessus sur l'identité des polynômes. Bien entendu, il suffit de montrer que si F est un polynôme réduit équivalent à 0, alors $F \equiv 0 \pmod{p}$.

Considérons tout d'abord le cas $n = 1$. Si le degré de x est inférieur à p

et F(c) ≡ 0 (mod *p*) pour tout c, alors F a un nombre de racines supérieur à son degré et cela n'est possible que si tous les coefficients de F sont divisibles par *p*, i. e. F ≡ 0 (mod *p*). Soit maintenant $n \geqslant 2$; nous écrirons F sous la forme

$$F(x_1, \ldots > x_n) = A_0(x_1, \ldots, x_{n-1}) + A_1(x_1, \ldots, x_{n-1})x_n + \ldots + A_{p-1}(x_1, \ldots, x_{n-1})x_n^{p-1}.$$

Considérons un système arbitraire de valeurs $x_1 = c_1, \ldots, x_{n-1} = c_{n-1}$ et posons

$$A_0(c_1, \ldots, c_{n-1}) = a_{,,} \ldots, A_{p-1}(c_1, \ldots, c_{n-1}) = a_{p-1}.$$

Ainsi

$$F(c_1, \ldots, c_{n-1}, x) = a_0 + a_1x_n + \ldots + a_{p-1}x_n^{p-1},$$

et nous avons obtenu un polynôme d'une seule variable x_n qui est équivalent à 0 puisque F ∼ 0. Mais le théorème est démontré pour les polynômes d'une variable et par suite ce polynôme est congru à 0. Ainsi

$$A_0(c_1, \ldots, c_{n-1}) \equiv 0 \pmod{p}$$
$$\vdots$$
$$A_{p_1}(c_1, \ldots, c_{n-1}) \equiv 0 \pmod{p},$$

i. e. $A_{,,} \sim 0, \ldots, A_{p-1} \sim 0$ (puisque $c_1, \ldots, c_{n-1}$ sont arbitraires). Puisque les polynômes $A_{,,}, \ldots, A_{p-1}$ de $(n - 1)$ variables sont réduits, alors, par hypothèse de récurrence, on a

$$A, \equiv 0 \pmod{p}, \ldots, A_{p-1} \equiv 0 \pmod{p},$$

d'où F ≡ 0 (mod *p*).

2) Théorèmes sur le nombre de solutions des congruences

Donnons déjà quelques conséquences des théorèmes 1 et 2.

THÉORÈME 3. — *Si la congruence* $F(x_1, \ldots, x_{,,}) \equiv 0 \pmod{p}$ *a une solution et si le degré total du polynôme* F *est strictement inférieur au nombre n des variables, alors cette congruence a au moins deux solutions.*

DÉMONSTRATION. — Supposons que le polynôme $F(x_1, \ldots, x_n)$ de degré *r* ait une solution unique

$$x_1 \equiv a, \pmod{p}, \ldots, x_n \equiv a_n \pmod{p}.$$

Posant $H(x_1, \ldots, x_n) = 1 - F(x_1, \ldots, x_n)^{p-1}$, nous avons, d'après les hypothèses faites sur F et le petit théorème de Fermat,

$$H(x_1, \ldots, x_n) \equiv \begin{cases} 1 \text{ si } x_1 \equiv a_1, \ldots, x_n \equiv a_n \pmod{p} \\ 0 \text{ sinon.} \end{cases}$$

Soit H* le polynôme réduit équivalent au polynôme H (cf. théorème 1); H* prend les mêmes valeurs que H. Mais il est facile, par ailleurs, de construire un polynôme réduit prenant les mêmes valeurs que H; c'est le polynôme

$$\prod_{i=1}^{n}\left(1 - (x_i - a_i)^{p-1}\right).$$

D'après le théorème 2, nous aurons donc

$$H^* \equiv \prod_{i=1}^{n}\left(1 - (x_i - a_i)^{p-1}\right) \pmod{p} \qquad (1)$$

et, d'après le théorème 1, le degré de H* est inférieur au degré de H, i. e. inférieur à $r(p-1)$, alors que son degré, d'après (1), est égal à $n(p-1)$. Il en résulte $n(p-1) \leqslant r(p-1)$, ce qui contredit l'hypothèse $r < n$.

COROLLAIRE (théorème de Chevalley). — *Si $F(x_1, \ldots, x_n)$ est une forme de degré strictement inférieur à n, la congruence*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

a une solution non nulle.

L'existence de cette solution résulte du théorème 3 puisque cette congruence admet trivialement la solution nulle.

Montrons qu'il est impossible d'améliorer l'inégalité $r < n$ dans le théorème de Chevalley; nous construirons à cet effet pour tout entier n une forme $F(x_1, \ldots, x,)$ de degré n telle que la congruence

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p} \qquad (2)$$

n'ait que la solution nulle. Nous utiliserons le fait que, pour tout $n \geqslant 1$, il existe un corps fini Σ à p^n éléments contenant $\mathbf{F}_p$ comme sous-corps (voir appendice, § 3, théorème 2); soit $\omega_1, \ldots, \omega_n$ une base du corps Σ sur le corps $\mathbf{F}_p$. Considérons les combinaisons linéaires $x_1\omega_1 + \ldots + x_n\omega_n$ où, $x_1, \ldots, x_n$ prennent des valeurs quelconques dans $\mathbf{F}_p$. La norme

$$N_{\Sigma/\mathbf{F}_p}(x_1\omega_1 + \ldots + x_n\omega_n) = \varphi(x_1, \ldots, x_n)$$

est une forme de degré n en $x_1, \ldots, x_n$, à coefficients dans $\mathbf{F}_p$. Par définition de la norme N(a) d'un élément $a = x_1\omega_1 + \ldots + x_n\omega_n$ ($x_i \in \mathbf{F}_p$) (cf. appen-

dice § 2, 2)), on a N(a) = 0 si et seulement si a = 0, i. e. $x_1 = \ldots = x_n = 0$. Ainsi, la forme φ est telle que l'équation $\varphi(x_1, \ldots, x_n) = 0$ admet seulement la solution nulle dans le corps $\mathbf{F}_p$. Remplaçons maintenant chaque coefficient de la forme φ, qui est une classe résiduelle **modulo** p, par un représentant de cette classe. Nous obtenons ainsi une forme $F(x_1, \ldots, x_n)$ à coefficients entiers, de degré n à n variables telle que la congruence (2) n'ait que la solution nulle.

Le théorème 3 est un cas particulier du résultat suivant.

THÉORÈME 4 (théorème de Warning). — ***Si le degré dupolynôme*** $F(x_1, \ldots . x,)$ ***est strictement inférieur à n, le nombre de solutions de la congruence***

$$F(x_1, \ldots, x,) \equiv 0 \pmod{p}$$

est divisible par p.

DÉMONSTRATION. — Supposons que la congruence considérée ait s solutions $A_i = (a_1^{(i)}, \ldots . a_n^{(i)})$, $i = 1, \ldots, s$. Posons, cette fois encore, $H = 1 - F^{p-1}$. Il est clair que

$$H(X) = \begin{cases} 1 \text{ si } X \equiv A_i \pmod{p} & i = 1, \ldots, s, \\ 0 \text{ dans les autres cas;} \end{cases}$$

ici, $X = (x_1, \ldots, x,)$ (les congruences entre vecteurs à coordonnées entières signifient que les composantes correspondantes de ces vecteurs vérifient la congruence). Pour $A = (a_1, \ldots, a_n)$, formons le polynôme

$$D_A(x_1, \ldots, x_n) = \prod_{j=1}^{n} (1 - (x_j - a_j)^{p-1}). \tag{3}$$

Il est clair que

$$D_A(X) = \begin{cases} 1 \text{ si } X \equiv A \pmod{p} \\ 0 \text{ sinon} \end{cases} \tag{4}$$

Posons

$$H^*(x_1, \ldots, x_n) = D_{A_1}(x_1, \ldots, x_n) + \ldots + D_{A_s}(x_1, \ldots, x_n). \tag{5}$$

La congruence (4) montre que H* prend les mêmes valeurs que H pour toutes les valeurs des variables $x_1, \ldots, x,,,$ i. e. $H \sim H^*$. Puisque chacun des polynômes D_{A_i} est réduit, H* est aussi réduit; il résulte alors des théorèmes 1 et 2 que le degré de H* est inférieur au degré de H, lui-même strictement inférieur à $n(p - 1)$. Mais dans chaque D_{A_i}, il y a un seul terme de degré $n(p-1)$, c'est le terme $(-1)^n (x_1 \ldots x_n)^{p-1}$. Puisque le degré de H* est strictement inférieur à $n(p-1)$, la somme de tous les termes de degré $p - 1$ est nulles

ce qui exige $s \equiv 0 \pmod{p}$. Ceci termine la démonstration du théorème 4.

Le théorème 3 résulte du théorème 4 : si $p \geqslant 2$, $s \neq 0$ et $s \equiv 0 \pmod{p}$ entraînent $s \geqslant 2$.

3) Les formes quadratiques modulo un nombre premier

Appliquons les résultats précédents aux formes quadratiques. Le théorème suivant est une conséquence immédiate du théorème de Chevalley.

THÉORÈME 5. — *Soit $f(x_1, \ldots, x_n)$ une forme quadratique à coefficients entiers. Si $n \geqslant 3$, la congruence*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

a une solution non nulle.

Le cas des formes quadratiques à une seule variable ne présente guère d'intérêt (si $a \not\equiv 0 \pmod{p}$, la congruence $ax^2 \equiv 0 \pmod{p}$ a seulement la solution nulle).

Considérons le cas des formes quadratiques à deux variables. Nous supposerons $p \neq 2$ (pour $n = 2$, $p = 2$, il est facile d'étudier directement toutes les formes quadratiques possibles). La forme peut alors s'écrire

$$f(x, y) = ax^2 + 2bxy + cy^2.$$

Nous designerons par d son déterminant $ac - b^2$.

THÉORÈME 6. — *La congruence*

$$f(x, y) \equiv 0 \pmod{p} \quad (p \neq 2) \tag{6}$$

a une solution non nulle si et seulement si — d est ou bien divisible par p ou bien est un résidu quadratique modulo p.

DÉMONSTRATION. — Il est clair que pour des formes f et f_1 équivalentes sur le corps $\mathbf{F}_p$ (voir appendice § 1, 1)), les congruences (6) ont simultanément une solution non nulle ou pas de solution non nulle. Puisque dans le passage d'une forme à une forme équivalente, son determinant est multiplié par le carre d'un élément non nul du corps $\mathbf{F}_p$, nous pouvons, dans la démonstration du théorème 6, remplacer la forme f par une autre qui lui soit équivalente. Chaque forme est Cquivalente à une forme diagonale (appendice § 1, théorème 3); par suite, nous pouvons supposer que

$$f = ax^2 + cy^2, \qquad d = ac.$$

Si a $\equiv$ 0 ou c $\equiv$ 0 (mod p), le théorème est évident. Si maintenant $ac \not\equiv 0 \pmod{p}$ et si la congruence (6) a une solution non nulle (x_0, y_0), alors, de la congruence

$$ax_0^2 + cy_0^2 \equiv 0 \pmod{p}$$

nous tirons

$$-ac \equiv \left(\frac{y_0}{x_0}\right)^2 \pmod{p}$$

(la fraction $w = \frac{u}{v}$ (modp) désigne le résultat de la division dans le corps $\mathbf{F}_p$, i. e. la solution de la congruence $vw \equiv u \pmod{p}$). Ainsi $\left(\frac{-d}{p}\right) = 1$. Réciproquement, si $\left(\frac{-d}{p}\right) = 1$ et $-ac \equiv u^2 \pmod{p}$, nous pouvons prendre

$$(x_0, y_0) = (u, a).$$

EXERCICES

1. Déterminer le polynôme réduit équivalent modulo p en monôme x^k.

2. Construire une forme cubique $F(x_1, x_2, x_3)$ telle que la congruence

$$F(x_1, x_2, x_3) \equiv 0 \pmod{2}$$

n'admette que la solution nulle.

3. Avec les notations de la démonstration du théorème de Warning, montrer que, pour $p \neq 2$, les composantes des solutions A_i (i = 1, . . . , s) vérifient les congruences

$$\sum_{i=1}^{s} a_1^{(i)} \equiv \ldots \equiv \sum_{i=1}^{s} a_n^{(i)} \equiv 0 \pmod{p}.$$

4. Généralisant le théorème 4 et l'exercice 3, montrer, avec ces notations, que l'on a les congruences

$$\sum_{i=1}^{s} \left(a_1^{(i)}\right)^k \equiv \ldots \equiv \sum_{i=1}^{s} \left(a_n^{(i)}\right)^k \equiv 0 \pmod{p}$$

pour $k = 0, 1, \ldots, p-2$.

5. Démontrer que si $F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)$ sont des polynômes à coefficients entiers de degrés $r_1, \ldots, r_m$ tels que $r_1 + \ldots + r_m < n$ et si le système des congruences

$$\left.\begin{aligned} F_1(x_1, \ldots, x_n) &\equiv 0 \pmod{p} \\ &\cdots \\ F_m(x_1, \ldots, x_n) &\equiv 0 \pmod{p} \end{aligned}\right\} \qquad (7)$$

a au moins une solution, alors il en a au moins deux.

6. Avec les hypothèses de l'exercice 5, montrer que le nombre de solutions du système (7) est divisible par p.

7. Montrer que si f est une forme quadratique sur le corps $\mathbf{F}_p$ de rang $\geqslant 2$ et $a \not\equiv 0 \pmod{p}$, alors la congruence

$$f \equiv a \pmod{p}$$

est résoluble.

8. Utilisant les théorèmes 2 et 3 de l'appendice, montrer que deux formes quadratiques non singulières sur le corps $\mathbf{F}_p$ ($p \neq 2$) sont équivalentes si et seulement si le produit de leurs déterminants est un carré.

9. Définir le groupe des classes de Witt de formes quadratiques sur le corps $\mathbf{F}_p$ ($p \neq 2$) (cf. exercice 5 du § 1 de l'appendice).

10. Montrer que le nombre de solutions non nulles de la congruence $f(x, y) \equiv 0 \pmod{p}$, où f est une forme quadratique de déterminant $d \not\equiv 0 \pmod{p}$, est égal à

$$(p-1)\left(1+\left(\frac{-d}{p}\right)\right).$$

11. Utilisant le théorème 7 du § 1 de l'appendice, montrer que si $f(x_1, \ldots, x_n)$ est une forme quadratique de déterminant $d \not\equiv 0 \pmod{p}$, $p \neq 2$, alors le nombre de solutions non nulles de la congruence $f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ est égal à

$$p^{n-1} - 1 + (p-1)\left(\frac{(-1)^{\frac{n}{2}}d}{p}\right)p^{\frac{n}{2}-1} \qquad \text{pour } n \text{ pair}$$

$$p^{n-1} - 1 \qquad \text{pour } n \text{ impair}$$

12. Avec les hypothèses de l'exercice 11, trouver le nombre de solutions de la congruence

$$f(x_1, \ldots, x_n) \equiv a \pmod{p}.$$

§ 2. — SOMMES TRIGONOMETRIQUES

1) Congruences et sommes trigonométriques

Dans ce paragraphe, nous considérerons encore les congruences modulo un nombre premier, mais d'un point de vue différent. Les théorèmes du § 1 donnent des résultats sur le nombre de solutions d'une congruence en liaison avec le degré et le nombre de variables du polynôme. Ici, c'est la grandeur du nombre premier p qui joue un rôle essentiel.

Nous avons dit au début de ce chapitre que pour que l'équation

$$F(x_1, \ldots, x_n) = 0$$

soit résoluble en nombres entiers, il est nécessaire que les congruences $F \equiv 0 \pmod{m}$ soient résolubles pour tous les entiers m; en fait, on a vu qu'il suffisait de considérer les cas où m est une puissance de nombre premier.

Nous allons voir que pour une classe très importante de polynômes, les congruences $F \equiv 0 \pmod{p}$ sont automatiquement résolubles pour tout entier p assez grand.

DÉFINITION. — Un polynôme $F(x_1, \ldots, x_n)$ à coefficients rationnels est dit ***absolument irréductible*** s'il n'est décomposable en produit de polynômes non triviaux dans aucune extension du corps des nombres rationnels.

Le théorème fondamental est le suivant :

THÉORÈME A. — *Si* $F(x_1, \ldots, x_n)$ *est un polynôme absolument irréductible à coefficients entiers, alors la congurence*

$$F(x_1, \ldots, x,) \equiv 0 \pmod{p} \qquad (1)$$

est résoluble pour tout nombre premier p supérieur à un certain nombre (dépendant du polynôme F).

On a un résultat analogue pour les solutions non nulles d'un polynôme homogène F et pour les systèmes de congruences (pour des notions appropriées d'irréductibilité absolue).

Le théorème A est trivial pour $n = 1$ (tout polynôme à une variable de degré supérieur à 1 se décompose dans le corps des nombres complexes et le théorème est trivial pour les polynômes du premier degré). Pour $n = 2$ déjà, la dtmonstration utilise des méthodes plus profondes de géométrie algébrique. Dans le cas $n = 2$, le théorème A a été obtenu par A. Weil (A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, *Act. Sci. Ind.*, 1041, Paris, Hermann, 1948). Des variantes de cette démonstration figurent dans les travaux de S. Lang (S. Lang, Abelian varietics, Interscience Tracts, n° 7, New York, 1959) et A. Mattuck et J. Tate (On the inequality of Castelnuovo-Severi, ***Abh. Math. Sem. Univ. Hamb., 1958,*** B. **22,** H. 3-4, 295-299).

Le passage de $n = 2$ au cas général s'effectue beaucoup plus simplement. C'est fait dans les travaux de L. B. Nisnevitch (Sur le nombre de points des variétés algébriques dans les corps premiers finis, ***Dokl. A. N. URSS,*** 1954, 99, n° 1, 17-20) et de S. Lang et A. Weil (Number of points of variety in finite fields, *Am. J. Math.*, 1954, 76, n° 4, 819-827).

Les ouvrages ci-dessus démontrent en fait plus que le théorème A; ainsi, on montre que si on fixe le polynôme F, le nombre $N(p)$ de solutions de la congruence (1) tend vers l'infini quand le nombre premier p tend vers l'infini. Plus précisément encore, on a évalué la rapidité de croissance du nombre $N(p)$. La formulation exacte de ce résultat est la suivante :

THÉORÈME B. -*Le nombre* N(F, *p) de solutions de la congruence* (1) *satisfait à l'inégalité*

$$| N(F, p) - p^{n-1} | < C(F) p^{n-1-\frac{1}{2}},$$

la constante C(F) *dépendant seulement du polynôme* F *et non de p.*

L'unique procédé de démonstration actuellement connu du théorème A est de le déduire du théorème B. Nous ne pourrons pas donner ici de démonstration des théorèmes A et B car il faut des outils algébriques beaucoup plus élabores que ceux dont nous disposons dans ce livre. Cependant, nous exposerons une méthode qui permet de démontrer ces théorèmes dans des cas particuliers; nous choisirons ici un de ces cas particuliers.

Tout repose sur le fait qu'on peut représenter le nombre de solutions de l'équation (1) comme somme de certaines racines $p^{\text{ièmes}}$ de l'unité. Les sommes de ce type sont dites **trigonométriques.**

Posons quelques notations. Si f(x) ou $f(x_1, \ldots, x_n)$ est une fonction à valeurs complexes dont les valeurs dépendent seulement des classes résiduelles des nombres $x_1, \ldots, x_n$ modulo p, nous désignerons par

$$\sum_x f(x) \qquad \text{ou} \qquad \sum_{x_1, \ldots, x_n} f(x_1, \ldots, x_n)$$

les sommes étendues à toutes les valeurs x ou $x_1, \ldots, x_n$ d'un système complet de résidus **modulo** p et par

$$\sum_x{}' f(x)$$

la somme étendue à toutes les valeurs x d'un système réduit de résidus.

Soit ζ une racine primitive $p^{\text{ième}}$ de 1 fixée. On voit alors facilement que

$$\sum_x \zeta^{xy} = \begin{cases} p & \text{si } y \equiv 0 \pmod p \\ 0 & \text{si } y \not\equiv 0 \pmod p. \end{cases} \tag{2}$$

Ces égalités vont nous permettre d'obtenir une expression très simple du nombre de solutions de la congruence (1).

Considérons la somme

$$S = \sum_{x_1, \ldots, x_n} \sum_x \zeta^{xF(x_1, \ldots, x_n)},$$

Si les valeurs $x_1, \ldots, x_n$ constituent une solution de la congruence **(1),** on a, en accord avec **(2),**

$$\sum_x \zeta^{xF(x_1, \ldots, x_n)} = p ;$$

si maintenant $F(x_1, \ldots, x_n) \not\equiv 0 \pmod p$, on a, toujours d'après **(2),**

$$\sum_x \zeta^{xF(x_1, \ldots, x_n)} = 0.$$

Ainsi S = Np, en désignant par N le nombre de solutions de la congruence (1). Énonçons ce résultat sous forme d'un théorème :

THÉORÈME *1. — Le nombre N de solutions de la congruence (1)* est donné par

$$N = \frac{1}{p} \sum_{x, x_1, \ldots, x_n} \zeta^{xF(x_1, \ldots, x_n)}. \tag{3}$$

Séparons les p^n termes de la somme (3) tels que $x \equiv 0 \bmod p$; chacun de ces termes est égal à 1 et on a donc

$$N = p^{n-1} + \frac{1}{p} \sum_{x}' \sum_{x_1, \ldots, x_n} \zeta^{xF(x_1, \ldots, x_n)} \tag{4}$$

Écrite ainsi, la formule donnant N suggère le théorème **B.** Il suffit seulement de démontrer (mais toute la difficulté est là !) que quand p croît, la somme des termes restants croît plus lentement que son terme principal.

2) Sommes de puissances

Nous appliquerons les résultats qui précèdent au cas où le polynôme **F** est de la forme

$$F(x_1, \ldots, x_n) = a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n}, \quad a_i \not\equiv 0 \pmod p.$$

Nous supposerons $n \geqslant 3$ puisque pour $n = 1$ ou $n = 2$ le nombre de solutions de la congruence $F \equiv 0 \pmod p$ se calcule trivialement.

En accord avec la formule (4), le nombre de solutions de la congruence

$$a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n} \equiv 0 \pmod p$$

est donné par la formule

$$N = p^{n-1} + \frac{1}{p} \sum_{x}' \sum_{x_1, \ldots, x_n} \zeta^{x\left(a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n}\right)},$$

qui peut aussi s'écrire

$$N = p^{n-1} + \frac{1}{p} \sum_{x}' \prod_{i=1}^{n} \sum_{x_i} \zeta^{a_i x_i^{r_i}}. \tag{5}$$

Cette formule nous conduit à l'étude des sommes de la forme

$$\sum_{\gamma} \zeta^{a\gamma^r} \qquad (a \not\equiv 0 \pmod p);$$

il est facile de vérifier que

$$\sum_{y} \zeta^{ay^r} = \sum_{x} m(x)\zeta^{ax}, \tag{6}$$

en désignant par m(x) le nombre de solutions en y de la congruence

$$y^r \equiv x \pmod{p}.$$

Il est clair que $m(0) = 1$; nous allons calculer m(x) pour $x \not\equiv 0 \pmod{p}$. Soit g une racine primitive modulo p; alors

$$x \equiv g^k \pmod{p}, \tag{7}$$

l'exposant k étant défini de manière unique modulo $p - 1$. Posant $y \equiv g_3^u \pmod{p}$, la congruence $y^r \equiv x \pmod{p}$ est équivalente à la congruence

$$ru \equiv k \pmod{(p - 1)}. \tag{8}$$

D'après la théorie générale des congruences du premier degré, la congruence (8) a $d = (r, p - 1)$ solutions en u ou n'a aucune solution suivant que k est divisible par d ou pas. Par suite,

$$m(x) = \begin{cases} d & \text{si } k \equiv 0 \pmod{d} \\ 0 & \text{si } k \not\equiv 0 \pmod{d}. \end{cases} \tag{9}$$

Donnons une autre évaluation plus utilisable du nombre m(x). Soit ε une racine primitive d'ordre d de 1 et définissons pour tous les nombres entiers x relativement premiers à p des fonctions χ_s ($s = 0, 1, \ldots, p - 1$) en posant

$$\chi_s(x) = \varepsilon^{ks} \tag{10}$$

où k vérifie la congruence (7) (d'après l'égalité $\varepsilon^{p-1} = 1$, la valeur ε^{ks} ne dépend pas du choix de k). Si $k \equiv 0 \pmod{d}$, alors $\varepsilon^{ks} = 1$ pour tout $s = 0, 1, \ldots, d - 1$ et par suite la somme

$$\sum_{s=0}^{d-1} \chi_s(x)$$

est égale à d. Si maintenant $k \not\equiv 0 \pmod{d}$ alors $\varepsilon^k \neq 1$ et par suite

$$\sum_{s=0}^{d-1} \varepsilon^{ks} = \frac{\varepsilon^{kd} - 1}{\varepsilon^k - 1} = 0.$$

Rapprochant ce résultat des égalités (9), nous obtenons (pour x non divisible par p) la formule

$$m(x) = \sum_{s=0}^{d-1} \chi_s(x)$$

L'expression donnée plus haut pour m(x) permet d'écrire l'égalité (6) sous la forme

$$\sum_{y} \zeta^{ay^r} = 1 + \sum_{x}{}' \sum_{s=0}^{d-1} \chi_s(x)\zeta^{ax}. \tag{11}$$

Les fonctions χ_s introduits ci-dessus possèdent, c'est clair, la propriété

$$\chi_s(xy) = \chi_s(x)\chi_s(y) \tag{12}$$

et s'appellent les ***caractères multiplicatif modulo p.*** Étendons-les à tous les entiers x en posant $\chi_s(x) = 0$ si x est divisible par p. Il est clair que, pour cette définition, la propriété (12) est conservée. Le caractère $\chi_0(n)$ dont la valeur pour px est égale à 1 s'appelle le ***caractère unité.***

Séparons dans la somme (11) les termes qui correspondent au caractère unité χ_0. Puisque

$$1 + \sum_{x}{}' \zeta^{ax} = \sum_{x} \zeta^{ax},$$

l'égalité (11) peut s'écrire sous la forme

$$\sum_{Y} \zeta^{ay^r} = \sum_{s=1}^{d-1} \sum_{x} \chi_s(x)\zeta^{ax} \tag{13}$$

(ici on peut considérer que x parcourt un système complet de résidus modulo p, puisque $\chi_s(x) = 0$ pour $x \equiv 0 \pmod p$).

Soient χ un des caractères χ_s et a un nombre entier. L'expression

$$\sum_{x} \chi(x)\zeta^{ax}$$

s'appelle ***somme de Gauss*** et se désigne par $\tau_a(\chi)$.

Les formules (5) et (13) nous permettent de formuler le théorème suivant.

THÉORÈME 2. — *Le nombre* N *de solutions de la congruence*

$$a_1x_1^{r_1} + \ldots + a_nx_n^{r_n} = 0 \pmod p, \qquad a_i \not\equiv 0 \pmod p \tag{14}$$

est donné par la formule

$$N = p^{n-1} + \frac{1}{p} \sum_{x}' \prod_{i=1}^{n} \sum_{s=1}^{d_i - 1} \tau_{a_i x}(\chi_{i,s}), \tag{15}$$

dans laquelle $d_i = (r_i, p-1)$, ***les caractères*** $\chi_{i,s}$ ***étant définis par l'égalité*** (10) ***avec*** $d = d_i$.

Remarquons que si un des d_i est égal à 1, i. e. si r_i relativement premier avec $p - 1$, alors dans la formule (15) la somme intérieure correspondante sera nulle (comme somme indexée par l'ensemble vide) et par suite dans ce cas on a la formule $N = p^{n-1}$. Cela est d'ailleurs clair directement puisque pour chaque choix des valeurs $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ il existe une valeur x_i et une seule pour laquelle la congruence (14) est satisfaite.

Le théorème 2 prend tout son sens grâce au fait que le module de la somme de Gauss peut être calculé exactement. Nous montrerons dans le point suivant que

$$|\tau_a(\chi)| = \sqrt{p} \quad \text{pour} \quad a \not\equiv 0 \pmod{p} \quad \text{et} \quad \chi \neq \chi_0$$

(cf. aussi exercice 8).

Voyons ce que donne le théorème (2) en utilisant ce résultat. Il résulte de la formule (15) que

$$|N - p^{n-1}| \leqslant \frac{1}{p} \sum_{x}' \prod_{i=1}^{n} \sum_{s=1}^{d_i - 1} |\tau_{a_i x}(\chi_{i,s})|$$

$$= \frac{1}{p} (p-1) \prod_{i=1}^{n} (d_i - 1) p^{\frac{1}{2}} = (p-1) p^{\frac{n}{2} - 1} \prod_{i=1}^{n} (d_i - 1).$$

Nous obtenons ainsi le théorème.

THÉORÈME 3. — ***Le nombre N de solutions de la congruence***

$$a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n} \equiv 0 \pmod{p}$$

pour tous les p premiers ne divisant pas $a_1, \ldots, a_n$ ***satisfait à l'inégalité***

$$|N - p^{n-1}| \leqslant C(p-1) p^{\frac{n}{2} - 1} \tag{16}$$

avec

$$C = (d_1 - 1) \ldots (d_n - 1), \qquad d_i = (r_i, p-1).$$

Pour $n \geqslant 3$, on peut obtenir le théorème B, pour les polynômes de la forme considérée, à partir du théorème 3. En effet

$$|N - p^{n-1}| \leqslant C p^{\frac{n}{2}} \leqslant C p^{n-1-\frac{1}{2}}$$

Remarquons, en passant, que l'inégalité (16) que nous avons obtenue pour $n > 3$ est plus précise que l'inégalité du théorème B.

Remarque. — Pour démontrer le théorème 3, il suffirait, d'après (5), de connaître une estimation du module de la somme $\sum_x \zeta^{ax^r}$. On peut obtenir une telle estimation plus rapidement, sans utiliser les sommes de Gauss (voir exercices 9 à 12 dus à H. M. Korobof). Nous exposons ici la démonstration avec les sommes de Gauss car les sommes de Gauss ontdenombreuses autres applications en théorie des nombres.

3) Module des sommes de Gauss

Considérons l'ensemble $\mathcal{F}$ de toutes les fonctions $f(x)$ à valeurs complexes définies pour x entier rationnel et telles que f(x) $\equiv f(y)$ si $x \equiv$ y (mod p). Puisque chaque fonction $f(x) \in 8$ est définie par ses valeurs sur un système complet de résidus modulo p, alors $\mathcal{F}$ est un espace vectoriel de dimension p sur le corps des nombres complexes. Introduisons sur $\mathcal{F}$ un produit scalaire hermitien en posant

$$(f, g) = \frac{1}{p} \sum_x f(x)\overline{g(x)} \qquad (f, g \in \mathcal{F}).$$

Une simple vérification montre que, pour ce produit scalaire, les p fonctions

$$f_a(x) = \zeta^{-ax} \qquad (a \text{ résidu mod } p) \tag{17}$$

forment une base orthonormale dans $\mathcal{F}$. En effet, d'après (2),

$$(f_a, f_{a'}) = \frac{1}{p} \sum_x \zeta^{(a'-a)x} = \begin{cases} 1 & \text{pour} \quad a \equiv a' \pmod p \\ 0 & \text{pour} \quad a \not\equiv a' \pmod p. \end{cases}$$

Les fonctions (17) qui possèdent la propriété

$$f_a(x + y) = f_a(x) f_a(y)$$

sont appelées des ***caractères additif modulo p.*** Cherchons les coordonnées d'un caractère multiplicatif χ dans la base (17). Soit

$$\chi = \sum_a \alpha_a f_a. \tag{18}$$

Alors

$$\alpha_a = (\chi, f_a) = \frac{1}{p} \sum_x \chi(x)\zeta^{ax} = \frac{1}{p} \tau_a(\chi). \tag{19}$$

Nous voyons ainsi que les sommes de Gauss $\tau_a(\chi)$ $\left(\text{à } \frac{1}{p} \text{ près}\right)$ sont les coordonnées du caractère multiplicatif χ dans la base des caractères additifs f_a.

Pour obtenir une importante relation entre les coordonnées a, (et par suite entre les sommes de Gauss $\tau_a(\chi)$), multiplions l'égalité

$$\chi(x) = \sum_a \alpha_a f_a(x) \tag{20}$$

par χ_c, oh c $\not\equiv 0 \pmod p$, et remplaçons l'indice de sommation a par ac :

$$\chi(cx) = \sum_a \chi(c)\alpha_{ac} f_{ac}(x) = \sum_a \chi(c)\alpha_{ac} f_a(cx).$$

Comparant ceci avec (20), nous obtenons

$$\alpha_a = \chi(c)\alpha_{ac}. \tag{21}$$

Supposant ici a = 1 et remarquant que $|\chi(c)| = 1$, nous trouvons

$$|\alpha_c| = |\alpha_1| \quad \text{pour } c \not\equiv 0 \pmod p. \tag{22}$$

Supposons maintenant que le caractère χ est distinct du caractère unité χ_0. Alors on peut choisir le nombre c (relativement premier avec p) tel que $\chi(c) \neq 1$ et l'égalité (21) pour a = 0 donne

$$\alpha_0 = 0. \tag{23}$$

Démontrons maintenant le résultat annoncé donnant le module de la somme de Gauss.

THÉORÈME 4. — *Si χ est un caractère multiplicatif modulo p, différent du caractère unité χ_0 et a un nombre entier relativement premier avec p, alors*

$$|\tau_a(\chi)| = \sqrt{p}.$$

DÉMONSTRATION. — Considérons dans l'espace $\mathcal{F}$ le produit scalaire (χ, χ). Puisque $|\chi(x)| = 1$ pour $x \not\equiv 0 \pmod p$, alors

$$(\chi, \chi) = \frac{1}{p}\sum_x \chi(x)\overline{\chi(x)} = \frac{p-1}{p}.$$

D'autre part, en utilisant l'expression (18) et en tenant compte de (22) et (23) nous trouvons

$$(\chi, \chi) = \sum_a |\alpha_a|^2 = (p-1)|\alpha_c|^2.$$

La réunion de ces deux résultats nous donne l'égalité

$$|\alpha_c| = \frac{1}{\sqrt{p}} \qquad (c \not\equiv 0 \pmod p),$$

d'où le résultat, d'après la formule (19).

EXERCICES

1. Montrer que le théorème A n'est pas vrai pour les solutions non nulles du polynôme $F = x^2 + y^2$ mais que, par contre, le théorème B est vrai pour le polynôme $F = x^2 - y^2$. Bien entendu, ces polynômes ne sont pas absolument irréductibles.

2. Soit $\varphi(x)$ une fonction définie pour tous les nombres entiers x premiers avec p et prenant des valeurs complexes différentes de zéro. Montrer que si $\varphi(x) = \varphi(y)$ pour $x \equiv y \pmod p$ et $\varphi(xy) = \varphi(x)\varphi(y)$, alors cette fonction coïncide avec une des fonctions $\chi_s(x) = \varepsilon^{ks}$, ε étant une racine primitive $(p-1)$-ème de 1 (k est défini par la congruence (7)).

3. Démontrer que toute fonction $f(x)$ de la variable entière x à valeurs complexes non nulles qui dépend seulement de la classe résiduelle de x modulo p et telle que $f(x + y) = f(x)f(y)$ est de la forme $f(x) = \zeta^{tx}$, où t est un certain entier et ζ une racine d'ordre p de 1.

4. Soit $p \neq 2$. Démontrer que le caractère $x = \chi_1$ défini par l'égalité (10) pour $d = 2$ (et $s = 1$) coïncide avec le symbole de Legendre :

$$\chi(x) = \left(\frac{x}{p}\right)$$

(ce caractère est appelé le *caractère quadratique* modulo p).

5. Supposons $ab \not\equiv 0 \pmod p$ et soit χ le caractère quadratique modulo $p \neq 2$. Démontrer la relation

$$\tau_a(\chi)\tau_b(\chi) = \left(\frac{-ab}{p}\right)p$$

pour les deux sommes de Gauss $\tau_a(\chi)$ et $\tau_b(\chi)$.

6. Avec les mêmes notations, démontrer que

$$\sum_x{}' \tau_x(\chi) = 0.$$

7. Résoudre les exercices 10, 11 et 12 du paragraphe précédent en utilisant le théorème 2 et les résultats des exercices 5 et 6.

8. Soient χ un caractère multiplicatif modulo p, différent du caractère χ_0 et $a \not\equiv 0 \pmod p$. Montrer que

$$|\tau_a(\chi)|^2 = \tau_a(\chi)\overline{\tau_a(\chi)} = p ;$$

en déduire une nouvelle démonstration du théorème 4.

9. Soient $f(x)$ un polynôme à coefficients entiers et ζ une racine primitive d'ordre m de 1. On pose $S_a = \sum_{x \bmod m} \zeta^{af(x)}$. Démontrer que l'on a

$$\sum_{a \bmod m} |S_a|^2 = m \sum_{c \bmod m} N(c)^2,$$

en désignant par N(c) le nombre de solutions de la congruence $f(x) \equiv c \pmod m$.

10. Soit ζ une racine primitive d'ordre p premier de 1 et posons $T_a = \sum_x' \zeta^{ax^r}$. Démontrer que

$$\sum_a' |T_a|^2 = p(p-1)(d-1),$$

avec $d = (r, p-1)$.

11. Avec les mêmes notations, montrer que les sommes T_a, a $\not\equiv 0 \pmod p$, sont décomposables en d groupes de $\frac{p-1}{d}$ sommes égales entre elles. Utilisant ce résultat et celui de l'exercice 1, en déduire que

$$|T_a| < d\sqrt{p}, \qquad a \not\equiv 0 \pmod p.$$

12. Remarquant que $\sum_a' T_a = 0$, obtenir pour T_a l'estimation meilleure

$$|T_a| \leqslant (d-1)\sqrt{p}, \qquad a \not\equiv 0 \pmod p$$

(D'après la formule (5), cette estimation nous donne une autre démonstration du théorème 3).

13. Montrer que la congruence

$$3x^3 + 4y^3 + 5z^3 \equiv 0 \pmod p,$$

a une solution non nulle pour tout p premier.

§ 3. — LES NOMBRES p-ADIQUES

1) Les nombres entiers p-adiques

Passons maintenant aux congruences modulo une puissance d'un nombre premier. Étudions un exemple. Soit la congruence

$$x^2 \equiv 2 \pmod{7^n}.$$

Pour $n = 1$, cette congruence a deux solutions :

$$x_0 = \pm 3 \pmod 7. \qquad (1)$$

Soit maintenant $n = 2$. De

$$x^2 \equiv 2 \pmod{7^2}, \tag{2}$$

résulte $x^2 \equiv 2 \pmod 7$ et par suite on peut chercher les solutions de la congruence (2) sous la forme $x_0 + 7t_1$, x_0 étant un des nombres définis par la congruence (1). Nous rechercherons les solutions de la forme $x_1 = 3 + 7t_1$ (les solutions de la forme $-3 + 7t_1$ s'étudient de la même manière). Portant cette expression de x_1 dans (2), nous obtenons

$$(3 + 7t_1)^2 \equiv 2 \pmod{7^2}$$
$$9 + 6.7t_1 + 7^2t_1^2 \equiv 2 \pmod{7^2}$$
$$1 + 6t_1 \equiv 0 \pmod 7$$
$$t_1 \equiv 1 \pmod 7.$$

D'où la solution $x_1 \equiv 3 + 7.1 \pmod{7^2}$.

De même, pour $n = 3$, on pose $x_2 = x_1 + 7^2t_2$ et à partir de la congruence

$$(3 + 7 + 7^2t_2)^2 \equiv 2 \pmod{7^3}$$

on obtient $t_2 \equiv 2 \pmod 7$, i. e.

$$x_2 \equiv 3 + 7.1 + 7^2.2 \pmod{7^3}.$$

Il est facile de voir que ce procédé s'étend indéfiniment. On obtient ainsi une suite

$$x_0, x_1, \ldots, x_n, \ldots \tag{3}$$

qui possède les propriétés :

$$x_0 \equiv 3 \pmod 7$$
$$x_n \equiv x_{n-1} \pmod{7^n}$$
$$x_n^2 \equiv 2 \pmod{7^{n+1}}.$$

Le procédé de construction de la suite (3) rappelle le procédé d'extraction de la racine carrée de 2. En effet, le calcul de $\sqrt{2}$ consiste en la construction d'une suite de nombres rationnels $r_1, r_2, \ldots, r_n, \ldots$ dont les carrés sont aussi proches que l'on désire de 2, par exemple

$$|r_n^2 - 2| < \frac{1}{10^n}.$$

Ici, on construit une suite de nombres entiers $x_0, x_1, \ldots, x_n, \ldots$ pour lesquels $x_n^2 - 2$ est divisible par 7^{n+1}. Cette analogie sera plus claire si nous convenons que deux nombres sont proches (plus exactement p-proches, p étant un nombre premier) quand leur différence est divisible par une puissance

de p suffisamment grande. On pourra dire alors que les carrés des nombres de la suite (3) sont, quand n croît, aussi 7-proches que l'on veut de 2.

La construction de la suite $\{ r_n \}$ définit le nombre réel $\sqrt{2}$. On peut dire que la suite (3) définit également un nombre a d'une « nouvelle nature » et tel, par suite, que $\alpha^2 = 2$.

Attirons l'attention du lecteur sur le fait suivant. Si une suite de nombres rationnels $\{ r'_n \}$ est telle que $| r_n - r'_n | < \frac{1}{10^n}$ pour tout n, alors sa limite sera encore $\sqrt{2}$. Nous supposerons donc également qu'une suite $\{ x'_n \}$ telle que $x_n \equiv x'_n \pmod{7^{n+1}}$ définit le même « nouveau nombre » a (pour cette nouvelle suite $\{ x'_n \}$, il est évident que l'on a aussi $x'^2_n \equiv 2 \pmod{7^{n+1}}$ et $x'_n \equiv x'_{n-1} \pmod 7$)).

Ces remarques nous conduisent à la définition suivante.

DÉFINITION. — *Soit p un nombre premier quelconque. Une suite de nombres entiers*

$$\{ x_n \} = \{ x_0, x_1, \ldots, x_n, \ldots \},$$

tels que

$$x_n \equiv x_{n-1} \pmod{p^n} \qquad (4)$$

définit un nouvel objet appelé nombre entier p-adique. Par définition deux suites $\{ x_n \}$ et $\{ x'_n \}$ définiront le même nombre entier p-adique si et seulement si $x_n \equiv x'_n \pmod{p_{n+1}}$ pour tout $n \geqslant 0$.

Nous exprimerons le fait que la suite $\{ x_n \}$ définit le nombre entier p-adique a par le symbole :

$$\{ x_n \} \to \alpha.$$

Nous désignerons par $\mathbf{Z}_p$ l'ensemble de tous les nombres entiers p-adiques. Pour les distinguer des nombres entiers p-adiques, les nombres entiers habituels seront appelés entiers rationnels.

A chaque nombre entier rationnel x, nous associerons le nombre entier p-adique défini par la suite { x, x, . . . , x, . . . } et nous désignerons par la même lettre x ce nombre entier p-adique. Deux entiers rationnels x et y distincts définissent deux entiers p-adiques distincts. En effet, leur égalité comme entiers p-adiques entraîne, pour tout n, la congruence $x \equiv y \pmod{p^n}$ ce qui exige x = y. Par suite, nous pourrons considérer l'ensemble Z des entiers rationnels comme un sous-ensemble de l'ensemble $\mathbf{Z}_p$ des nombres entiers p-adiques.

Pour concrétiser plus clairement l'ensemble $\mathbf{Z}_p$, donnons un procédé pour choisir une suite standard dans l'ensemble de toutes les suites définissant un nombre entier p-adique donné.

Soit un nombre entier p-adique défini par une suite $\{ x_n \}$. Désignons par $\bar{x}_n$ le plus petit nombre positif ou nul congru à x_n modulo p^{n+1} :

$$x_n \equiv \bar{x}_n \pmod{p^{n+1}} \tag{5}$$

$$0 \leqslant \bar{x}_n < p^{n+1}. \tag{6}$$

La congruence (5) montre que

$$\bar{x}_n \equiv x_n \equiv x_{n+1} \equiv \bar{x}_{n+1} \pmod{p^n} ;$$

ainsi, la suite $\{ \bar{x}_n \}$ définit un nombre entier p-adique, qui est le même que celui défini par la suite $\{ x_n \}$. Une suite dont tous les termes satisfont aux conditions (4) et (6) sera dite ***canonique.*** Ainsi, chaque entier p-adique est défini par une suite canonique.

Il est facile de voir que deux suites canoniques différentes définissent des entiers p-adiques différents. En effet, si deux suites canoniques $\{ \bar{x}_n \}$ et $\{ \bar{y}_n \}$ définissent le même entier p-adique, alors, d'après les congruences

$$\bar{x}_n \equiv \bar{y}_n \pmod{p^{n+1}}$$

et les conditions $0 \leqslant \bar{x}_n < p^{n+1}$, $0 \leqslant \bar{y}_n < p^{n+1}$, on a $\bar{x}_n = \bar{y}_n$ pour tout $n \geqslant 0$. Ainsi, les nombres entiers p-adiques sont en correspondance biunivoque avec les suites canoniques. La condition (4) entraîne que

$$\bar{x}_{n+1} = \bar{x}_n + a_{n+1}p^{n+1},$$

et, puisque $0 \leqslant \bar{x}_{n+1} < p^{n+2}$, on a $0 \leqslant a_{n+1} < p$; toute suite canonique est donc de la forme

$$\{ a_0, a_0 + a_1p, a_0 + a_1p + a_2p^2, \ldots \},$$

avec $0 \leqslant a_i < p$. Il est évident que, réciproquement, toute suite de cette forme est une suite canonique définissant un nombre entier p-adique. Il est facile de démontrer à partir de là que l'ensemble des suites canoniques et par conséquent l'ensemble des entiers p-adiques, ont la puissance du continu.

2) L'anneau des nombres entiers p-adiques

DÉFINITION. — ***On appelle somme et produit de deux nombres entiers p-adiques α et β définis par les suites $\{ x_n \}$ et $\{ y_n \}$ les nombres entiers p-adiques définis respectivement par les suites $\{ x_n + y_n \}$ et $\{ x_n y_n \}$.***

Pour que cette définition ait un sens, il faut montrer que les suites $\{ x_n + y_n \}$ et $\{ x_n y_n \}$ définissent des nombres entiers p-adiques et que ces nombres dependent seulement de α et β et non du choix des suites qui les définissent.

La démonstration de ces propriétés est triviale et nous l'omettrons.

Il est clair à partir de ces définitions que pour ces opérations, les entiers p-adiques forment un anneau commutatif contenant comme sous-anneau l'anneau Z des entiers rationnels.

La notion de divisibilité se définit ici comme dans tout anneau (voir appendice § 4-l)) : α est divisible par β s'il existe un entier p-adique y tel que $a = \beta\gamma$. Pour étudier les propriétés de divisibilité, il est important de connaître les entiers p-adiques qui admettent un inverse; ces nombres seront appelés diviseurs de l'unité, ou unités. Nous les appellerons aussi unités *p-adiques.*

THÉORÈME 1. — *Un nombre* entier *p-adique a défini par une suite* $\{ x_0, x_1, \ldots, x_n, \ldots \}$ *est une unité si et seulement si* $x_0 \not\equiv 0 \pmod{p}$.

DÉMONSTRATION. — Supposons que a est une unité. Il existe alors un entier p-adique β tel que $\alpha\beta = 1$. Si β est défini par la suite $\{ y_n \}$, la condition $\alpha\beta = 1$ signifie que

$$x_n y_n \equiv 1 \pmod{p^{n+1}}. \tag{7}$$

En particulier $x_0 y_0 \equiv 1 \pmod{p}$, d'où $x_0 \not\equiv 0 \pmod{p}$. Réciproquement, supposons $x_0 \not\equiv 0 \pmod{p}$. Il résulte facilement de (4) que

$$x_n \equiv x_{n-1} \equiv \ldots \equiv x_0 \pmod{p}$$

d'où $x_n \not\equiv 0 \pmod{p}$. Par suite, pour tout n, on peut trouver y_n tel que la congruence (7) soit vérifiée. Puisque $x_n \equiv x_{n-1} \pmod{p^n}$ et $x_n y_n \equiv x_{n-1} y_{n-1} \pmod{p^n}$, alors $y_n \equiv y_{n-1} \pmod{p_n}$. Cela signifie que la suite $\{ y_n \}$ définit un nombre entier p-adique β, qui est l'inverse de a d'après (7) .

Ce théorème entraîne qu'un nombre entier rationnel a, considéré comme un élément de l'anneau $\mathbf{Z}_p$, est une unité si et seulement si $a \not\equiv 0 \pmod{p}$. Si cette condition est remplie, alors $a^{-1} \in \mathbf{Z}_p$; il en résulte que tout entier rationnel b est divisible par a dans $\mathbf{Z}_p$, i. e. tout nombre rationnel de la forme $\frac{b}{a}$ où a et b sont entiers et $a \not\equiv 0 \pmod{p}$ appartient à $\mathbf{Z}_p$. Les nombres rationnels de cette forme sont appelés *p-entiers.* Ils forment un anneau de manière évidente. On peut formuler ainsi ce résultat :

COROLLAIRE. — *L'anneau* $\mathbf{Z}_p$ *des nombres* entiers *p-adiques contient un sous-anneau isomorphe à l'anneau des nombres rationnels p-entiers.*

THÉORÈME 2. — *Tout entier p-adique a différent de 0 s'écrit de manière unique sous la forme*

$$\alpha = p^m \varepsilon \tag{8}$$

où ε *est une unité de l'anneau* $\mathbf{Z}_p$

DÉMONSTRATION. — Si a est une unité, alors (8) est satisfait pour $m = 0$. Supposons que $\{ x_n \} \to a$ et que a n'est pas une unité, i. e. $x_0 \not\equiv 0 \pmod{p}$. Puisque $a \neq 0$, les congruences $x_n \equiv 0 \pmod{p^{n+1}}$ ne peuvent pas avoir lieu pour tout n; soit m le plus petit entier tel que :

$$x_m \not\equiv 0 \pmod{p^{m+1}}. \tag{9}$$

Pour $s \geqslant 0$,

$$x_{m+s} \equiv x_{m-1} \equiv 0 \pmod{p^m}$$

et par suite le nombre $y_s = \dfrac{x_{m+s}}{p^m}$ est un entier. De la congruence

$$p^m y_s - p^m y_{s-1} = x_{m+s} - x_{m+s-1} \equiv 0 \pmod{p^{m+s}},$$

il résulte que

$$y_s \equiv y_{s-1} \pmod{p^s}$$

pour tout $s \geqslant 0$. La suite $\{ y_s \}$ définit donc $\varepsilon \in \mathbf{Z}_p$. Puisque $y_0 = \dfrac{x_m}{p_m} \not\equiv 0 \pmod{p}$, il résulte alors du théorème 1 que ε est une unité. Enfin, la congruence $p^m y_s = x_{m+s} \equiv x_s \pmod{p^{s+1}}$ entraîne que $p^m \varepsilon = a$, i. e. on a la décomposition (8).

Supposons maintenant que a admette une autre décomposition $a = p^k \eta$ avec $k \geqslant 0$ et η une unité. Si $\{ z_s \} \to \eta$, alors

$$p^m y_s \equiv p^k z_s \pmod{p^{s+1}} \tag{10}$$

pour tout $s \geqslant 0$ et, d'après le théorème 1, tous les y, et z_s ne sont pas divisibles par p puisque ε et η sont des unités. Faisant $s = m$ dans la congruence (10), on obtient

$$p^m y_m \equiv p^k z_m \not\equiv 0 \pmod{p^{m+1}},$$

d'où l'inégalité $k \leqslant m$. Par symétrie, on a de même $m \leqslant k$, i. e. $k = m$. Remplaçons s par $s + m$ dans la congruence (10) et simplifions par p^m. Nous obtenons

$$y_{m+s} \equiv z_{m+s} \pmod{p^{s+1}},$$

et, puisque $y_{m+s} \equiv y, \pmod{p^{s+1}}$ et $z_{m+s} \equiv z_s \pmod{p^{s+1}}$ d'après (4), on a bien, pour tout $s \geqslant 0$,

$$y_s \equiv z_s \pmod{p^{s+1}},$$

ce qui montre que $\varepsilon = \eta$.

COROLLAIRE 1. — *Un nombre entier p-adique a défini par une suite* $\{x_n\}$ *est divisible par* p^k *si et seulement si* $x_n \equiv 0 \pmod{p^{n+1}}$ *pour tout*

$$n = 0, 1, \ldots, k - 1.$$

En effet, l'exposant m dans (8) a été défini comme le plus petit entier pour lequel on a (9).

COROLLAIRE *2. — L'anneau* $\mathbf{Z}_p$ *n'a pas de diviseur de zéro.*

En effet, si $\alpha \neq 0$ et $\beta \neq 0$, alors on a les représentations $\alpha = p^m\varepsilon$ et $\beta = p^k\eta$, ε et η étant des unités (ε et η ont donc des inverses ε^{-1} et η^{-1} dans l'anneau $\mathbf{Z}_p$). Si $\alpha\beta = 0$, alors, multipliant l'égalité $p^{m+k}\varepsilon\eta = 0$ par $\varepsilon^{-1}\eta^{-1}$, nous obtiendrions $p^{m+k} = 0$, ce qui est impossible.

DÉFINITION. — *Le nombre* m *qui figure dans la décomposition (8) d'un nombre entier p-adique a différent de zéro s'appelle la valuation p-adique de a et se désigne par* $\nu_p(\alpha)$.

Si le nombre premier p est fixé sans ambiguïté, on appellera simplement ce nombre la valuation de α et on le désignera par $\nu(a)$. Pour que la fonction $\nu(a)$ soit définie pour tous les nombres entiers p-adiques, nous poserons $\nu(0) = \infty$ (cette définition formelle est justifiée par le fait que 0 est divisible par des puissances de p arbitrairement grandes).

Une démonstration immédiate donne les propriétés suivantes de la valuation :

$$\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta) \tag{11}$$

$$\nu(\alpha + \beta) \geqslant \min(\nu(\alpha), \nu(\beta)) \tag{12}$$

$$\nu(\alpha + \beta) = \min(\nu(\alpha), \nu(\beta)), \quad \text{si } \nu(\alpha) \neq (\beta). \tag{13}$$

Les propriétés de divisibilité des nombres entiers p-adiques s'expriment très simplement au moyen de la valuation. En particulier, on obtient facilement, à partir du théorème 3 :

COROLLAIRE *3. — Un nombre entier p-adique a est divisible par* β *si et seulement si* $\nu(a) \geqslant \nu(\beta)$.

Ainsi, l'arithmétique de l'anneau $\mathbf{Z}_p$ est très simple. Il y a un seul élément premier (à un élément associé près), c'est le nombre p. Tout élément de $\mathbf{Z}_p$ différent de 0 est caractérisé par sa valuation et *son* unité.

En conclusion, nous étudierons les congruences dans l'anneau $\mathbf{Z}_p$. La congruence est définie ici comme pour les nombres entiers et plus généralement pour tout anneau (cf. appendice § 4-l)) : $a \equiv \beta \pmod{\gamma}$ signifie que $a - \beta$ est divisible par γ. Si $\gamma = p^n\varepsilon$, ε étant une unité, alors la congruence modulo γ est équivalente à la congruence modulo p^n. Par suite, on peut se limiter à l'examen des congruences modulo p^n.

THÉORÈME *3.* — ***Tout nombre entier p-adique est congru à un nombre entier rationnel modulo p^n. Deux nombres entiers rationnels sont congrus modulo p^n dans l'anneau $\mathbf{Z}_p$ si et seulement s'ils sont congrus modulo p^n dans l'anneau $\mathbf{Z}$.***

DÉMONSTRATION. — Pour démontrer la première affirmation, établissons que si a est un nombre entier p-adique et $\{ x_n \}$ une suite de nombres entiers rationnels qui le définit, alors

$$a \equiv x_{n-1} \pmod{p^n}. \tag{14}$$

Puisque x_{n-1} est défini par la suite $\{ x_{n-1}, x_{n-1}, \ldots \}$, une suite définissant $a - x_{n-1}$ est $\{ x_0 - x_{n-1}, x_1 - x_{n-1}, \ldots \}$. Appliquons à l'entier p-adique $a - x_{n-1}$ le corollaire 1 du théorème 2. Nous voyons que la congruence (14) équivaut aux congruences

$$x_n - x_{n-1} \equiv 0 \pmod{p^{k+1}}, \qquad k = 0, 1, \ldots . \text{ n-l},$$

dont la vérification découle de la condition (4) de la définition des entiers p-adiques.

Démontrons maintenant que pour deux entiers rationnels x et y, la congruence modulo p^n dans $\mathbf{Z}_p$ équivaut à la congruence modulo p^n dans $\mathbf{Z}$. Posons

$$x - y = p^m a, \qquad a \not\equiv 0 \pmod{p} \tag{15}$$

(on suppose $x \neq y$). La congruence

$$x \equiv y \pmod{p^n}. \tag{16}$$

dans l'anneau $\mathbf{Z}$ est équivalente à $n \leqslant m$. D'autre part (15) est la représentation (8) du nombre x — y puisque a est une unité p-adique. Par suite $v_p(x - y) = m$ et la condition $n \leqslant m$ peut s'écrire sous la forme $v_p(x-y) \geqslant n$, ce qui est équivalent à la congruence (16) dans $\mathbf{Z}_p$ puisque $v(p^n) = n$ (cf. corollaire 3 du théorème 2).

COROLLAIRE. — ***Le nombre des classes résiduelles modulo p^n dans $\mathbf{Z}_p$ est égal à p^n.***

3) Fractions p-adiques

Puisque l'anneau $\mathbf{Z}_p$ est sans diviseur de zéro (corollaire 2 du théorème 2), on peut l'inclure dans un corps en utilisant la construction du corps des fractions d'un domaine d'intégrité. Ici, cette construction nous conduit à étudier les fractions de la forme $\frac{\alpha}{p^k}$, où a est un entier p-adique quelconque et $k \geqslant 0$. La fraction est ici simplement un symbole commode pour désigner la paire (a, p^k).

DÉFINITION. — *Le symbole fractionnaire* $\frac{\alpha}{p^k}$, $a \in \mathbf{Z}_p$, $k \geqslant 0$ *définit un nombre fractionnaire p-adique ou, plus simplement, un nombre p-adique. Deux fractions* $\frac{\alpha}{p^k}$ *et* $\frac{\beta}{p^m}$ *définissent le même nombre p-adique si* $\alpha p^m = \beta p^k$ *dans* $\mathbf{Z}_p$

Nous désignerons par $\mathbf{Q}_p$ l'ensemble de tous les nombres p-adiques.

Tout nombre entier p-adique définit un élément $\frac{\alpha}{1} = \frac{\alpha}{p^0}$ de $\mathbf{Q}_p$. Il est clair que des nombres entiers p-adiques différents définissent des nombres p-adiques différents de $\mathbf{Q}_p$. Par suite, nous pouvons considérer $\mathbf{Z}_p$ comme un sous-ensemble de l'ensemble $\mathbf{Q}_p$.

Les opérations dans $\mathbf{Q}_p$ sont définies par les règles :

$$\frac{\alpha}{p^k} + \frac{\beta}{p^m} = \frac{\alpha p^m + \beta p^k}{p^{k+m}}$$

$$\frac{\alpha}{p^k} \cdot \frac{\beta}{p^m} = \frac{\alpha\beta}{p^{k+m}}.$$

Une vérification triviale montre que le résultat des opérations ci-dessus ne dépend pas du choix des fractions qui définissent les éléments correspondants de $\mathbf{Q}_p$ et que $\mathbf{Q}_p$ est un corps pour ces opérations, le ***corps des nombres p-adiques.*** Il est évident que la caractéristique du corps $\mathbf{Q}_p$ est nulle et par suite il contient le corps des nombres rationnels.

THÉORÈME *4.* — *Tout nombre p-adique* $\xi \neq 0$ *est représentable de manière unique sous la forme*

$$\xi = p^m \varepsilon, \tag{17}$$

où m est un entier rationnel et ε *une unité de* $\mathbf{Z}_p$

DÉMONSTRATION. — Soit $\xi = \frac{\alpha}{p^k}$, $a \in \mathbf{Z}_p$. D'après le théorème 2, $a = p^l \varepsilon$, $l \geqslant 0$, où ε est une unité de l'anneau $\mathbf{Z}_p$. Ainsi $\xi = p^m \varepsilon$ avec $m = l - k$. L'unicité de la représentation (17) découle de l'affirmation correspondante pour les nombres entiers p-adiques démontrée dans le théorème 2.

La notion de valuation introduite ci-dessus se généralise facilement aux nombres p-adiques. Nous poserons

$$v_p(\xi) = m,$$

où m est l'exposant dans la représentation (17). On vérifie facilement que les propriétés (1 1), (12) et (13) sont encore valables dans le corps $\mathbf{Q}_p$. Il est clair que le nombre p-adique ξ est un nombre entier p-adique si et seulement si $v_p(\xi) \geqslant 0$.

4) Convergence dans le corps des nombres p-adiques

Dans le sous-paragraphe 1), nous avons attiré l'attention sur l'analogie qui existe entre les nombres entiers p-adiques et les nombres réels : les uns et les autres sont définis par des suites de nombres rationnels.

Puisque chaque nombre réel est, comme on le sait, la limite de toute suite de nombres rationnels qui le définit, il est intuitif de penser qu'il en sera de même pour les nombres p-adiques pour une notion de convergence appropriée. Pour définir la limite d'une suite de nombres réels, on s'appuie essentiellement sur la notion de proximité : deux nombres réels ou rationnels sont considérés comme proches si la valeur absolue de leur différence est suffisamment petite. Pour définir la convergence dans le corps des nombres p-adiques, il faut donc définir la notion de nombres p-adiques proches.

Dans l'exemple du début de ce paragraphe, nous avons déjà parlé de la p-proximité de deux nombres entiers rationnels x et y en entendant par là que la différence $x - y$ est divisible par des puissances de p suffisamment grandes. Ainsi, apparaît une nouvelle analogie entre les nombres réels et p-adiques pour la notion de proximité. Si on utilise la notion de p-valuation ν_p, il est clair que la p-proximité de x et y sera caractérisée par la valeur du nombre $\nu_p(x - y)$. Cela signifie que deux nombres p-adiques quelconques ξ et η (non nécessairement entiers) doivent être considérés comme proches si la valeur $\nu_p(x - y)$ est suffisamment grande. En d'autres termes, les nombres p-adiques « petits » sont caractérisés par de grandes valeurs de leurs valuations.

Après ces remarques préparatoires, passons à une définition précise.

DÉFINITION. — Une suite

$$\{\xi_n\} = \{\xi_0, \xi_1, \ldots, \xi_n, \ldots\}$$

de nombres p-adiques est dite convergente vers un nombre p-adique ξ ***(ce que nous noterons*** $\lim_{n\to\infty} \xi_n = \xi$ ou $\{\xi_n\} \to \xi$***) si***

$$\lim_{n\to\infty} \nu_p(\xi_n - \xi) = \infty.$$

On peut donner à la définition ci-dessus un aspect moins surprenant en considérant, au heu de l'exposant ν_p défini sur le corps $\mathbf{Q}_p$, une autre fonction, à valeurs réelles positives, qui tend vers 0 lorsque l'exposant tend vers l'infini. Par exemple, choisissant un nombre réel ρ tel que $0 < \rho < 1$, posons

$$\varphi_\rho(\xi) = \begin{cases} \rho^{\nu_p(\xi)} & \text{si} \quad \xi \neq 0 \\ 0 & \text{si} \quad \xi = 0. \end{cases} \tag{18}$$

DÉFINITION. — *La fonction $\varphi_p(\xi)$, $\xi \in \mathbf{Q}_p$, définie la formule (18) s'appelle une métrique p-adique. La valeur du nombre $\varphi_p(\xi)$ s'appelle la grandeur du nombre p-adique ξ pour cette métrique.*

Comme pour la valuation, nous dirons fréquemment que la fonction φ_p est une métrique et nous la désignerons par cp.

Il résulte facilement des propriétés (11) et (12) de l'exposant que la métrique possède les propriétés :

$$\varphi(\xi\eta) = \varphi(\xi)\,\varphi(\eta) \tag{19}$$

$$\varphi(\xi + \eta) \leqslant \max(\varphi(\xi), \varphi(\eta)). \tag{20}$$

Cette dernière inégalité entraîne d'ailleurs

$$\varphi(\xi + \eta) \leqslant \varphi(\xi) + \varphi(\eta). \tag{21}$$

Les propriétés (19) et (21) et la propriété $\varphi(\xi) > 0$ pour $\xi \neq 0$ montrent que la notion de métrique introduite ci-dessus pour les nombres p-adiques est analogue à la notion de valeur absolue sur le corps des nombres réels (ou de module sur le corps des nombres complexes).

A l'aide de la métrique φ_p, la définition de la convergence dans le corps $\mathbf{Q}_p$ devient : la suite $\{\xi_n\}$, $\xi_n \in \mathbf{Q}_p$, converge vers le nombre p-adique ξ si

$$\lim_{n\to\infty} \varphi_p(\xi_n - \xi) = 0.$$

On peut facilement formuler et démontrer pour le corps $\mathbf{Q}_p$ les théorèmes habituels de l'analyse sur les limites des suites. Montrons par exemple que si $\{\xi_n\} \to \xi$ et $\xi \neq 0$, alors $\left\{\frac{1}{\xi_n}\right\} \to \frac{1}{\xi}$. Tout d'abord, à partir d'un certain rang, i. e. $n \geqslant n_0$, nous aurons $\nu(\xi_n - \xi) > \nu(\xi)$, d'où, d'après (13),

$$\nu(\xi_n) = \min(\nu(\xi_n - \xi), \nu(\xi)) = \nu(\xi);$$

en particulier $\nu(\xi_n) \neq$ co, i. e. $\xi_n \neq 0$ et par suite $\frac{1}{\xi_n}$ a un sens pour tout $n \geqslant n_0$. De plus,

$$\nu\left(\frac{1}{\xi_n} - \frac{1}{\xi}\right) = \nu(\xi - \xi_n) - \nu(\xi_n) - \nu(\xi) = \nu(\xi_n - \xi) - 2\nu(\xi) \to \infty$$

pour $n \to \infty$, ce qui démontre notre affirmation.

THÉORÈME 5. — *Si le nombre entierp-adique α est défini par une suite $\{x_n\}$ de nombres entiers rationnels, alors cette suite converge vers a. Tout nombre p-adique ξ est limite d'une suite de nombres rationnels.*

DÉMONSTRATION. — De la congruence (14) résulte que $v_p(x_n - a) \geqslant n + 1$. Par suite $v(x_n - \alpha) \to \infty$ pour $n \to \infty$, donc $x_n \to a$. Considérons maintenant une fraction p-adique $\xi = \frac{\alpha}{p^k}$. Puisque

$$v\left(\frac{x_n}{p^k} - \xi\right) = v\left(\frac{x_n - \alpha}{p^k}\right) = v(x_n - \alpha) - k \to \infty$$

pour $n \to \infty$, ξ est la limite de la suite de nombres rationnels $\left\{\frac{x_n}{p^k}\right\}$.

De toute suite bornée de nombres réels on peut toujours, comme on le sait, extraire une sous-suite convergente. On a une propriété analogue pour les nombres p-adiques.

DÉFINITION. — ***Une suite $\{\xi_n\}$ de nombres p-adiques est dite bornée si toutes les valeurs $\varphi_p(\xi_n)$ sont bornées supérieurement ou, ce qui revient au même,*** si ***tous les nombres $v_p(\xi_n)$ sont bornés inférieurement.***

THÉORÈME 6. — *De* toute ***suite bornée de nombres p-adiques (en particulier, de toute suite de nombres entiers p-adiques) on peut extraire une sous-suite convergente.***

DÉMONSTRATION. — Démontrons tout d'abord le théorème pour une suite $\{a_n\}$ de nombres entiersp-adiques. Puisque dans l'anneau $\mathbf{Z}_p$ le nombre de classes résiduelles modulo p est fini (corollaire du théorème 3), il existe dans la suite a_n une infinité de termes congrus modulo p à un même nombre entier rationnel x_0. Extrayant tous ces termes, nous obtenons une suite $\{\alpha_n^{(1)}\}$ dont tous les termes satisfont à la congruence

$$\alpha_n^{(1)} \equiv x_0 \pmod{p}.$$

De la même manière, on extrait de la suite $\alpha_n^{(1)}$ une suite $\alpha_n^{(2)}$ telle que

$$\alpha_n^{(2)} \equiv x_1 \pmod{p^2},$$

où x_1 est un certain nombre entier rationnel. Continuant ce processus indéfiniment, nous obtenons pour tout k une suite $\{\alpha_n^{(k)}\}$ qui est une sous-suite de la suite précédente $\{\alpha_n^{(k-1)}\}$ et dont les termes vérifient la congruence

$$\alpha_n^{(k)} \equiv x_{k-1} \pmod{p^k}$$

pour un certain entier rationnel x_{k-1}. Puisque $x_k \equiv \alpha_n^{(k+1)} \pmod{p^{k+1}}$ et puisque la suite $\{\alpha_n^{(k+1)}\}$ est extraite de la suite $\{\alpha_n^{(k)}\}$, alors

$$x_k \equiv x_{k-1} \pmod{p^k}$$

pour tout $k \geqslant 1$. La suite $\{ x \}$ définit par suite un certain nombre entier p-adique a. Formons maintenant la « suite diagonale » $\{ \alpha_n^{(n)} \}$. Il est clair que c'est une sous-suite extraite de la suite a_n; montrons que $\{ \alpha_n^{(n)} \} \to a$. En effet, d'après (14), nous avons : $a \equiv x_{n-1} \pmod{p^n}$; d'autre part

$$\alpha_n^{(n)} \equiv x_{n-1} \pmod{p^n}$$

et par suite $\alpha_n^{(n)} \equiv a \pmod{p^n}$, i. e. $v(\alpha_n^{(n)} - a) \geqslant n$. Ainsi $v(\alpha_n^{(n)} - a) \to \infty$ pour $n \to \infty$, i. e. $\{ \alpha_n^{(n)} \} \to a$.

Demontrons le théorème dans le cas général. Si pour une suite de nombres p-adiques $\{ \xi_n \}$ on a $v(\xi_n) \geqslant -k$ (k étant un entier rationnel), alors pour $a_n = \xi_n p^k$, on aura $v(\alpha_n) \geqslant 0$ et a_n est un nombre entier p-adique. D'après ce qui précède, on peut extraire de la suite $\{ a_n \}$ de nombres entiers p-adiques une suite convergente $\{ \alpha_{n_i} \}$. Mais alors, la suite $\{ \xi_{n_i} \} = \{ \alpha_{n_i} p^{-k} \}$ est une sous-suite convergente de $\{ \xi_n \}$. Ceci termine la démonstration.

Les nombres p-adiques vérifient également le critère de Cauchy : une suite

$$\{ \xi_n \}, \qquad \xi_n \in \mathbf{Q}_p, \tag{22}$$

est convergente si et seulement si

$$\lim_{m,n \to \infty} v(\xi_m - \xi_n) = \infty. \tag{23}$$

La nécessité de cette condition est claire. Pour dtmontrer la suffisance, remarquons tout d'abord que (23) entraîne que la suite (22) est bornée. En effet, la condition (23) entraîne l'existence d'un n_0 tel que $v(\xi_m - \xi_{n_0}) \geqslant 0$ pour tout $m \geqslant n_0$. Mais alors, d'après la propriété (12), pour tout $m \geqslant n_0$, on a l'inégalité

$$v(\xi_m) = v((\xi_m - \xi_{n_0}) + \xi_{n_0}) \geqslant \min (0, v(\xi_{n_0})) ;$$

ainsi (22) est bornée. D'après le théorème 6, on peut extraire de (22) une sous-suite $\{ \xi_{n_i} \}$ convergente vers un certain nombre ξ. Soit M un nombre quelconque, arbitrairement grand; d'après (23) et la définition de la convergence, il existe un entier naturel N tel que $v(\xi_m - \xi_n) \geqslant$ M pour $m, n \geqslant N$ et $v(\xi_{n_i} - \xi) \geqslant$ M pour $n \geqslant$ N. Par suite

$$v(\xi_m - \xi) \geqslant \min (v(\xi_m - \xi_{n_i}), \quad v(\xi_{n_i} - \xi)) \geqslant \mathrm{M}$$

pour tout $m \geqslant$ N. Par suite, $\lim_{m \to \infty} v(\xi_m - \xi) = \infty$, i. e. la suite (22) est convergente.

On peut donner une forme plus forte au critère de convergence dans le

corps des nombres p-adiques. Si la suite (22) satisfait à la condition **(23),** il est clair que

$$\lim_{n\to\infty} v(\xi_{n+1} - \xi_n) = \infty. \tag{24}$$

Montrons maintenant que la condition (24) entraîne (23). En effet, si $v(\xi_{n+1} - \xi_n) \geqslant M$ pour tout $n \geqslant N$, d'après **(12),** l'égalité

$$\xi_m - \xi_n = \sum_{i=n}^{m-1} (\xi_{i+1} - \xi_1), \qquad m > n \geqslant N,$$

entraîne

$$v(\xi_m - \xi_n) \geqslant \min_{i=n,\ \ldots,\ m-1} v(\xi_{i+1} - \xi_i) \geqslant M,$$

i. e. $v(\xi_m - \xi_n) \to \infty$ pour $m, n \to \infty$. Ainsi, on a :

THÉORÈME 7. — *Pour qu'une suite* $\{ \xi_n \}$ *de nombres p-adiques soit convergente, il faut et il suffit que*

$$\lim_{n\to\infty} v(\xi_{n+1} - \xi_n) = \infty.$$

L'existence d'une notion de convergence dans le corps $\mathbf{Q}_p$ nous permet de parler de fonctions p-adiques continues d'une variable p-adique. Une fonction $F(\xi)$ sera dite continue pour $\xi = \xi_0$ si pour toute suite $\{ \xi_n \}$ convergente vers ξ_0, la suite des valeurs $\{ F(\xi_n) \}$ converge vers $F(\xi_0)$. La définition pour des fonctions de plusieurs variables est analogue. De même que dans l'analyse réelle, on démontre facilement les théorèmes usuels sur les opérations arithmétiques appliquées aux fonctions p-adiques continues. En particulier, il est facile de vérifier que tout polynôme d'un nombre quelconque de variables à coefficients p-adiques est une fonction p-adique continue. Nous utiliserons par la suite ce résultat simple (§ 5, 1)).

Pour terminer, donnons quelques résultats sur les séries p-adiques.

DÉFINITION. — ***Si la suite des sommes partielles***

$$S_n = \sum_{i=0}^{n} \alpha_i$$

d'une série

$$\sum_{i=0}^{\infty} \alpha_i = \alpha_0 + \alpha_1 + \ldots + a_n + \ldots \tag{25}$$

à termes p-adiques, converge vers un nombre p-adique α, ***on dit que cette série converge et que sa somme est égale à a.***

Le théorème 7 entraîne immédiatement le critère suivant de convergence des séries.

THÉORÈME *8.* — ***Pour que la série (25) soit convergente, il faut et il suffit que son terme général tende vers zéro, i. e. que*** $\nu(\alpha_n) \to \infty$ ***pour*** $n \to \infty$.

Il est clair que l'on peut additionner, soustraire et multiplier par un nombre p-adique constant des séries p-adiques.

THÉORÈME *9.* — ***La convergence et la somme d'une série ne changent pas si on permute l'ordre des termes.***

Nous laissons au lecteur la démonstration très simple de ce théorème.

On montre dans les cours classiques d'analyse dans le domaine réel que la propriété exprimée par le théorème 9 caractérise les séries absolument convergentes. Ainsi, toutes les séries p-adiques convergentes sont « absolument convergentes ». Il en résulte facilement que dans le corps des nombres p-adiques on peut multiplier les séries convergentes selon les règles usuelles de l'analyse classique.

Si le nombre entier p-adique a est défini par la suite canonique

$$\{ a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots \} \qquad \text{(cf. § 1)},$$

alors, en accord avec le théorème 5, il est égal à la somme de la série convergente

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots \tag{26}$$
$$0 \leqslant a_n \leqslant p - 1 \qquad (n = 0, 1, \ldots).$$

Puisque des suites canoniques différentes définissent des nombres entiers p-adiques différents, la représentation de α comme somme d'une série du type (26) est unique. Réciproquement, il est évident que toute série de type (26) converge vers un certain nombre entier p-adique.

La représentation des nombres entiers p-adiques par des séries du type (26) rappelle l'écriture des nombres réels sous forme de fractions décimales infinies.

Si on considère plus généralement la série

$$b_0 + b_1 p + \ldots + b_n p^n + \ldots \tag{27}$$

oh les b_i sont des entiers rationnels quelconques, il est clair qu'elle converge vers un certain entier p-adique a (puisque $\nu(b_n p^n) \geqslant n$). Pour obtenir la représentation du nombre a comme somme d'une strie du type (26), il faut remplacer successivement chaque coefficient b_n par le reste de sa division par p, en faisant rentrer le quotient partiel obtenu dans le terme suivant. Cette remarque est très importante pour effectuer des opérations dans l'anneau $\mathbf{Z}_p$, car en ajoutant, soustrayant ou multipliant des séries (26) suivant les règles usuelles de l'analyse on obtient des séries du type (27).

Il résulte facilement du théorème 1 qu'un entier p-adique représenté comme somme de la série (26) est une unité de $\mathbf{Z}_p$ si et seulement si $a \neq 0$. Réuni au théorème 4, cela nous donne le résultat suivant

THÉORÈME 10. — Tout nombre p-adique $\xi \neq 0$ s'écrit de manière unique sous la forme

$$\xi = p^m(a_0 + a_1 p + \ldots + a_n p^n + \ldots) \tag{28}$$

avec

$$m = v_p(\xi),\ 1 \leqslant a_0 \leqslant p-1,\ 0 \leqslant a_n \leqslant p-1\ (n = 1, 2, \ldots).$$

EXERCICES

1. Posant $x_n = 1 + p + \ldots + p^{n-1}$, montrer que dans le corps des nombres p-adiques, la suite $\{ x_n \}$ converge vers $\frac{1}{1 - p}$.

2. Soient $p \neq 2$ et c un résidu quadratique modulo p. Montrer qu'il existe deux nombres p-adiques distincts dont les carres sont égaux à c.

3. Soit c un entier rationnel non divisible par p. Montrer que la suite $\{ c^{p^n} \}$ est convergente dans le corps $\mathbf{Q}_p$. Soit y la limite de cette suite; montrer que

$$y \equiv c \pmod{p} \qquad \text{et} \qquad y^{p-1} = 1.$$

4. Utilisant l'exercice précédent, montrer que le polynôme $t^{p-1} - 1$ se décompose en facteurs linéaires dans le corps $\mathbf{Q}_p$

5. Dans le corps des nombres p-adiques, écrire le nombre -1 comme somme d'une série du type (26).

6. Dans le corps des nombres 5-adiques, écrire le nombre $-\frac{2}{3}$ comme somme d'une série du type (26).

7. Pour $p \neq 2$, montrer qu'il n'existe pas d'autre racine $p^{\text{ième}}$ de 1 que 1 dans le corps des nombres p-adiques.

8. Dans le corps $\mathbf{Q}_p$, montrer que, dans la représentation d'un nombre rationnel $\neq 0$ comme somme d'une série (28), les coefficients sont périodiques (à partir d'un certain rang). Réciproquement, toute série du type (28) telle que $a_{m+k} = a_k$ pour $k \geqslant k_0$ $(m > 0)$ a pour somme un nombre rationnel.

9. Pour les polynômes sur le corps des nombres p-adiques, démontrer le test d'irréductibilité d'Eisenstein : le polynômef (x) = $a_0x^n + a_1x^{n-1} + \ldots + a_n$ à coefficients entiers p-adiques est irréductible si, a_0 n'étant pas divisible par p et tous les autres coefficients étant divisibles par p, le terme constant a_n n'est pas divisible par p^2.

10. Montrer qu'il existe des extensions finies de degré quelconque du corps des nombres p-adiques.

11. Démontrer, que pour des nombres premiers p et q distincts, les corps $\mathbf{Q}_p$ et $\mathbf{Q}_q$ ne sont pas isomorphes. Démontrer également qu'aucun des corps $\mathbf{Q}_p$ n'est isomorphe au corps des nombres réels.

12. Démontrer que le seul automorphisme du corps des nombres p-adiques est l'identité (c'est également vrai pour le corps des nombres réels).

§ 4. — CARACTÉRISATION AXIOMATIQUE DU CORPS DES NOMBRES p-ADIQUES

Le corps des nombres p-adiques est un des instruments fondamentaux de la théorie des nombres. Les paragraphes suivants de ce chapitre seront consacrés à quelques applications. Cependant, nous nous écarterons ici de l'esprit fondamental de ce chapitre en situant les corps de nombres p-adiques dans la théorie générale des corps.

1) Les corps métriques

Nous avons déjà souligné l'analogie qui existe entre les nombres p-adiques et les nombres réels. Nous exposerons ici une axiomatique des corps métriques qui comprend ces deux exemples comme cas particuliers. Cette méthode, dans le cas particulier des nombres réels, coïncide avec la méthode de construction des nombres réels à partir des suites de Cauchy, due à Cantor.

L'extension de la méthode de Cantor à d'autres corps repose sur les remarques suivantes. La notion essentielle ici est celle de convergence d'une suite de nombres rationnels. Cette notion s'appuie elle-même sur la notion de valeur absolue (on dit qu'une suite de nombres rationnels $\{ r_n \}$ converge vers un nombre rationnel r si la valeur absolue $| r_n - r |$ tend vers zéro). Remarquons que l'on utilise ici seulement des propriétés simples de la valeur absolue. Par suite, si on suppose l'existence sur un corps k d'une fonction à valeurs réelles possédant les mêmes propriétés fondamentales que la valeur absolue, on peut définir dans k une notion de convergence et, en appliquant la méthode de Cantor, construire un nouveau corps.

DÉFINITION. — ***Soit k un corps. Une fonction φ définie sur les éléments α du corps k et à valeurs réelles s'appelle une métrique si elle possède les propriétés suivantes***

1° $\varphi(\alpha) > 0$ pour $\alpha \neq 0$, $\varphi(0) = 0$;

2° $\varphi(\alpha + \beta) \leqslant \varphi(\alpha) + \varphi(\beta)$;

3° $\varphi(\alpha\beta) = \varphi(\alpha)\,\varphi(\beta)$.

Un corps k muni d'une métrique s'appelle un corps métrique (et est parfois désigné par (k, φ)). De cette définition découlent facilement les propriétés suivantes :

$$\varphi(\pm 1) = 1 ;$$
$$\varphi(-\alpha) = \varphi(\alpha) ;$$

$$\varphi(\alpha - \beta) \leqslant \varphi(\alpha) + \varphi(\beta);$$
$$\varphi(\alpha \pm \beta) \geqslant |\varphi(\alpha) - \varphi(\beta)|;$$
$$\varphi\left(\frac{\alpha}{\beta}\right) = \frac{\varphi(\alpha)}{\varphi(\beta)} \quad (\beta \neq 0).$$

Donnons des exemples de métriques :

1° la valeur absolue dans le corps des nombres rationnels;

2° la valeur absolue dans le corps des nombres réels;

3° le module dans le corps des nombres complexes;

4° la métrique p-adique φ_p, définie au § 3-4), sur le corps $\mathbf{Q}_p$ des nombres p-adiques;

5° la fonction $\varphi(\alpha)$ définie sur un corps quelconque k par les conditions

$$\varphi(0) = 0, \qquad y(a) = 1 \qquad \text{si} \qquad a \neq 0.$$

Une telle métrique est dite triviale.

Si on considère la restriction au corps Q des rationnels de la métrique φ_p définie sur $\mathbf{Q}_p$, on obtient une nouvelle métrique sur Q. Cette métrique, que nous désignerons encore par φ_p, s'appelle métriquep-adique du corps **Q.** Sa valeur sur un nombre rationnel $x = p^{v_p(x)}\frac{a}{b}$ (a et b non divisible par p) est donnée par

$$\varphi_p(x) = \rho^{v_p(x)}, \tag{1}$$

où ρ est un nombre rtel fixé satisfaisant à la condition $0 < \rho < 1$. Nous verrons ci-dessous que la construction de Cantor appliquée au corps des nombres rationnels muni de la métrique p-adique (au lieu de la valeur absolue) nous conduit au corps $\mathbf{Q}_p$ des nombres p-adiques.

Dans tout corps métrique (k, φ), on peut définir une notion de convergence : une suite $\{\alpha_n\}$ d'éléments de k est dite convergente vers un élément $a \in k$ si $\varphi(\alpha_n - a) \to 0$ pour $n \to \infty$. On dit encore que a est la limite de $\{a,\}$ et on écrit

$$\{\alpha_n\} \to \alpha \qquad \text{ou} \qquad a = \lim_{n\to\infty} \alpha_n.$$

DÉFINITION. — *Une suite $\{a_n\}$ d'éléments d'un corps métrique k est dite de Cauchy pour la métrique φ si $\varphi(\alpha_n - a_m) \to 0$ pour $n, m \to \infty$.*

Il est clair que toute suite convergente est de Cauchy. En effet, si $\{a,\} \to a$, alors, d'après l'inégalité

$$\varphi(\alpha_n - \alpha_m) = \varphi(\alpha_n - \alpha + \alpha - \alpha_m) \leqslant \varphi(\alpha_n - \alpha) + \varphi(\alpha_m - \alpha),$$
$$\varphi(\alpha_n - \alpha_m) \to 0 \text{ (car } \varphi(\alpha_n - a) \to 0 \quad \text{et} \quad \varphi(\alpha_m - \alpha) \to 0).$$

La réciproque n'est pas vraie pour tous les corps métriques; elle est vraie pour le corps réel et pour les corps p-adiques, d'après le critère de Cauchy (§ 3, 4)), mais n'est pas vraie pour le corps des rationnels muni de la valeur absolue ou d'une métrique p-adique.

DÉFINITION. — *Un corps métrique est dit complet si toute suite de Cauchy est convergente.*

La méthode de Cantor consiste à plonger le corps non complet des nombre rationnels (en prenant la valeur absolue comme métrique) dans le corps complet des nombres rationnels. On montre qu'un tel plongement est possible pour tout corps métrique, en transcrivant presque littéralement la construction introduite par Cantor.

Fixons la terminologie suivante. On dira qu'un corps métrique (k, φ) est un sous-corps d'un corps métrique (k_1, φ_1) si $k \subset k_1$ et si $\varphi(x) = \varphi_1(x)$ pour $x \in k$. De plus, un sous-ensemble d'un corps k sera dit partout dense dans k si tout élément de k est limite d'une suite d'éléments de ce sous-ensemble. On a alors le théorème 1.

THÉORÈME 1. — *Pour tout corps métrique k, il existe un corps métrique complet $\bar{k}$ contenant k comme sous-corps partout dense.*

Pour énoncer le théorème suivant, nous avons encore besoin d'une définition.

DÉFINITION. — *Soient (k_1, φ_1)* et *(k_2, φ_2) deux corps métriques isomorphes entre eux. Un isomorphisme $\sigma : k_1 \to k_2$ est dit bicontinu ou topologique si pour toute suite $\{ a_n \}$ d'éléments de k_1 convergente vers a pour la métrique φ_1, la suite $\sigma(\alpha_n)$ converge vers $\sigma(\alpha)$ pour la métrique φ_2 et réciproquement.*

THÉORÈME 2. -*Le corps $\bar{k}$ introduit dans le théorème 1 est défini de manière unique, à un isomorphisme topologique près laissant jixe les éléments du corps k.*

DÉFINITION. — *Le corps $\bar{k}$, dont l'existence et l'unicité sont établies par les théorèmes 1 et 2 s'appelle le complété du corps k.*

Il est clair que le corps des nombres réels est le complété du corps des nombres rationnels Q, muni de la valeur absolue comme métrique. Si on munit le corps des nombres rationnels de la métrique p-adique (1), alors le complété de ce corps métrique est le corps $\mathbf{Q}_p$ des nombres p-adiques. En effet, d'après la deuxième partie du théorème 5 du § 3, Q est partout dense dans $\mathbf{Q}_p$ et le critère de convergence de Cauchy (théorème 7, § 3) montre que $\mathbf{Q}_p$ est complet. Nous avons ainsi obtenu une nouvelle définition axiomatique du corps des nombres p-adiques.

Le corps des nombres p-adiques est le complété du corps des nombres rationnels muni de la métrique p-adique (1).

Passons à la démonstration rapide des théorèmes 1 et 2, en omettant les passages qui reproduisent textuellement les raisonnements classiques du cas réel.

DÉMONSTRATION DU THÉORÈME 1. — Nous dirons que deux suites de Cauchy $\{x_n\}$ et $\{y_n\}$ d'éléments du corps métrique (k, φ) sont équivalentes si la suite $\{x_n - y_n\}$ tend vers zéro. Nous désignerons par $\bar{k}$ l'ensemble de toutes les classes d'équivalence de suites de Cauchy pour cette relation. Définissons de la manière suivante des opérations dans $\bar{k}$: si α et β sont deux classes et $\{x_n\} \in a$, $\{y_n\} \in \beta$ alors nous appellerons somme (resp. produit) des classes a et β la classe de la suite $\{x_n + y_n\}$ (resp. $\{x_n y_n\}$). Il est facile de démontrer que $\{x_n + y_n\}$ et $\{x_n y_n\}$ sont effectivement des suites de Cauchy et que leurs classes ne dépendent pas du choix des suites $\{x_n\}$ et $\{y_n\}$ dans les classes a et β.

Une vérification évidente montre que $\bar{k}$ est un anneau avec unité; la classe nulle et la classe unité sont les classes des suites (0, 0, . . .) et (1, 1, 1, . ..).

Démontrons que $\bar{k}$ est un corps. Si a est une classe différente de zéro et $\{x_n\} \in a$, alors il est facile de voir que tous les x_n sont différents de zéro à partir d'un certain rang (par exemple pour $n \geqslant n_0$). Considérons la suite $\{y_n\}$ définie par

$$y_n = \begin{cases} 1 & \text{pour} \quad n < n_0 \\ \dfrac{1}{x_n} & \text{pour} \quad n \geqslant n_0. \end{cases}$$

On vérifie facilement que $\{y_n\}$ est une suite de Cauchy et que sa classe est l'inverse de la classe a.

Définissons maintenant une métrique sur le corps $\bar{k}$. Remarquons pour cela que, comme il est facile de le vérifier, si $\{x_n\}$ est une suite de Cauchy d'éléments du corps k, alors $\{\varphi(x_n)\}$ est une suite de Cauchy de nombres réels, donc est convergente vers un certain nombre réel qui ne dépend que de la classe d'équivalence de $\{x_n\}$. Nous poserons $\varphi(\alpha) = \lim_{n\to\infty} \varphi(x_n)$ si a est la classe contenant la suite $\{x_n\}$. Il est facile de vérifier que la fonction φ ainsi définie est une métrique et par suite $(\bar{k}, \varphi)$ est un corps métrique.

Associons à tout élément a du corps k la classe contenant la suite {a, a, . . . }. Nous obtenons une application de k dans $\bar{k}$ qui réalise un isomorphisme conservant la métrique du corps métrique k sur un sous-corps du corps $\bar{k}$. Nous ne distinguerons pas un élément de k de son image dans $\bar{k}$, i. e. nous considérerons que $k \subset \bar{k}$. Il est clair que k est partout dense dans $\bar{k}$. En effet, si a est une classe contenant la suite de Cauchy $\{x_n\}$, alors $\{x_n\} \to a$.

Il nous reste à démontrer que le corps $\bar{k}$ est complet. Soit α_n une suite de Cauchy d'éléments du corps $\bar{k}$. Puisque a, est limite d'une suite d'éléments du corps k, il existe un élément $x_n \in k$ tel que $\varphi(\alpha_n - x_n) < \frac{1}{n}$.

La suite $\{\alpha_n\}$ étant de Cauchy, la suite $\{x_n\}$ d'éléments du corps k l'est aussi. Soit α la classe de la suite $\{x_n\}$. On vérifie alors facilement que $\{\alpha_n\} \to \alpha$, ce qui termine la démonstration.

DÉMONSTRATION DU THÉORÈME 2. — Soient $\bar{k}$ et $\bar{k}_1$ deux corps complets contenant k comme sous-corps partout dense. Montrons qu'il existe une correspondance biunivoque entre les corps $\bar{k}$ et $\bar{k}_1$, en laissant le soin au lecteur de vérifier que cette correspondance est un isomorphisme métrique.

Soit a un élément du corps $\bar{k}$. Par hypothèse, il existe une suite $\{x_n\}$ d'éléments du corps k telle que $\{x_n\} \to \alpha$. Puisque la suite $\{x_n\}$ est convergente, c'est une suite de Cauchy et cette propriété est conservée si nous la considérons comme une suite d'éléments du corps $\bar{k}_1$. Ce corps étant complet, cette suite est convergente dans $\bar{k}_1$ vers une limite que nous désignerons par α_1. Il est facile de vérifier que si $\{y_n\}$ est une autre suite d'éléments de k convergente vers a dans $\bar{k}$ alors la limite de $\{y_n\}$ dans le corps $\bar{k}_1$ est encore le même élément a,. Ainsi, l'élément α_1 du corps $\bar{k}_1$ est défini sans ambiguïté par l'élément α du corps $\bar{k}$. La correspondance $\alpha \to \alpha_1$ est ainsi un isomorphisme.

2) Les métriques du corps des nombres rationnels

On se propose ici de montrer que les seules métriques possibles sur le corps Q des nombres rationnels sont la métrique usuelle et les métriques p-adiques (pour p entier premier quelconque).

La définition de la métrique p-adique φ_p sur le corps Q fait intervenir le choix d'un nombre réel p auquel on impose seulement les conditions $0 < \rho < 1$ (cf. égalités (1) et (18) du § 3). Ainsi, il existe une infinité de métriques associées au même nombre premier p, mais toutes ces métriques définissent la même notion de convergence sur Q et par suite les complétés pour toutes ces métriques coïncident et sont tous égaux au corps $\mathbf{Q}_p$ des nombres p-adiques.

Montrons que, de même, pour tout choix de α réel tel que $0 < a \leqslant 1$, la fonction

$$\varphi(x) = |x|^{\alpha} \qquad (2)$$

est une métrique du corps R. En effet, il est clair que φ satisfait aux conditions 1° et 3° de définition d'une métrique. Soit $|x| \geqslant |y|$, $x \neq 0$; alors

$$|x+y|^\alpha = |x|^\alpha \left|1+\frac{y}{x}\right|^\alpha \leqslant |x|^\alpha \left(1+\left|\frac{y}{x}\right|^\alpha\right)$$
$$\leqslant |x|^\alpha \left(1+\left|\frac{y}{x}\right|\right) \leqslant |x|^\alpha \left(1+\left|\frac{y}{x}\right|^\alpha\right) = |x|^\alpha + |y|^\alpha,$$

i. e. la condition 2° est satisfaite.

D'après (2), la convergence dans Q définie par cette métrique coïncide avec la convergence pour la valeur absolue et par suite les complétés pour toutes ces métriques sont le corps des nombres réels.

THÉORÈME 3 (théorème d'Ostrowski). — ***Les métriques du type (2) et les métriques p-adiques pour tout entier premier p sont les seules métriques non triviales du corps Q des nombres rationnels.***

DÉMONSTRATION. — Soit φ une métrique non triviale du corps des nombres rationnels. Deux cas sont possibles : ou bien il existe au moins un entier naturel $a > 1$ tel que $\varphi(a) > 1$ ou bien $\varphi(n) \leqslant 1$ pour tout entier naturel. Considérons tout d'abord le premier cas. Puisque

$$\varphi(n) = \varphi(1+1+\ldots+1) \leqslant \varphi(1)+\ldots+\varphi(1) = n \tag{3}$$

on peut poser

$$\varphi(a) = a^\alpha \tag{4}$$

où le nombre réel α est tel que $0 < \alpha \leqslant 1$.

Décomposons tout entier naturel N suivant les puissances de a :

$$N = x_0 + x_1 a + \ldots + x_{k-1} a^{k-1}$$

avec

$$0 \leqslant x_i \leqslant a-1 \quad (0 \leqslant i \leqslant k-1), \quad x_{k-1} \geqslant 1.$$

Par suite, on a pour N l'inégalité

$$a^{k-1} \leqslant N < a^k.$$

D'après les propriétés de la métrique et les formules (3) et (4) nous obtenons

$$\varphi(N) \leqslant \varphi(x_0) + \varphi(x_1)\varphi(a) + \ldots + \varphi(x_{k-1})\varphi(a)^{k-1}$$
$$\leqslant (a-1)(1+a^\alpha+\ldots+a^{(k-1)\alpha})$$
$$= (a-1)\frac{a^{k\alpha}-1}{a^\alpha-1} < (a-1)\frac{a^{k\alpha}}{a^\alpha-1} = \frac{(a-1)}{a^\alpha-1} a^\alpha \cdot a^{(k-1)\alpha}$$
$$\leqslant \frac{(a-1)a^\alpha}{a^\alpha-1} N^\alpha = CN^\alpha,$$

i. e.

$$\varphi(N) < CN^{\alpha},$$

la constante C étant indépendante. de N. Remplaçant N par N^m dans cette inégalité, nous obtenons, pour tout m,

$$\varphi(N)^m = \varphi(N^m) < CN^{m\alpha},$$

d'où

$$\varphi(N) < \sqrt[m]{C} \cdot N^{\alpha}.$$

Faisant tendre m vers l'infini, nous obtenons l'inégalité

$$\varphi(N) \leqslant N^{\alpha}. \tag{5}$$

Posons maintenant $N = a^k - b$, avec $0 < b \leqslant a^k - a^{k-1}$. D'après 2°, nous avons

$$\varphi(N) \geqslant \varphi(a^k) - \varphi(b) = a^{\alpha k} - \varphi(b).$$

D'après ce qu'on a vu,

$$\varphi(b) \leqslant b^{\alpha} \leqslant (a^k - a^{k-1})^{\alpha},$$

d'où

$$\varphi(N) \geqslant a^{\alpha k} - (a^k - a^{k-1})^{\alpha} = \left(1 - \left(1 - \frac{1}{a}\right)^{\alpha}\right) a^{\alpha k} = C_1 a^{\alpha k} > C_1 N^{\alpha},$$

où la constante C_1 est indépendante de N. Soit de nouveau m un entier naturel quelconque. En remplaçant N par N^m dans la dernière inégalité, nous obtenons

$$\varphi(N)^m = \varphi(N^m) > C_1 N^{\alpha m},$$

d'où

$$\varphi(N) > \sqrt[m]{C_1} \cdot N^{\alpha},$$

et par suite, pour $m \to \infty$, on a

$$\varphi(N) \geqslant N^{\alpha}. \tag{6}$$

La réunion de (5) et (6) nous montre que $\varphi(N) = N^{\alpha}$ pour tout entier naturel N. Soit maintenant $x = \pm \frac{N_1}{N_2}$ un nombre rationnel quelconque $\neq 0$ (N, et N_2 sont des entiers naturels;. Alors

$$\varphi(x) = \varphi\left(\frac{N_1}{N_2}\right) = \frac{\varphi(N_1)}{\varphi(N_2)} = \frac{N_1^{\alpha}}{N_2^{\alpha}} = |x|^{\alpha}.$$

Ainsi, nous avons démontré que si $\varphi(\alpha) > 1$ pour au moins un entier naturel a, alors la métrique φ est de la forme (2).

Passons maintenant à l'étude du cas

$$\varphi(n) \leqslant 1 \tag{7}$$

pour tout entier naturel n.

Si nous avions $\varphi(p) = 1$ pour tout nombre premier p, alors, d'après la propriété 3°, nous aurions aussi $\varphi(n) = 1$ pour tout entier naturel; cela contredit la non-trivialité de la métrique cp. Ainsi, il existe unp premier tel que $\varphi(p) < 1$. Supposons que pour un autre nombre premier q, $q \neq p$, on ait $\varphi(q) < 1$ et choisissons des entiers k et l tels qu'on ait les inégalités

$$\varphi(p)^k < \frac{1}{2}, \qquad \varphi(q)^l < \frac{1}{2}.$$

Puisque p^k et q^l sont premiers entre eux, il existe des entiers rationnels u et v tels que $up^k + vq^l = 1$. D'après (7), nous avons $\varphi(u) \leqslant 1$ et $\varphi(v) \leqslant 1$, d'où

$$1 = \varphi(1) = \varphi(up^k + vq^l) \leqslant \varphi(u)\varphi(p)^k + \varphi(v)\varphi(q)^l < \frac{1}{2} + \frac{1}{2},$$

La contradiction obtenue montre qu'il n'existe qu'un nombre premier p tel que

$$\varphi(p) = \rho < 1.$$

Puisque $\varphi(q) = 1$ pour tous les autres nombres premiers, il est clair que $\varphi(a) = 1$ pour tout entier a relativement premier avec p. Soit $x = p^m \frac{a}{b}$ un nombre rationnel non nul (a et b premiers à p). Alors

$$\varphi(x) = \varphi(p^m)\frac{\varphi(a)}{\varphi(b)} = \varphi(p)^m = \rho^m.$$

Ainsi, dans ce cas, la métrique φ coïncide avec la métrique p-adique (1).

Ceci termine la démonstration du théorème 3.

EXERCICES

1. Montrer que sur un corps fini, il existe une métrique et une seule (la métrique triviale).

2. Deux métriques φ et ψ sur un corps k sont dites *équivalentes* si elles définissent la même notion de convergence sur k, i. e. si les conditions $\varphi(x_n - x) \to 0$ et $\psi(x_n - x) \to 0$ sont équivalentes. Démontrer que φ et ψ sont équivalentes si et seulement si les conditions $\varphi(x) < 1$ et $\psi(x) < 1$ ($x \in k$) sont équivalentes.

3. Démontrer que si φ et ψ sont des métriques équivalentes d'un corps k, alors il existe un nombre réel δ tel que $\varphi(x) = (\psi(x))^\delta$ pour tout $x \in k$.

4. Une métrique φ sur un corps k est dite *non archimédienne* si elle vérifie la condition suivante, plus forte que la condition 2° de 1) :

2° $$\varphi(\alpha + \beta) \leqslant \max(\varphi(\alpha), \varphi(\beta))$$

(si cette condition n'est pas réalisée, la métrique φ est dite archimédienne). Montrer qu'une métrique φ est non archimédienne si et seulement si $\varphi(x) \leqslant 1$ pour tout entier naturel n (plus précisément, pour tout multiple naturel de l'élément unité du corps k).

5. Montrer que toute métrique d'un corps de caractéristique $p \neq 0$ est non archimédienne.

6. Soit k_0 un corps et $k = k_0(t)$ le corps des fractions rationnelles sur k_0. Tout élément $u \in k$, $u \neq 0$, peut s'écrire sous la forme

$$u = t^m \frac{f(t)}{g(t)} \quad (f(0) \neq 0,\ g(0) \neq 0)$$

où f et g sont des polynômes. Montrer que la fonction

$$\varphi(u) = \rho^m \quad (0 < \rho < 1), \qquad \varphi(0) = 0 \tag{8}$$

est une métrique sur le corps k.

7. Démontrer que le complété du corps $k = k_0(t)$ pour la métrique (8) est isomorphe au corps des séries formelles généralisées $k_0\{t\}$ formé par toutes les séries formelles du type

$$\sum_{n=m}^{\infty} a_n t^n \qquad (a_n \in k_0,\ m \in \mathbf{Z})$$

avec les opérations habituelles sur les séries.

§ 5. — CONGRUENCES ET NOMBRES ENTIERS p-ADIQUES

1) Congruences et équations dans l'anneau $\mathbf{Z}_p$

Au début du § 3, nous avons étudié la résolution de la congruence $x^2 \equiv 2 \pmod{7^n}$ pour $n = 1, 2, \ldots$ et cela nous a conduit à la notion de nombre entier p-adique. Cela suggère un important lien entre les nombres p-adiques et les congruences.

THÉORÈME 1. — *Soit $F(x_1, \ldots, x_n)$ un polynôme à coefficients entiers rationnels. Les congruences*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{1}$$

sont résolubles pour tout entier $k \geqslant 1$ si et seulement si l'équation

$$F(x_1, \ldots, x_n) = 0 \tag{2}$$

est résoluble dans l'anneau des nombres entiers p-adiques.

DÉMONSTRATION. — Supposons que l'équation (2) ait une solution $a_1, \ldots, \alpha_n$ dans les nombres entiers p-adiques. Pour tout k, il existe alors des nombres entiers rationnels $x_1^{(k)}, \ldots, x_n^{(k)}$, tels que

$$\alpha_1 \equiv x_1^{(k)} \pmod{p^k}, \ldots, \alpha_n \equiv x_n^{(k)} \pmod{p^k}. \tag{3}$$

Il en résulte que

$$F\left(x_1^{(k)}, \ldots, x_n^{(k)}\right) \equiv F(or_1, \ldots, \alpha_n) \equiv 0 \pmod{p^k},$$

i. e. $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$ est une solution de la congruence (1).

Supposons maintenant que la congruence (1) a une solution $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$ pour tout k. Extrayons de la suite des nombres entiers rationnels $\left\{ x_1^{(k)} \right\}$ une sous-suite p-adiquement convergente (théorème 6, § 3). Extrayons de nouveau une sous-suite convergente de la suite $\left\{ x_2^{(k_i)} \right\}$; en répétant n fois ce processus, nous obtenons une sous-suite $\{ l_1, l_2, \ldots \}$ de la suite des entiers telle que chacune des suites $\left\{ x_i^{(l_1)}, x_i^{(l_2)}, \ldots \right\}$, soit p-adiquement convergente. Posons

$$\lim_{n \to \infty} x_i^{(l_m)} = \alpha_i.$$

Montrons que $(\alpha_1, \ldots, \alpha_n)$ est une solution de la congruence (2). Puisque le polynôme $F(x_1, \ldots, x_n)$ est une fonction continue, alors

$$F(\alpha_1, \ldots, \alpha_n) = \lim_{m \to \infty} F\left(x_1^{(l_m)}, \ldots, x_n^{(l_m)}\right).$$

D'autre part, d'après la construction de la suite,

$$F\left(x_1^{(l_m)}, \ldots, x_n^{(l_m)}\right) \equiv 0 \pmod{p^{l_m}},$$

d'où

$$\lim_{m \to \infty} F\left(x_1^{(l_m)}, \ldots, x_n^{(l_m)}\right) = 0.$$

Ainsi $F(\alpha_1, \ldots, \alpha_n) = 0$ et le théorème 1 est démontré.

Considérons maintenant le cas où $F(x_1, \ldots, x_n)$ est une forme à coefficients entiers rationnels et supposons que l'équation $F(x_1, \ldots, x_n) = 0$ a une solution non nulle $(\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ dans les nombres entiers p-adiques. Posons $m = \min (v_p(\bar{\alpha}_i), \ldots, v_p(\bar{\alpha}_n))$. Alors les $\bar{\alpha}_i$ s'écrivent sous la forme

$$\bar{\alpha}_i = p^m \alpha_i \qquad (i = 1, \ldots, n)$$

tous les α_i étant entiers et l'un au moins d'entre eux n'étant pas divisible par p. Il est évident que $(\alpha_1, \ldots, \alpha_n)$ est encore une solution de l'équation $F(x_1, \ldots, x_n) = 0$. Les nombres $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$ satisfaisant aux condi-

tions (3) donnent, comme nous l'avons vu, une solution de la congruence (1) et l'un d'entre eux n'est pas divisible par p.

Supposons que, réciproquement, la congruence (1) pour F homogène a pour tout k une solution $(x_1^{(k)}, \ldots, x_n^{(k)})$ telle qu'au moins un des nombres $x_i^{(k)}$ ne soit pas divisible par p. Il est clair qu'il existe un indice $i = i_0$ tel que le nombre $x_{i_0}^{(m)}$ ne soit pas divisible par p pour une infinité de valeurs de m. Par suite, nous pouvons choisir la suite $\{l_1, l_2, \ldots\}$ de telle sorte qu'aucun des $x_{i_0}^{(l_m)}$ ne soit divisible par p. Mais alors, l'égalité $\alpha_{i_0} = \lim_{m\to\infty} x_{i_0}^{(l_m)}$ entraîne que α_{i_0} n'est pas divisible par p d'où $\alpha_{i_0} \neq 0$. On a donc démontré le théorème suivant.

THÉORÈME 2. — *Soit* $F(x_1, \ldots, x_n)$ *une forme à coefficients entiers rationnels. Pour que l'équation* $F(x_1, \ldots, x_n) = 0$ *ait une solution non triviale dans l'anneau* $\mathbf{Z}_p$, *il faut et il suffit que, pour tout entier m, la congruence*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}$$

ait une solution dont une au moins des composantes n'est pas divisible par p.

Il est évident qu'on peut aussi considérer dans les théorèmes 1 et 2 des polynômes à coefficients entiers p-adiques.

2) Sur la résolubilité de certaines congruences

Le théorème 1, démontré dans le point précédent, ramène la question de la résolubilité de l'équation (2) dans les nombres entiersp-adiques à la résolubilité de la suite infinie des congruences (1). La question de savoir s'il suffit d'examiner seulement un nombre fini de ces congruences est, dans le cas général, assez compliquée. Nous nous bornerons ici à examiner un cas particulier.

THÉORÈME 3. — *Soient* $F(x_1, \ldots, x_n)$ *un polynôme à coefficients entiers p-adiques et* $(\gamma_1, \ldots, \gamma_n)$ *des nombres entiers p-adiques tels que l'on ait, pour un certain i* $(1 \leqslant i \leqslant n)$:

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{2\delta+1}},$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{\delta}}$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p^{\delta+1}}$$

(δ étant un entier naturel). Alors, il existe des entiersp-adiques $\theta_1, \ldots, \theta_n$ tels que

$$F(\theta_1, \ldots . \theta_n) = 0$$

et

$$\theta_1 \equiv \gamma_1 \pmod{p^{\delta+1}}, \ldots, \theta_n \equiv y,, \pmod{p^{\delta+1}}.$$

DÉMONSTRATION. — Considérons le polynôme

$$f(x) = F(\gamma_1, \ldots, \gamma_{i-1}, x, \gamma_{i+1}, \ldots, \gamma_n).$$

Pour démontrer le théorème, il suffit d'établir l'existence d'un nombre entier p-adique α tel que f(u) = 0 et $\alpha \equiv \gamma_i \pmod{p^{\delta+1}}$ (si on trouve un tel a, alors on peut poser $\theta_j = \gamma_j$ pour $j \neq i$ et θ_i = a). Posant γ_i = y, construisons par récurrence une suite

$$\alpha_0, \alpha_1, \ldots . a,, \ldots \tag{3'}$$

de nombres p-adiques congrus à δ modulo $p^{\delta} + 1$ et tels que

$$f(\alpha_m) \equiv 0 \pmod{p^{2\delta+1+m}} \tag{4}$$

pour tout $m \geqslant 0$. Pour $m = 0$, on peut prendre α_0 = y; supposons que pour un certain $m \geqslant 1$ on ait construit des nombres $\alpha_0, \ldots, \alpha_{m-1}$ satisfaisant aux conditions ci-dessus et tels, en particulier, que $\alpha_{m-1} \equiv y \pmod{p^{\delta+1}}$ et $f(\alpha_{m-1}) \equiv 0 \pmod{p^{2\delta+m}}$. Ordonnons le polynôme f(x) suivant les puissances de $x - \alpha_{m-1}$:

$$f(x) = \beta_0 + \beta_1(x - \alpha_{m-1}) + \beta_2(x - \alpha_{m-1})^2 + \ldots \qquad (\beta_i \in \mathbf{Z}_p).$$

Par hypothèse de récurrence, $\beta_0 = f(\alpha_{m-1}) = p^{2\delta+m}A$, A étant un entier p-adique. De plus, puisque $\alpha_{m-1} \equiv y \pmod{p^{\delta+1}}$, alors $\beta_1 = f'(\alpha_{m-1}) = p^{\delta}B$ où le nombre $B \in \mathbf{Z}_p$ n'est pas divisible par p. Posant $x = \alpha_{m-1} + \xi p^{m+\delta}$, on a

$$f(\alpha_{m-1} + \xi p^{m+\delta}) = p^{2\delta+m}(A + B\xi) + \beta_2 p^{2\delta+2m}\xi^2 + \ldots$$

Posons maintenant $\xi = \xi_0 \in \mathbf{Z}_p$ tel que $A + B\xi_0 \equiv 0 \pmod{p}$ (puisque $B \not\equiv 0 \pmod{p}$, la congruence $A + B\xi \equiv 0 \pmod{p}$ est résoluble). Remarquant que $k\delta + km \geqslant 2\delta + 1 + m$ pour $k \geqslant 2$, nous obtenons

$$f(\alpha_{m-1} + \xi_0 p^{m+\delta}) \equiv 0 \pmod{p^{2\delta+1+m}}.$$

Nous pourrons alors poser a, $= \alpha_{m-1} + \xi_0 p^{m+\delta}$. Puisque $m + \delta \geqslant \delta + 1$, alors $a,,, \equiv y \pmod{p^{\delta+1}}$. Par construction, $v_p(\alpha_m - \alpha_{m-1}) \geqslant m + \delta$ et par suite la suite (3') trouvée est convergente; nous désignerons sa limite par a. Il est évident que $a \equiv y \pmod{p^{\delta+1}}$. Il résulte alors de (4) que $\lim_{m\to\infty} f(\alpha_m) = 0$; d'autre part, d'après la continuité du polynôme, $\lim_{m\to\infty} f(\alpha_m) = f(\alpha)$, d'où

$$f(u) = 0.$$

COROLLAIRE. — *Soient* $F(x_1, \ldots, x_n)$ *un polynôme à coefficients entiers p-adiques et* $\gamma_1, \ldots, \gamma_n$ *des entiersp-adiques tels que, pour un certain i(* $1 \leqslant i \leqslant n$*) on ait*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p}$$

$$F'_{x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p};$$

alors il existe des entiers p-adiques $\theta_1, \ldots, \theta_n$ *tels que*

$$F(\theta_1, \ldots, \theta_n) = 0$$

et

$$\theta_1 \equiv \gamma_1 \pmod{p}, \ldots, \theta_n \equiv y_n \pmod{p}.$$

Ainsi, toute solution $c_1, \ldots, c_n$ de la congruence $F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ peut être prolongée en une solution de l'équation $F(x_1, \ldots, x_n) = 0$ dans l'anneau $\mathbf{Z}_p$, sauf, peut-être, celles pour lesquelles on a simultanément

$$\left.\begin{aligned} F'_{x_1}(c_1, \ldots, c_n) &\equiv 0 \pmod{p} \\ &\cdots \\ F'_{x_n}(c_1, \ldots, c_n) &\equiv 0 \pmod{p} \end{aligned}\right\}$$

Ce dernier résultat a une importante application à la question dont nous avons parle au début du § 2. Nous avons vu que la résolubilité de la congruence

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{m}$$

pour tout entier m est liée à la satisfaction d'une infinité de conditions. Dans le cas d'un module premier, les théorèmes A et B, formulés au début du § 2-1) nous permettent de ramener ces conditions à un nombre fini de vérifications. Nous pouvons énoncer un résultat pour les entiers quelconques; comme nous l'avons déjà remarqué, il suffit de considérer des modules qui sont des puissances de nombres premiers et pour des modules de la forme p^k $(k = 1, 2, \ldots)$, la résolubilité des congruences (1) est équivalente, d'après le théorème 1 à la résolubilité de l'équation F = 0 dans l'anneau $\mathbf{Z}_p$ des nombres entiers p-adiques.

En s'appuyant sur les théorèmes A et B formulés (mais non démontrés) dans le § 2-1) et sur le théorème 3 de ce paragraphe, nous pouvons établir le résultat suivant.

THÉORÈME C. -Si $F(x_1, \ldots, x_p)$ *est un polynôme absolument irréductible à coefficients entiers rationnels, alors l'équation* $F(x_1, \ldots, x_n) = 0$ *est résoluble dans l'anneau* $\mathbf{Z}_p$ *des nombres entiers p-adiques pour tout nombre premier p plus grand qu'un certain nombre ne dépendant que du polynôme* F.

Par suite, pour tous les nombres premiers p, sauf un nombre fini, la congruence

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{5}$$

est résoluble pour tous les entiers k.

Le théorème C réduit ainsi la question de la résolubilité de toutes les congruences (5) à la question de la résolubilité de l'équation F = 0 dans l'anneau $\mathbf{Z}_p$ pour seulement un nombre fini d'entiers p. Nous n'étudierons pas ici la résolubilité de l'équation F = 0 dans l'anneau $\mathbf{Z}_p$ (cela sera fait, dans le cas d'un polynôme de deuxième degré au § 6).

Donnons une idée de la démonstration du théorème 6. En utilisant la valeur du nombre de solutions de la congruence (2), § 2, exprimée par le théorème B, montrons que le nombre de solutions de cette congruence pour p assez grand est supérieur au nombre de solutions du système de congruences

$$\left.\begin{aligned} F(x_1, \ldots, x_n) &\equiv 0 \pmod{p} \\ F'_{x_n}(x_1, \ldots, x_n) &\equiv 0 \pmod{p} \end{aligned}\right\} \tag{6}$$

Il nous faut pour cela obtenir une nouvelle estimation du nombre de solutions d'une congruence.

LEMME. — ***Si aucun des coefficients du polynôme*** $F(x_1, \ldots, x_n)$ ***n'est divisible par p, alors le nombre N(p) de solutions de la congruence***

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p} \tag{7}$$

satisfait à l'inégalité

$$N(p) \leqslant Lp^{n-1}, \tag{8}$$

dans lequel la constante L ***est égale au degré total du polynôme*** F.

Démontrons le lemme par récurrence sur n. Pour $n = 1$, il résulte du fait que le nombre de racines, dans le corps $\mathbf{F}_p$, d'un polynôme non nul ne peut pas dépasser son degré.

Si $n > 1$, nous considérerons $F(x_1, \ldots, x_n)$ comme un polynôme de $x_1, \ldots, x_{n-1}$ dont les coefficients sont des polynômes de x_n. Désignons par $f(x_n)$ le plus grand commun diviseur de ces coefficients modulo p. Alors

$$F(x_1, \ldots, x_n) \equiv f(x_n) F_1(x_1, \ldots, x_n) \pmod{p}$$

et par suite le polynôme $F_1(x_1, \ldots, x_{n-1}, a)$ n'est congru identiquement à zéro modulo p pour aucune valeur de a. Soient l et L_1 les degrés des polynômes f et F_1. Il est clair que f et F_1 peuvent être choisis tels que $l + L_1 \leqslant L$. Évaluons maintenant le nombre de solutions $(c_1, \ldots, c_n)$ de la congruence (7)

et portons notre attention sur la valeur de x_n dans cette solution. Considérons tout d'abord les solutions telles que

$$f(c_n) \equiv 0 \pmod{p}. \tag{9}$$

Si la congruence (9) est satisfaite, la congruence (7) est automatiquement satisfaite pour tout $c_1, \ldots, c_{n-1}$. Puisque le nombre de valeurs de c_n modulo p satisfaisant à la condition (9) ne dépasse pas L, le nombre de valeurs de la congruence (7) pour lesquelles on a (9) ne dépasse pas Lp^{n-1}. Considérons maintenant les solutions $(c_1, \ldots, c_n)$ telles que $f(c_n) \not\equiv 0 \pmod{p}$. Il est clair que toutes ces solutions satisfont à la congruence $F_1(x_1, \ldots, x_n) \equiv 0 \pmod{p}$. Puisque $F_1(x_1, \ldots, x_{n-1}, c,)$ n'est pas identiquement congru à 0 modulo p, alors, par hypothèse de récurrence, le nombre $N(p, c_n)$ de solutions de la congruence $F(x_1, \ldots, x_{n-1}, c_n) \equiv 0 \pmod{p}$ satisfait à l'inégalité

$$N(p, c_n) \leqslant L_1 p^{n-2}.$$

Puisque c_n peut prendre au plus p valeurs, le nombre des solutions considérées ne dépasse pas $L_1 p^{n-1}$. Ainsi, le nombre de toutes les solutions de la congruence (7) ne dépasse pas $lp^{n-1} + L_1 p^{n-1} \leqslant Lp^{n-1}$, c. q. f. d.

DÉMONSTRATION DU THÉORÈME C. — Nous pouvons supposer que le polynôme F dépend effectivement de la variable x_n. Considérons F comme un polynôme de x_n dont les coefficients sont des polynômes de $x_1, \ldots, x_{n-1}$. L'irréductibilité absolue de F entraîne alors que le discriminant $D_{x_n}(x_1, \ldots, x_{n-1})$ du polynôme F considéré comme polynôme de x_n n'est pas un polynôme de $x_1, \ldots, x_{n-1}$ identiquement nul, car sinon F serait divisible par le carré d'un certain polynôme. Considérons les nombres premiers p qui ne divisent pas tous les coefficients de $D_{x_n}(x_1, \ldots, x_{n-1})$ et évaluons dans ce cas, le nombre $N_1(p)$ de solutions de système des congruences (6). Si $(c_1, \ldots, c_n)$ est une solution du système (6), alors c_n est une racine commune modulo p des polynômes

$$F(c_1, \ldots, c_{n-1}, x_n) \quad \text{et} \quad F'_{x_n}(c_1, \ldots, c_{n-1}, x_n),$$

d'où

$$D_{x_n}(c_1, \ldots, c_{n-1}) \equiv 0 \pmod{p}.$$

D'après le lemme, le nombre de systèmes $(c_1, \ldots, c_{n-1})$ qui satisfont à cette congruence ne dépasse pas $K_1 p^{n-2}$, K_1 étant une constante dépendant seulement du polynôme F. Pour $c_1, \ldots, c_{n-1}$ donnés la valeur c_n est définie par la congruence

$$F(c_1, \ldots, c_{n-1}, x_n) \equiv 0 \pmod{p}$$

et par suite le nombre de ces valeurs ne dépasse pas le degré m du polynôme F par rapport à la variable x_n. Ainsi le nombre $N_1(p)$ de solutions du système (6) ne dépasse pas Kp^{n-2}, avec $K = mK_1$. Démontrons maintenant que le nombre N(p) de solutions de la congruence (7), pour p assez grand, est supérieur au nombre $N_1(p)$ de solutions du système (6). En effet, il résulte du théorème B que

$$N(p) > p^{n-1} - Cp^{n-1-\frac{1}{2}},$$

et nous venons de démontrer que $N_1(p) < Kp^{n-2}$. Par suite,

$$N(p) - N_1(p) > p^{n-1} - Cp^{n-1-\frac{1}{2}} - Kp^{n-2} = p^{n-2}(p - Cpf - K),$$

et cela entraîne $N(p) > N_1(p)$ pour p assez grand. Ainsi, pourp assez grand, la congruence $F \equiv 0 \pmod p$ a une solution $\gamma_1, \ldots, \gamma_n$ telle que

$$\frac{\partial F}{\partial x_n}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod p.$$

D'après le corollaire du théorème 3, il en résulte que l'équation F = 0 est résoluble dans l'anneau $\mathbf{Z}_p$ pour tout p assez grand.

EXERCICES

1. Démontrer que si m et p sont premiers entre eux, toute unité p-adique ε telle que $c \equiv 1 \pmod p$ est une puissance $m^{\text{ième}}$ dans $\mathbf{Q}_p$

2. Soit $m = p^\delta m_0$, $(m_0, p) = 1$ et soit ε une unité p-adique telle que $\varepsilon \equiv 1 \pmod{p^{\delta+1}}$. Montrer que ε est une puissance $m^{\text{ième}}$ dans $\mathbf{Q}_p$.

3. Démontrer que, pourp $\neq 2$, la résolubilité de la congruence $\alpha x^p \equiv \beta \pmod{p^2}$ par des entiers p-adiques α et β non divisibles par p entraîne la résolubilité de l'équation $\alpha x^p = \beta$ dans le corps $\mathbf{Q}_p$

4. Soit la forme $G = \varepsilon_1 x_1^p + \ldots + \varepsilon_n x_n^p$, dont les coefficients sont des unités p-adiques $p \neq 2$). Montrer que si la congruence $G \equiv 0 \pmod{p^2}$ a une solution telle que la valeur de l'une au moins des inconnues ne soit pas divisible par p, alors l'équation G = 0 a une solution non nulle dans le corps $\mathbf{Q}_p$.

5. Considérons une forme $G = \alpha_1 x_1^p + \ldots + \alpha_n x_n^p$ dont les coefficients sont des nombres entiers p-adiques non divisibles par p^p.

Démontrer que l'équation G = 0 a une solution non nulle dans le corps $\mathbf{Q}_p$ si la congruence $G \equiv 0 \pmod{p^{p+2}}$ a une solution telle que toutes les valeurs des inconnues ne soient pas divisibles par p.

(Dans le cas $p \neq 2$, il suffit que la congruence $G \equiv 0 \pmod{p^{p+1}}$ soit résoluble).

6. Considérons une forme quadratique $F = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ dont les coefficients sont des entiers p-adiques ($p \neq 2$) non divisibles par p^2. Démontrer que si la congruence $F \equiv 0 \pmod{p^2}$ a une solution telle que toutes les valeurs des inconnues ne soient pas divisibles par p, alors l'équation F = 0 a une solution, non nulle dans $\mathbf{Q}_p$

7. Soit la forme $F = \alpha_1 x_1^m + \ldots + \alpha_n x_n^m$, où les α_i sont des entiers p-adiques non nuls; posons $r = v_p(m)$, $s = \max(v_p(\alpha_1), \ldots, v_p(\alpha_n))$ et $N = 2(r+s)+1$. Montrer que l'équation $F = 0$ a une solution non nulle dans le corps $\mathbf{Q}_p$ si et seulement si la congruence $F \equiv 0 \pmod{p^N}$ a une solution telle que la valeur de l'une au moins des inconnues ne soit pas divisible par p.

8. Montrer que la forme $3x^3 + 4y^3 + 5z^3$ représente zéro dans le corps $\mathbf{Q}_p$ pour tout p (cf. exercice 13 du § 2).

9. Soit $F(x_1, \ldots, x_n)$ un polynôme à coefficients entiers p-adiques et désignons par c_m le nombre de solutions de la congruence $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}$. La série $\varphi(t) = \sum_{m=0}^{\infty} c_m t^m$ est appelée la série de Poincaré du polynôme F et on conjecture que sa somme est une fonction rationnelle de t. Trouver la série de Poincaré du polynôme $F = \varepsilon_1 x_1^2 + \ldots + \varepsilon_n x_n^2$ où les ε_i sont des unités p-adiques et vérifier que la fonction $\varphi(t)$ est rationnelle.

10. Trouver la série de Poincaré d'un polynôme $F(x_1, \ldots, x_n)$ à coefficients entiers qui possède la propriété suivante : pour toute solution de la congruence $F \equiv 0 \pmod{p}$, il existe un certain indice i ($i = 1, 2, \ldots, n$) tel que $\frac{\partial F}{\partial x_i} \not\equiv 0 \pmod{p}$.

11. Déterminer la série de Poincaré du polynôme $F(x, y) = x^2 - y^3$.

§ 6. — FORMES QUADRATIQUES A COEFFICIENTS p-ADIQUES

Dans ce paragraphe et le suivant, nous appliquerons la théorie des nombres p-adiques à la représentation des nombres rationnels et p-adiques par des formes quadratiques. Nous aurons besoin des résultats algébriques sur les formes quadratiques exposés dans le § 1 de l'appendice.

1) Les carrés dans le corps des nombres p-adiques

Pour étudier les formes quadratiques sur un corps, il est important de savoir quels éléments du corps sont des carrés. C'est pourquoi nous commencerons par l'étude des carrés dans le corps $\mathbf{Q}_p$ des nombres p-adiques.

Nous savons (théorème 4, § 3) que tout nombre p-adique $a \neq 0$ s'écrit de manière unique $a = p^m \varepsilon$, où ε est une unité p-adique (i. e. une unité dans l'anneau $\mathbf{Z}_p$ des entiers p-adiques). Si a est le carré d'un nombre p-adique $y = p^k \varepsilon_0$, alors $m = 2k$ et $\varepsilon = \varepsilon_0^2$. Par suite, il est nécessaire de connaître quelles sont les unités de $\mathbf{Z}_p$ qui sont des carrés.

THÉORÈME 1. — *Soit $p \neq 2$. Pour qu'une unité p-adique*

$$\varepsilon = c_0 + c_1 p + c_2 p^2 + \ldots \qquad (0 \leqslant c_i < p,\ c_0 \neq 0) \tag{1}$$

soit un carré, il faut et il suffit que le nombre c_0 soit un résidu quadratique modulo p.

DÉMONSTRATION. — Si $\varepsilon = \eta^2$ et $\eta \equiv b \pmod p$ (*b* entier rationnel), alors $c_0 \equiv b^2 \pmod p$. Réciproquement, si $c_0 \equiv b^2 \pmod p$, alors, considérant le polynôme $F(x) = x^2 - E$, nous obtenons : $F(b) \equiv 0 \pmod p$ et

$$F'(b) = 2b \not\equiv 0 \pmod p.$$

D'après le corollaire du théorème 3 du § 5, il existe $\eta \in \mathbf{Z}_p$ tel que $F(\eta) = 0$ et $\eta \equiv b \pmod p$. Ainsi $\varepsilon = \eta^2$ et le théorème est démontré.

COROLLAIRE 1. — ***Pour $p \neq 2$, toute unité p-adique congrue à 1 mod p est un carré dans $\mathbf{Q}_p$***

COROLLAIRE 2. — ***Pour $p \neq 2$, l'indice $(\mathbf{Q}_p^* : \mathbf{Q}_p^{*2})$ du sous-groupe $\mathbf{Q}_p^{*2}$ des carrés dans le groupe multiplicatif du corps des nombres p-adiques est égal à 4.***

En effet, si une unité ε n'est pas un carré, alors le rapport de deux des nombres $1, \varepsilon, p, p\varepsilon$ n'est jamais un carré dans le corps $\mathbf{Q}_p$. De plus, tout nombre p-adique différent de 0 est représentable comme produit d'un des nombres $1, \varepsilon, p, p\varepsilon$ par un carré.

Pour $p \neq 2$, nous poserons, pour toute unité (1),

$$\left(\frac{\varepsilon}{p}\right) = \begin{cases} +1 & \text{si } \varepsilon \text{ est un carré dans } \mathbf{R}_p \\ -1 & \text{sinon.} \end{cases}$$

D'après le théorème 1, nous avons

$$\left(\frac{\varepsilon}{p}\right) = \left(\frac{c_0}{p}\right),$$

où $\left(\frac{c_0}{p}\right)$ est le symbole de Legendre. Si ε est un entier rationnel premier avec p, alors il est clair que le symbole $\left(\frac{\varepsilon}{p}\right)$ introduit ici coïncide avec le symbole de Legendre. Il est facile d'ailleurs de voir que, pour des unités p-adiques ε et η, on a

$$\left(\frac{\varepsilon\eta}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{\eta}{p}\right).$$

Revenons sur le cas $p = 2$.

THÉORÈME 2. — ***Pour qu'une unité 2-adique ε soit un carré (dans le corps $\mathbf{Q}_2$), il faut et il suffit que $\varepsilon \equiv 1 \pmod 8$.***

DÉMONSTRATION. — La nécessité résulte du fait que le carré d'un nombre impair est toujours congru à 1 modulo 8. Pour démontrer la suffisance de cette condition, considérons le polynôme $F(x) = x^2 - \varepsilon$ et appliquons-lui le

corollaire du théorème 3, § 5 pour $\delta = 1$ et $y = 1$. Puisque $F(1) \equiv 0 \pmod 8$, $F'(1) = 2 \not\equiv 0 \pmod 4$, alors, d'après ce théorème, il existe $\eta \equiv 1 \pmod 4$ tel que $F(\eta) = 0$ i. e. $\varepsilon = \eta^2$.

COROLLAIRE. — *L'indice* $(\mathbf{Q}_2^* : \mathbf{Q}_2^{*2})$ *du sous-groupe des carrés dans le groupe multiplicatif du corps des nombres 2-adiques est égal à 8.*

En effet, d'après le théorème 2, le système des résidus 1, 3, 5, 7 modulo 8 est un système de représentants des classes résiduelles du quotient du groupe des unités 2-adiques par le sous-groupe de ses carrés. Ajoutant à ces nombres les produits 2.1, 2.3, 2.5, 2.7, nous obtenons un système complet de représentants des classes du groupe quotient du groupe $\mathbf{Q}_2^*$ par le sous-groupe $\mathbf{Q}_2^{*2}$.

2) Représentation de zéro par des formes quadratiques p-adiques

Comme dans tout corps, une forme quadratique non singulière sur le corps $\mathbf{Q}_p$ peut s'écrire, par une transformation linéaire de la variable, sous la forme

$$\alpha_1 x_1^2 + \ldots + \alpha_n x_n^2 \qquad (\alpha_i \neq 0)$$

(cf. appendice § l-l)). Si $\alpha_i = p^{2k_i}\varepsilon_i$ ou $\alpha_i = p^{2k_i+1}\varepsilon_i$ (ε_i unité dans $\mathbf{Z}_p$), alors, par la transformation $y_i = p^{k_i}x_i$, on se ramène à une forme dont tous les coefficients sont des entiers p-adiques divisibles au plus une seule fois par p. Ainsi toute forme quadratique non singulière sur $\mathbf{Q}_p$ est équivalente à une forme du type

$$F = F_0 + pF_1 = \varepsilon_1 x_1^2 + \ldots + \varepsilon_r x_r^2 + p(\varepsilon_{r+1}x_{r+1}^2 + \ldots + \varepsilon_n x_n^2), \quad (2)$$

où les ε_i sont des unités p-adiques.

Dans la recherche des représentations de zéro, nous pouvons supposer $r \geqslant n - r$. En effet, il est clair que la forme pF est équivalente à la forme $F_1 + pF_0$. Puisque F et pF représentent simultanément zéro ou pas, à la place de la forme $F_0 + pF_1$, nous pouvons considérer la forme $F_1 + pF_0$.

Considérons d'abord le cas $p \neq 2$.

THÉORÈME 3. — *Soit* $p \neq 2$ *et* $0 < r < n$. *La forme (2) représente zéro dans le corps* $\mathbf{Q}_p$ *si et seulement si une au moins des formes* F_0 *ou* F_1 *représente zéro.*

DÉMONSTRATION. — Supposons que la forme (2) représente zéro :

$$\varepsilon_1\xi_1^2 + \ldots + \varepsilon_r\xi_r^2 + p(\varepsilon_{r+1}\xi_{r+1}^2 + \ldots + \varepsilon_n\xi_n^2) = 0. \quad (3)$$

Il est clair que nous pouvons supposer que tous les ξ_i sont entiers et que l'un au moins d'entre eux n'est pas divisible par p. Si $\xi_1 \not\equiv 0 \pmod{p}$, alors, passant à la congruence modulo p dans (3), on a :

$$F_0(\xi_1, \ldots, \xi_r) \equiv 0 \pmod{p} ;$$

$$\frac{\partial F_0}{\partial x_1}(\xi_1, \ldots, \xi_r) = 2\varepsilon_1\xi_1 \not\equiv 0 \pmod{p}.$$

D'après le corollaire du théorème 3 § 5, la forme F_0 représente zéro. Supposons maintenant que toutes les valeurs $\xi_1, \ldots, \xi_r$ sont divisibles par p, d'où $\varepsilon_1\xi_1^2 + \ldots + \varepsilon_r\xi_r^2 \equiv 0 \pmod{p^2}$. Passons à la congruence modulo p^2 dans (3). Simplifiant cette congruence par p, nous obtenons

$$F_1(\xi_{r+1}, \ldots, \xi_n) \equiv 0 \pmod{p}$$

où l'un au moins des $\xi_{r+1}, \ldots, \xi_n$ n'est pas divisible par p. En appliquant à nouveau le corollaire du théorème 3 du § 5, nous en concluons que, dans ce cas, la forme F_1 représente zéro. Puisque la suffisance de la condition est évidente, la démonstration du théorème 3 est terminée.

Nous avons incidemment obtenu le résultat suivant.

COROLLAIRE 1. — *Si $\varepsilon_1, \ldots, \varepsilon_r$ sont des unités p-adiques, alors, pour $p \neq 2$, la forme $f = \varepsilon_1x_1^2 + \ldots + \varepsilon_rx_r^2$ représente zéro dans $\mathbf{Q}_p$ si et seulement si la congruence $f(x_1, \ldots, x_r) \equiv 0 \pmod{p}$ a une solution non triviale dans $\mathbf{Z}_p$*

COROLLAIRE 2. — *Sous les mêmes hypothèses, si $r \geqslant 3$, alors la forme $f(x_1, \ldots, x_r)$ représente toujours zéro dans $\mathbf{Z}_p$*

En effet, d'après le théorème 5, § 1, la congruence $f(x_1, \ldots, x_r) \equiv 0 \pmod{p}$ a une solution non triviale.

Dans la démonstration du théorème 3, nous n'avons pas complètement utilisé l'égalité (3) : nous avons seulement eu besoin des congruences $F \equiv 0 \pmod{p}$ et $F \equiv 0 \pmod{p^2}$. Ainsi, il résulte de la résolubilité de la deuxième de ces congruences que l'une des formes F_0 ou F_1 et par suite F, représente zéro. Nous avons donc

COROLLAIRE 3. — *Pour $p \neq 2$, la forme (2) représente zéro si et seulement si la congruence $F \equiv 0 \pmod{p^2}$ a une solution telle que la valeur d'une au moins des inconnues ne soit pas divisible par p.*

Passons maintenant à l'étude des formes quadratiques sur le corps des nombres 2-adiques. Dans ce cas, le théorème 3 et tous ses corollaires sont faux. Par exemple, pour la forme $f = x_1^2 + x_2^2 + x_3^2 + x_4^2$, l'équation $f = 0$ n'a pas de solution non triviale dans $\mathbf{Q}_2$ (puisque déjà la congruence $f \equiv 0 \pmod{8}$ n'a pas de solution dont l'une des inconnues soit impaire). Pourtant, la forme $f + 2x_5^2$ représente zéro dans $\mathbf{Q}_2$ (théorème 5).

THÉORÈME 4. — ***Dans le corps des nombres 2-adiques, la forme (2)*** (avec ***p = 2) représente zéro si et seulement si la congruence*** $F \equiv 0 \pmod{16}$ ***admet une solution dont l'une des inconnues est impaire.***

DÉMONSTRATION. — Soit $F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod{16}$, l'un au moins des nombres entiers p-adiques ξ n'étant pas divisible par 2. Supposons tout d'abord que $\xi_i \not\equiv 0 \pmod 2$ pour au moins un $i \leqslant r$; soit par exemple $\xi_1 \not\equiv 0 \pmod 2$. Puisque $F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod 8$ et $\frac{\partial F}{\partial x_1}(\xi_1, \ldots, \xi_n) \not\equiv 0 \pmod 4$, alors, d'après le thtorème 3 § 5 (avec $\delta = 1$) la forme F représente zéro. Supposons maintenant que $\xi_1, \ldots, \xi_r$ sont divisibles par 2, i. e. $\xi_i = 2\eta^i$ $(1 \leqslant i \leqslant r)$, les η_i étant des entiers 2-adiques. Simplifiant par 2 la congruence

$$4\sum_{i=1}^{r} \varepsilon_i \eta_i^2 + 2\sum_{i=r+1}^{n} \varepsilon_i \xi_i^2 \equiv 0 \pmod{16},$$

nous obtenons

$$\sum_{i=r+1}^{n} \varepsilon_i \xi_i^2 + 2\sum_{i=1}^{r} \varepsilon_i \eta_i^2 \equiv 0 \pmod 8,$$

l'un des $\xi_{r+1}, \ldots, \xi_n$ n'étant pas divisible par 2. Comme ci-dessus, cette congruence entraîne que la forme $F_1 + 2F_0$ représente zéro. Mais la forme 2F qui lui est Cquivalente représente alors aussi zéro, d'ou la suffisance de la condition. La réciproque est évidente.

Dans la démonstration du théorème 4, nous avons aussi obtenu le résultat suivant.

COROLLAIRE. — ***Si pour la forme (2) (avec p = 2), la congruence*** $F \equiv 0 \pmod 8$ ***a une solution dont l'une au moins des inconnues*** $x_1, \ldots, x_r$ ***est impaire, alors cette forme représente zéro dans le corps*** $\mathbf{Q}_2$.

THÉORÈME 5. — ***Dans le corps*** $\mathbf{Q}_p$ ***des nombres p-adiques, toute forme quadratique non singulière de cinq ou plus de cinq variables représente toujours zéro.***

DÉMONSTRATION. — On peut supposer que la forme donnée est du type (2) avec $r \geqslant n - r$. Puisque $n \geqslant 5$, alors $r \geqslant 3$. Supposons $p \neq 2$. Dans ce cas, d'après le corollaire 2 du théorème 3, la forme F_0 représente zéro, ce qui entraîne que la forme F représente zéro.

Soit maintenant $p = 2$. Si $n - r > 0$, considérons la forme « partielle »

$$f = \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 + 2\varepsilon_n x_n^2.$$

Une telle forme représente toujours zéro dans $\mathbf{Q}_2$. En effet, puisque $\varepsilon_1 + \varepsilon_2 = 2\alpha$ (α entier 2-adique), alors

$$\varepsilon_1 + \varepsilon_2 + 2\varepsilon_n \alpha^2 \equiv 2\alpha + 2\alpha^2 = 2\alpha(1 + \alpha) \equiv 0 \pmod 4,$$

i. e. $\varepsilon_1 + \varepsilon_2 + 2\varepsilon_n\alpha^2 = 4\beta$, β entier 2-adique. Posant $x_1 = x_2 = 1$, $x_3 = 2\beta$, $x_n = a$, nous avons

$$\varepsilon_1 . 1^2 + \varepsilon_2 . 1^2 + \varepsilon_3(2\beta)^2 + 2\varepsilon_n\alpha^n \equiv 4\beta + 4\beta^2 \equiv 0 \pmod 8.$$

D'après le corollaire du théorème 4, la formefreprésente zéro; mais alors F représente aussi zéro. Dans le cas où n = Y, on prend pour forme « partielle »

$$f = \varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 + \varepsilon_4 x_4^2 + \varepsilon_5 x_5^2.$$

Si $\varepsilon_1 + \varepsilon_2 \equiv \varepsilon_3 + \varepsilon_1 \equiv 2 \pmod 4$, posons $x_1 = x_2 = x_3 = x_4 = 1$ et si par exemple $\varepsilon_1 + \varepsilon_2 \equiv 0 \pmod 4$ posons $x_1 = x_2 = 1$, $x_3 = x_4 = 0$. Dans les deux cas

$$\varepsilon_1 x_1^2 + \varepsilon_2 x_2^2 + \varepsilon_3 x_3^2 + \varepsilon_4 x_4^2 = 4\gamma,$$

y entier 2-adique. Posant $x_5 = 2\gamma$, nous obtenons

$$f \equiv 4\gamma + 4\gamma^2 \equiv 0 \pmod 8.$$

Le corollaire du théorème 4 montre que, dans ce cas, le théorème est démontré.

D'après le théorème 6, § 1 de l'appendice, le théorème 5 entraîne ce qui suit.

COROLLAIRE 1. — *Dans le corps $\mathbf{Q}_p$, toute forme quadratique non singulière de quatre ou plus de quatre variables représente tous les nombres p-adiques.*

COROLLAIRE 2. — *Soit $F(x_1, \ldots . x_n)$ une forme quadratique non singulière à coefficients entiers rationnels. Si $n \geqslant 5$, pour tout entier m la congruence $F(x_1, \ldots . x_n) \equiv 0 \pmod m$ a une solution non triviale.*

En effet, puisque la forme F représente zéro dans $\mathbf{Q}_p$, pour tout entier $s \geqslant 1$, la congruence $F \equiv 0 \pmod{p^s}$ a une solution pour laquelle une au moins des inconnues n'est pas divisible par p.

3) Formes binaires

Les formes quadratiques binaires constituent un important exemple de la théorie générale des formes quadratiques. Nous considérerons ici le problème de la représentation des nombres du corps $\mathbf{Q}_p$ par une forme quadratique binaire du type

$$x^2 - \alpha y^2, \qquad \alpha \neq 0, \qquad \alpha \in \mathbf{Q}_p \tag{4}$$

(Il est évident que le cas général d'une forme binaire quelconque s'y réduit par transformation des variables et multiplication de la forme par un certain nombre p-adique).

Nous désignerons par H_α l'ensemble de tous les nombres p-adiques différents de zéro représentables par la forme (4). Cet ensemble est toujours un groupe pour la multiplication. En effet, si $\beta = x^2 - ay^2$, $\beta_1 = x_1^2 - ay_1^2$, alors, comme le montre un calcul évident,

$$\beta\beta_1 = (xx_1 + \alpha yy_1)^2 - \alpha(xy_1 + yx_1)^2,$$

$$\beta^{-1} = \left(\frac{x}{\beta}\right)^2 - \alpha\left(\frac{y}{\beta}\right)^2.$$

Donnons une autre démonstration de ce fait, basée sur l'étude de l'extension quadratique $\mathbf{Q}_p(\sqrt{\alpha})$ du corps $\mathbf{Q}_p$ (à condition que a ne soit pas un carré dans $\mathbf{Q}_p$).

L'égalité $\beta = x^2 - ay^2$ est équivalente au fait que β est la norme du nombre $\xi = x + y\sqrt{\alpha}$ dans $\mathbf{Q}_p(\sqrt{\alpha})$. Mais si $\beta = N(\xi)$ et $\beta_1 = N(\xi_1)$, alors

$$\beta\beta_1 = N(\xi_1\xi) \qquad \text{et} \qquad \beta^{-1} = N(\xi^{-1}).$$

Si a est un carré dans $\mathbf{Q}_p$, la forme (4) représente zéro et par suite tous les nombres de $\mathbf{Q}_p$. Par suite, H_α coïncide avec tout le groupe multiplicatif du corps $\mathbf{Q}_p$.

Puisque la forme (4) représente tous les carrés du corps $\mathbf{Q}_p$ (pour y = 0), alors $\mathbf{Q}_p^{*2} \subset H$,. Mais, d'après les corollaires des théorèmes 1 et 2, l'indice $(\mathbf{Q}_p^* : \mathbf{Q}_p^{*2})$ est fini et par suite H_α a un indice fini dans $\mathbf{Q}_p^*$.

THÉORÈME 6. — *Si le nombre* $a \in \mathbf{Q}_p^*$ *n'est pas un carré, alors* $(\mathbf{Q}_p^* : H_\alpha) = 2$.

DÉMONSTRATION. — Remarquons d'abord que la forme (4) représente un nombre p-adique β si et seulement si la forme

$$\alpha x^2 + \beta y^2 - z^2 \tag{5}$$

représente zéro (théorème 6, § 1 de l'appendice). De plus, la condition pour que la forme (5) représente zéro ne change pas si on multiplie a et β par des carrés; nous pouvons donc supposer que a et β sont des éléments fixés dans chaque classe résiduelle du quotient du groupe $\mathbf{Q}_p^*$ par le groupe $\mathbf{Q}_p^{*2}$.

Considérons d'abord le cas $p \neq 2$ et montrons que $H_\alpha \neq \mathbf{Q}_p^{*2}$. C'est évident si $-a$ n'est pas un carré (puisque $-a \in H$,). Si maintenant $-a$ est un carré, la forme $x^2 - \alpha y^2$ est équivalente à la forme $x^2 + y^2$ qui représente toutes les unités p-adiques (corollaire 2 du thtorème 3); cela signifie que, dans ce cas, H_α ne coïncide pas avec $\mathbf{Q}_p^{*2}$. De plus, H_α ne coïncide pas avec $\mathbf{Q}_p^*$ (si, bien sûr, $a \notin \mathbf{Q}_p^{*2}$). En effet, choisissant une unité p-adique ε qui n'est pas un carré, nous pouvons nous borner à donner à a les valeurs ε, p et $p\varepsilon$. Mais d'après le théorème 3 (et le théorème 10 du § 1 de l'appendice), la forme (5) ne représente pas zéro pour $a = E$, $\beta = p$ ni pour $a = p$, $p\varepsilon$,

β = E. Ainsi, on a bien $H_\alpha \neq Q_p^*$. Appliquons maintenant le corollaire 2 du théorème 1. Puisque $Q_p^* \supset H_\alpha \supset Q_p^{*2}$, alors l'indice $(Q_p^* : H,)$ est un diviseur de l'indice $(Q_p^* : Q_p^{*2}) = 4$. Mais, d'après ce qui précède, il ne peut être égal ni à 4 ni à 1; par suite, $(Q_p^* : H,) = 2$, ce qui démontre le théorème 6 dans le cas $p \neq 2$.

Soit maintenantp = 2. Il existe alors 8 classes résiduelles de Q_2^* selon Q_2^{*2} dont on peut prendre comme représentants les nombres 1, 3, 5, 7, 2.1, 2.3, 2.5, 2.7. Nous considérerons donc que a et β dans la forme (5) coïncident avec l'un de ces nombres et nous expliciterons dans quels cas cette forme représente zéro dans Q,. La réponse à cette question est donnée par le tableau ci-dessous, dans lequel le signe + indique que pour les valeurs correspondantes de a et β la forme représente zéro; les cases vides correspondent à des formes ne représentant pas zéro.

α \ β	1	3	5	7	2.1	2.3	2.5	2.7
1	+	+	+	+	+	+	+	+
3	+		+			+		i-
5	+	+	+	+				
7	+		+		+		+	
2.1	+			+	+			+
2.3	+	+					i-	+
2.5	+			+		+	+	
2.7	+	+			+	+		

(D'après la symétrie des rôles de α et β dans la forme (5), les signes + du tableau sont répartis symétriquement par rapport à la diagonale principale). Dans chaque ligne à l'exception de la première, le signe + figure dans quatre cases. Cela signifie que pour tout $\alpha \in Q_2^*$ qui n'est pas un carre, il y a quatre classes résiduelles selon le sous-groupe Q_2^{*2} qui sont représentables par la

forme (4). Ainsi $(H_\alpha : Q_2^{*2}) = 4$ et puisque $(Q_2^* : Q_2^{*2}) = 8$ (corollaire du théorème 2), alors $(Q_2^* : H,) = 2$.

Le tableau est établi à partir des résultats de 2). Soient $a = 2\varepsilon, \beta = 2\eta$, où ε et η sont des unités 2-adiques et supposons

$$2\varepsilon x^2 + 2\eta y^2 - z^2 = 0. \tag{6}$$

Nous pouvons supposer que x, y, z sont des entiers qui ne sont pas tous divisibles simultanément par 2. Il est clair que $z \equiv 0 \pmod 2$ et que x et y ne sont pas simultanément divisibles par 2 (car sinon la partie gauche de (6) ne serait pas divisible par (4)). Posant $z = 2t$, l'égalité (6) devient

$$\varepsilon x^2 + \eta y^2 - 2t^2 = 0;$$

en accord avec le corollaire du théorème 4, cette égalité équivaut à une congruence modulo 8 (avec x et y impairs). Puisque $x^2 \equiv y^2 \equiv 1 \pmod 8$ et $2t^2 \equiv 2 \pmod 8$ ou $2t^2 \equiv 0 \pmod S$, alors nous obtenons que la résolubilité de l'équation (6) est équivalente à la réalisation d'une au moins des congruences.

$$\varepsilon + \eta \equiv 2 \pmod 8, \qquad \varepsilon + \eta \equiv 0 \pmod 8.$$

Soit maintenant $\alpha = 2\varepsilon, \beta = \eta$. Dans l'égalité $2\varepsilon x^2 + \eta y^2 - z^2 = 0$ (avec x, y, z entiers 2-adiques non divisibles par 2 simultanément), nous avons, pour ces mêmes raisons, $y \not\equiv 0 \pmod 2$ et $z \not\equiv 0 \pmod 2$. Par suite, la réalisation de cette égalité (d'après le même corollaire du théorème 4) est équivalente à la réalisation d'une au moins des congruences

$$2\varepsilon + \eta \equiv 1 \pmod 8, \qquad \varepsilon \equiv 1 \pmod 8, \tag{7}$$

qui correspondent aux cas $2 \nmid x$ et $2|x$.

Il reste encore à examiner le cas $\alpha = \varepsilon, \beta = \eta$. Si dans l'égalité

$$\varepsilon x^2 + \eta y^2 - z^2 = 0,$$

les entiers 2-adiques x, y, z ne sont pas tous divisibles par 2 alors l'un d'entre eux est divisible par 2 mais les autres pas. Si $z \equiv 0 \pmod 2$, alors

$$\varepsilon x^2 + \eta y^2 \equiv \varepsilon + \eta \equiv 0 \pmod 4,$$

d'où il résulte que soit $\varepsilon \equiv 1 \pmod 4$, soit $\eta \equiv 1 \pmod 4$. Si maintenant $z \not\equiv 0 \pmod 2$, alors $\varepsilon x^2 + \eta y^2 \equiv 1 \pmod 4$ et puisque l'un des nombres x ou y est divisible par 2, alors l'autre ne l'est pas. Nous obtenons alors de nouveau que l'une des congruences

$$\varepsilon \equiv 1 \pmod 4, \qquad \eta \equiv 1 \pmod 4 \tag{8}$$

est réalisée. Réciproquement, supposons par exemple que $\varepsilon \equiv 1 \pmod 4$. Alors la congruence $\varepsilon x^2 + \eta y^2 - z^2 \equiv 0 \pmod 8$ est réalisée pour x = 1, $y = 0, z = 1$ si $\varepsilon \equiv 1 \pmod 8$ et pour $x = 1, y = 2, z = 1$ si $\varepsilon \equiv 5 \pmod 8$; cela signifie que la forme $\varepsilon x^2 + \eta y^2 - z^2$ représente zéro.

Après avoir terminé la vérification du tableau, on a, en même temps, démontré le théorème 6.

Du théorème 6 résulte que pour un nombre p-adique $\alpha \neq 0$ qui n'est pas un carré, le groupe quotient $\mathbf{Q}_p^*/\mathrm{H}_\alpha$ est un groupe cyclique d'ordre 2. On peut donc établir un isomorphisme de ce groupe avec le groupe $\{ 1, -1 \}$ des racines d'ordre 2 de 1. Cet isomorphisme entre $\mathbf{Q}_p^*/\mathrm{H}_\alpha$ et $\{ 1, -1 \}$ associe au sous-groupe H_α le nombre + 1 et à la classe résiduelle $\beta\mathrm{H}_\alpha$ distincte de H_α le nombre — 1. Il convient d'examiner cet homomorphisme du groupe $\mathbf{Q}_p^*$ dans le groupe $\{ + 1, -1 \}$, de noyaux H,.

DÉFINITION. — ***Pour des nombres p-adiques $a \neq 0$ et $\beta \neq 0$, définissons le symbole (α, β) comme égal à + 1 ou — 1 suivant que la forme $\alpha x^2 + \beta y^2 - z^2$ représente ou non zéro dans le corps Q,. Le symbole (a, β) s'appelle symbole de Hilbert.***

De cette définition résulte immédiatement que si ***a*** est un carré, alors $(a, \beta) = 1$ pour tout β. Si maintenant $\alpha \notin \mathbf{Q}_p^{*2}$, alors $(a, \beta) = 1$ si et seulement si $\beta \in \mathrm{H},$. On en déduit facilement que pour tout $a \neq 0$, l'application $\beta \to (\alpha, \beta)$ est un homomorphisme du groupe $\mathbf{Q}_p^*$ dans le groupe $\{ 1, -1 \}$ de noyau H_α. En d'autres termes, on a la formule

$$(\alpha, \beta_1\beta_2) = (\alpha, \beta_1)\,(\alpha, \beta_2). \tag{9}$$

De plus, la valeur du symbole (a, β) dépend de la résolubilité de l'équation (5) qui dépend symétriquement de a et β; par suite

$$(\alpha, \beta) = (\beta, \alpha), \tag{10}$$

d'où, d'après (9),

$$(\alpha_1\alpha_2, \beta) = (\alpha_1, \beta)\,(\alpha_2, \beta). \tag{11}$$

Remarquons encore que

$$(\alpha, -\alpha) = 1 \tag{12}$$

pour tout $a \in \mathbf{Q}_p^*$ (puisque l'équation $\alpha x^2 - \alpha y^2 - z^2 = 0$ admet la solution x = y = 1, $z = 0$), d'où, d'après (9),

$$(a, a) = (a, -1). \tag{13}$$

D'après les formules (9) à (13), le calcul du symbole (α, β) dans le cas général se ramène au calcul des valeurs (p, ε) et (E, η), ε et η étant des unités p-adiques. En effet, si $\alpha = p^k\varepsilon$, $\beta = p^l\eta$, alors

$$(p^k\varepsilon, p^l\eta) = (p, p)^{kl}(\varepsilon, p)^l(p, \eta)^k(\varepsilon, \eta) = (p, \varepsilon^l\eta^k(-1)^{kl})(\varepsilon, \eta).$$

Effectuons le calcul des valeurs (p, ε) et (E, η). Si $p \neq 2$, alors, d'après le théorème 3, la forme $px^2 + \varepsilon y^2 - z^2$ représente zéro si et seulement si $\varepsilon y^2 - z^2$ représente zéro, i. e. si l'unité ε est un carré. Ainsi $(p, \varepsilon) = \frac{\varepsilon}{0P}$ pour $p \neq 2$ (voir 1)). De plus, d'après le corollaire 2 du théorème 3, la forme $\varepsilon x^2 + \eta y^2 - z^2$ représente toujours zéro et cela signifie que $(E, \eta) = +1$ pour tout couple E, η d'unités p-adiques $(p \neq 2)$.

Dans le cas $p = 2$, les valeurs des symboles $(2, \eta)$ et (ε, η) pour des unités 2-adiques ε et η ont déjà été virtuellement déterminées dans la démonstration du théorème 6. En effet, d'après (7) (pour $\varepsilon = 1$), la forme $2x^2 + \eta y^2 - z^2$ représente zéro si et seulement si $\eta \equiv +1 \pmod 8$. Par suite,

$$(2, \eta) = (-1)^{\frac{\eta^2-1}{8}}.$$

De plus, nous avons vu que la forme $\varepsilon x^2 - \eta y^2 - z^2$ représente zéro si et seulement si une des congruences (8) est réalisée. Par suite,

$$(E, \eta) = (-1)^{\frac{\varepsilon-1}{2}\cdot\frac{\eta-1}{2}}.$$

Formulons le résultat obtenu.

THÉORÈME 7. — *Les valeurs des symboles de Hilbert (p, ε) et (E, η) pour des unités p-adiques ε et η sont définies par les formules*

$$(p, \varepsilon) = \left(\frac{\varepsilon}{p}\right), \qquad (\varepsilon, \eta) = 1 \quad \text{pour } p \neq 2;$$

$$(2, \varepsilon) = (-1)^{\frac{\varepsilon^2-1}{8}}, \qquad (\varepsilon, \eta) = (-1)^{\frac{E-1}{2}\cdot\frac{\eta-1}{2}} \quad \text{pour } p = 2.$$

4) Équivalence des formes binaires

Le symbole de Hilbert permet d'écrire sous forme évidente la condition d'équivalence de deux formes quadratiques binaires dans le corps $\mathbf{Q}_p$. Soient $f(x, y)$ et $g(x, y)$ deux formes quadratiques binaires non singulières

à coefficients dans $\mathbf{Q}_p$ et soient S(f) et 6(g) leurs déterminants. Pour que les deux formes f et g soient équivalentes, il est nécessaire que 6(f) et 6(g) diffèrent par un facteur multiplicatif appartenant à $\mathbf{Q}_p^{*2}$ (théorème 1, § 1 de l'appendice). Pour formuler une condition nécessaire et suffisante d'équivalence, établissons le théorème suivant.

THÉORÈME *8.* — ***Pour tout nombre p-adique $a \neq 0$ représentable par une forme binaire f de déterminant $\delta \neq 0$, la valeur du symbole de Hilbert $(a, -\delta)$ est la même.***

DÉMONSTRATION. — Soient a et *a'* deux nombres p-adiques non nuls représentables par la forme *f*. D'après le théorème 2, § 1 de l'appendice la forme *f* est équivalente à une forme f_1 du type $\alpha x^2 + \beta y^2$. Puisque *a'* est également représentable par la forme f_1, alors

$$a' = \alpha x_0^2 + \beta y_0^2, \qquad \text{d'où} \qquad \alpha\alpha' - \alpha\beta y_0^2 - (\alpha x_0)^2 = 0.$$

Cette dernière équation exprime que la forme $\alpha\alpha' x^2 - \alpha\beta y^2 - z^2$ représente zéro et par suite $(\alpha\alpha', -\alpha\beta) = 1$. Mais $\alpha\beta$ diffère de δ par un carré ; c'est pourquoi nous avons aussi $(\alpha\alpha', -\delta) = -1$ et cela entraîne, d'après la propriété (11), $(a, -\delta) = (a', -\delta)$; ainsi, notre théorème est démontré.

D'après le théorème 8, nous pouvons introduire pour toute forme binairef un nouvel invariant

$$e(f) = (\alpha, -\delta(f))$$

où *a* est un nombre p-adique différent de zéro représentable par la forme *f*.

THÉORÈME *9.* — ***Pour que deux formes quadratiques binaires non singulières f et g sur $\mathbf{Q}_p$ soient équivalentes, il faut et il suffit que les conditions ci-dessous soient réalisées :***

1) $\delta(f) = \delta(g)\gamma^2, \qquad \gamma \in \mathbf{Q}_p^*$;

2) $e(f) = e(g).$

DÉMONSTRATION. — La nécessité de ces deux conditions est tvidente. Pour démontrer la suffisance montrons que, si les conditions du théorème sont remplies, les formes *f* et g représentent les mêmes nombres p-adiques. Soit $y \in \mathbf{Q}_p^*$ un nombre représentable par la forme g. Supposant la forme *f* du type $\alpha x^2 + \beta y^2$, nous aurons

$$(\alpha, -\alpha\beta) = e(f) = e(g) = (\gamma, -\delta(g)) = (\gamma, -\alpha\beta),$$

d'oh

$$(\gamma\alpha^{-1}, -\alpha\beta) = 1.$$

D'après la définition du symbole de Hilbert, cela signifie que l'équation

$$\gamma\alpha^{-1}x^2 - \alpha\beta y^2 - z^2 = 0$$

est résoluble avec x, y, z différents de zéro. Mais alors

$$\gamma = \alpha\left(\frac{z}{x}\right)^2 + \beta\left(\frac{\alpha y}{x}\right)^2$$

i. e. la forme f représente y. L'équivalence de f et g résulte alors du théorème 11, § 1 de l'appendice.

5) Remarques sur les formes de degré plus grand

Le théorème 5 traduit un phénomène que l'on rencontre souvent en théorie des nombres : « tout se passe bien » si le nombre de variables est assez grand. Dans notre cas, « bien » signifie que la forme quadratique représente zéro dans le corps $\mathbf{Q}_p$ et « suffisamment grand » que le nombre de variables est $\geqslant 5$. Il serait très intéressant de continuer cette étude pour des formes de degré plus grand sur le corps des nombres p-adiques.

Le résultat exact est le suivant. Pour tout nombre naturel r, il existe un nombre N(r) tel que toute forme de degré r sur le corps des nombresp-adiques dont le nombre de variables est $>$ N(r) représente zéro. L'existence d'un tel nombre N(r) est loin d'être évidente *a priori*. Nous avons examiné ci-dessus le cas $r = 2$; les exemples de formes de degré supérieur que l'on peut examiner rendent très probable que $N(r) = r^2$, i. e. on a la conjecture suivante :

Toute forme de degré r à coefficients p-adiques et dont le nombre de variables est plus grand que r^2 représente zéro (*).

On connaît très peu de résultats généraux en direction de cette conjecture. Brauer a démontré la finitude du nombre $N(r)$ mais l'estimation obtenue à partir de sa démonstration est bien supérieure à r^2 (R. Brauer, A note on systems of homogeneous algebraic equations. ***Bull. Amer. Math. Soc.***, 1945, 51, 749-755). Pour $r = 2$, la vérification de la conjecture repose sur le théorème 5. Pour $r = 3$, la conjecture a été démontrte par V. B. Demianov et D. J. Lewis : ils ont démontré que toute forme cubique sur le corps des nombres p-adiques dont le nombre de variable est $\geqslant 10$ représente zéro (V. B. Demianov, Sur les formes cubiques dans les corps métriques. ***Dokl. Akad. Nauk URSS***, 1950, 74, n° 5, 889-891; D. J. Lewis, Cubic homogeneous polynomials over p-adic number fields. ***Ann. Math.***, 1952, 56, n° 3, 473-478).

(*) On sait maintenant, grâce à un exemple construit par G. Terjanian, que cette conjecture est *fausse* ; cf. ***C. R. Acad. Sci.***, Paris, 1966. Toutefois, J. Ax et S. Kochen ont prouvé que, pour un degré) r donné, elle est vraie pour toutes les valeurs de p sauf un nombre fini (dépendant de r) ; cf. ***Amer. J. of Math.***, 1965 (note communiquée par M. J. P. Serre).

En outre, Lang a démontré que si la conjecture est vraie pour tout r, on a également le résultat plus fort suivant :

Le système d'équations

$$\left.\begin{aligned} F_1(x_1, \ldots, x_m) &= 0 \\ \cdot \\ F_k(x_1, \ldots, x_m) &= 0 \end{aligned}\right\} \qquad (14)$$

dans lequel $F_1, \ldots, F_k$ sont des formes de degrés $r_1, \ldots, r_k$ à coefficients p-adiques a une solution non nulle si le nombre m de variables est plus grand que $r_1^2 + \ldots + r_k^2$ (S. Lang, On quasi algebraic closure. Ann. Math., 1952, 55, n° 2, 373-390).

Dans le cas de deux formes quadratiques, pour $m \geqslant 9$, la résolubilité du système (14) a été démontrée par V. B. Demianof (une démonstration simple du résultat de Demianov est contenue dans : B. J. Birch, D. J. Lewis et T. G. Murphy, Simultaneous quadratic forms. *Amer. J. Math.*, 1962, 84, n° 1, 110-115).

Il est enfin facile de montrer que la valeur hypothétique $N(r) = r^2$ est une borne inférieure, i. e. pour tout r il existe des formes de degré r à r^2 variables ne représentant pas zéro dans le corps des nombres p-adiques. Construisons un exemple d'une telle forme.

Rappelons dans ce but que, au point 2 § 1 de ce chapitre, on a construit une forme $F(x_1, \ldots, x_n)$ de degré n et à n variables telle que la congruence

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

n'ait que la seule solution :

$$x_1 \equiv 0 \pmod{p}, \ldots, x_n \equiv 0 \pmod{p}. \qquad (15)$$

Posons

$$\Phi(x_1, \ldots, x_{n^s}) = F(x_1, \ldots, x_n) + pF(x_{n+1}, \ldots, x_{2n}) + \ldots + p^{n-1}F(x_{n^s-n+1}, \ldots, x_{n^s})$$

et démontrons que la forme Φ ne représente pas zéro dans le corps des nombresp-adiques. Raisonnons par l'absurde, i. e. supposons que l'équation

$$\Phi(x_1, \ldots, x_n) = 0 \qquad (16)$$

ait une solution non nulle. D'après l'homogénéité de Φ, nous pouvons supposer que toutes les inconnues sont des entiers et que l'un au moins n'est pas divisible par p. Considérant (16) modulo p, on a $F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ d'où, d'après (15), $x_1 = px_1', \ldots, x_n = px_n'$. L'égalité (16) prend maintenant la forme

$$p^n F(x_1', \ldots, x_n') + pF(x_{n+1}, \ldots, x_{2n}) + \ldots + p^{n-1}F(x_{n^s-n+1}, \ldots, x_{n^s}) = 0$$

ou encore, après simplification par p,

$$F(x_{n+1}, \ldots, x_{2n}) + \ldots + p^{n-2}F(x_{n^2-n+1}, \ldots, x_{n^2}) + \ldots + p^{n-1}F(x'_1, \ldots, x'_n) = 0.$$

Par suite, $x_{n+1}, \ldots, x_{2n}$ sont divisibles par p. Répétant ce raisonnement n fois, nous démontrerions que $x_1, \ldots, x_{n^2}$ sont tous divisibles par p ce qui contredit notre hypothèse initiale.

EXERCICES

1. Démontrer les propriétés suivantes du symbole de Hilbert :

1) $(\alpha, 1 - a) = +1, \quad \alpha \neq 1;$

2) $(\alpha, \beta) = (\gamma, -\alpha\beta), \quad Y = \alpha\xi^2 + \beta\eta^2 \neq 0;$

3) $(\alpha\gamma, \beta\gamma) = (\alpha, \beta)(\gamma, -\alpha\beta).$

2. Soit $f = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ $(\alpha_i \in \mathbf{Q}_p^*)$ une forme quadratique ; l'expression

$$c_p(f) = (-1, -1) \prod_{1 \leqslant i \leqslant j \leqslant n} (\alpha_i, \alpha_j)$$

s'appelle le symbole de Hasse de la forme f. Démontrer que

$$c_p(\alpha x^2 + f) = c_p(f)(\alpha, -\delta),$$

$$c_p(\alpha x^2 + \beta y^2 + f) = c_p(f)(\alpha\beta, -\delta)(\alpha, \beta)$$

(δ est le déterminant de la forme f).

3. Soit $f = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ une forme à coefficients p-adiques représentant un nombre $y \neq 0$ de $\mathbf{Q}_p$. Montrer que y peut s'écrire sous la forme

$$y = \alpha_1 \xi_1^2 + \ldots + \alpha_n \xi_n^2 \qquad (\xi_i \in \mathbf{Q}_p),$$

toutes les sommes « partielles »

$$\gamma_k = \alpha_1 \xi_1^2 + \ldots + \alpha_k \xi_k^2 \qquad (1 \leqslant k \leqslant n)$$

étant différentes de zéro (utiliser les théorèmes 5 et 8 du § 1 de l'appendice).

4. Sous les hypothèses de l'exercice précédent, montrer que la forme f est équivalente à une forme diagonale du type

$$g = \gamma y_1^2 + \beta_2 y_2^2 + \ldots + \beta_n y_n^2 \quad \text{telle que} \quad c_p(g) = c_p(f)$$

(on démontrera tout d'abord que par le changement de variable $x = \mu X - \nu\beta Y$, $y = \nu X + \mu\alpha Y$ $(\alpha\mu^2 + \beta\nu^2 = y \neq 0)$ la forme $\alpha x^2 + \beta y^2$ s'écrit $\gamma X^2 + \alpha\beta\gamma Y^2$, d'où $(\alpha, \beta) = (\gamma, \alpha\beta\gamma)$).

5. Montrer, par récurrence sur le nombre des variables, que les symboles de Hasse de deux formes quadratiques diagonales non singulières équivalentes sur le corps $\mathbf{Q}_p$ sont égaux (Utiliser le théorème 4 du § 1 de l'appendice). On peut

donc maintenant définir le symbole de Hasse pour des formes quadratiques non singulières quelconques (non nécessairement diagonales) : si la forme f est équivalente à une forme quadratique f_0, nous poserons $c_p(f) = c_p(f_0)$.

6. Soient f_1 et f_2 deux formes quadratiques sur le corps $\mathbf{Q}_p$, de déterminants δ_1 et δ_2. Démontrer que :

$$c_p(f_1 + f_2) = c_p(f_1)\, c_p(f_2)\, (-1, -1)\, (\delta_1, \delta_2).$$

7. Soit f une forme quadratique non singulière sur le corps $\mathbf{Q}_p$, de déterminant δ et soit $a \neq 0$ un nombre du corps $\mathbf{Q}_p$. Montrer que

$$c_p(af) = \begin{cases} c_p(f)\left(\alpha, (-1)^{\frac{n+1}{2}}\right), & \text{si } n \text{ impair,} \\ c_p(f)\left(\alpha, (-1)^{\frac{n}{2}}\delta\right), & \text{si } n \text{ pair} \end{cases}$$

8. Démontrer qu'une forme quadratique non singulière f de trois variables sur le corps $\mathbf{Q}_p$ représente zéro si et seulement si $c_p(f) = +1$.

9. Soit f une forme quadratique non singulière de quatre variables sur le corps $\mathbf{Q}_p$, de déterminant 8. Montrer que f ne représente pas zéro dans $\mathbf{Q}_p$ si et seulement si δ est un carré dans $\mathbf{Q}_p$ et $c_p(f) = -1$.

10. Soit f une forme quadratique non singulière de n variables sur le corps $\mathbf{Q}_p$, de déterminant δ. Montrer que f représente un nombre p-adique $a \neq 0$ si et seulement si l'une des conditions suivantes est remplie :

1) $n = 1$ et $a\delta$ est un carré dans $\mathbf{Q}_p$;
2) $n = 2$ et $c_p(f) = (-a, -\delta)$;
3) $n = 3$, $a\delta$ est un carré dans $\mathbf{Q}_p$ et $c_p(f) = 1$;
4) $n = 3$ et $a\delta$ n'est pas un carré dans $\mathbf{Q}_p$;
5) $n \geqslant 4$.

11. Donner des conditions pour qu'une forme quadratique non singulière sur le corps $\mathbf{Q}_p$ ne représente pas zéro (sauf de manière triviale) mais représente tous les autres nombres p-adiques.

12. Dans quels corps de nombres p-adiques la forme $2x^2 - 5y^2 + 14z^2$ ne représente-t-elle pas zéro ?

13. Quels sont les nombres 5-adiques qui sont représentes par la forme $2x^2 + 5y^2$?

14. Soient f et f' deux formes quadratiques non singulières à n variables sur le corps $\mathbf{Q}_p$ et δ et δ' leurs déterminants. Démontrer que f et f' sont équivalentes si et seulement si $c_p(f) = c_p(f')$ et $\delta = \delta'a^2$ ($a \in \mathbf{Q}_p$).

§ 7. — FORMES QUADRATIQUES RATIONNELLES

1) Le théorème de Minkowski-Hasse

Nous exposerons ici la démonstration d'un des plus beaux résultats de la thtorie des nombres, le théorème de Minkowski-Hasse.

THÉORÈME 1 (Minkowski-Hasse). — ***Une forme quadrutique à coefficients rationnels représente zéro dans le corps des nombres rationnels si et seulement si elle représente zéro dans le corps des nombres rationnels et dans tous les corps de nombres p-adiques (pour tout nombre premier p).***

La démonstration de ce théorème dépend de manière essentielle du nombre n de variables de la forme quadratique. Pour $n = 1$, c'est trivial. Pour $n = 2$, la démonstration est encore très simple. Si une forme quadratique binaire rationnellefde discriminant $d \neq 0$ représente zéro dans le corps des réels, alors $-d > 0$ (cf. appendice § 1, théorème 10); par suite

$$-d = p_1^{k_1} \dots p_s^{k_s},$$

où les p_i sont des nombres premiers deux à deux distincts. Si f représente zéro dans le corps $\mathbf{Q}_{p_i}$, alors, puisque $-d$ est un carré dans $\mathbf{Q}_{p_i}$, l'exposant k_i est pair $(i = 1, \dots, s)$. Mais alors $-d$ est un carré aussi dans le corps Q des nombres rationnels et par suite f représente zéro dans Q.

Pour $n \geqslant 3$, la démonstration du théorème est beaucoup plus compliquée. Faisons quelques remarques pour commencer.

Nous supposerons que les coefficients de la forme quadratique considérée sont des entiers rationnels (car s'il n'en est pas ainsi, nous multiplierons la forme par le dénominateur commun de ses coefficients). Il est clair que la résolubilité de l'équation (1) dans Q ou dans le corps $\mathbf{Q}_p$ des nombres p-adiques est équivalente, d'après l'homogénéité, à sa résolubilité dans l'anneau $\mathbf{Z}$ des entiers rationnels ou dans l'anneau $\mathbf{Z}_p$ des nombres entiers p-adiques. La résolubilité de (1) dans le corps des nombres réels est équivalente au fait que f est une forme non définie. Par suite et d'après le théorème 2 du § 5, on peut donner au théorème de Minkowski-Hasse la forme suivante :

Pour que l'équation (1) ***soit résoluble dans les nombres entiers rationnels, il faut et il suffit que la forme f soit non définie et que pour tout entier de la forme p^m, la congruence***

$$f(x_1, \dots, x_n) \equiv 0 \pmod{p^m}$$

ait une solution telle que la valeur de l'une au moins des inconnues ne soit pas divisible par p.

D'après le théorème 5, § 6, toute forme de cinq variables ou plus représente toujours zéro dans le corps des nombres p-adiques. Par suite pour de telles formes le théorème de Minkowski-Hasse devient :

Pour qu'une forme quadratique rationnelle non singulière de $n \geqslant 5$ variables représente zéro dans le corps des nombres rationnels, il faut et il suffit qu'elle soit non définie.

Ainsi, il suffit de vérifier les conditions de résolubilité dans les corps de nombres p-adiques pour $n = 3,4$. Pour ces valeurs particulières, le théorème de Minkowski-Hasse nous donne également un critère effectif de réso-

lubilité de l'équation (1). En effet, si la formefest réduite à une somme de carrés, $f = \Sigma a_i x_i^2$, p premier impair ne divisant aucun des coefficients a_i, la forme f, pour $n \geqslant 3$, représente toujours zéro dans $\mathbf{Q}_p$, d'après le corollaire 2 du théorème 3, § 6. Par suite, les vérifications à effectuer sont relatives seulement à un nombre fini d'entiers premiers. Pour chacun de ces p, la question de la représentation de zéro par f dans $\mathbf{Q}_p$ est résoluble par les théorèmes du paragraphe précédent.

D'après le théorème 6, § 1 de l'appendice, le théorème 1 entraîne le résultat suivant.

COROLLAIRE. — *Pour qu'une forme quadratique non singulière à coefficients rationnels représente un nombre rationnel a, il faut et il suffit qu'elle représente a dans le corps des nombres réels et dans tous les corps $\mathbf{Q}_p$ de nombres p-adiques.*

2) Formes de trois variables

Démontrons le théorème de Minkowski-Hasse dans le cas $n = 3$. Pour les formes de 3 variables, le thtorème 1 a été démontré (sous une autre forme) par Legendre. La formulation de Legendre est exposée dans l'exercice 1.

Supposons la forme réduite à une somme de carrés $a_1x^2 + a_2y^2 + a_3z^2$. Dire que la forme est non définie signifie que les trois coefficients a_1, a_2, a_3 ne sont pas de même signe. Multipliant la forme par — 1 si cela est nécessaire, nous sommes ramenés au cas où deux coefficients sont positifs et le troisième négatif. Nous pouvons d'autre part supposer que les nombres a_1, a_2, a_3 sont entiers, non divisibles par des carrés et premiers dans leur ensemble. De plus, si par exemple a_1 et a_2 ont un facteur premier commun p, multipliant la formule par p et prenant px et py comme nouvelles variables, on obtient une forme à coefficients $\frac{a_1}{p}, \frac{a_2}{p}, pa_3$. Répétant plusieurs fois cette opération, notre forme devient une forme du type

$$ax^2 + by^2 - cz^2 \tag{2}$$

dans laquelle $a, b,$ c sont premiers deux à deux (et sans carrés).

Soit p un diviseur premier impair du nombre c. Puisque, par hypothèse, la forme 2 représente zéro dans $\mathbf{Q}_p$, alors, d'après le théorème 3 du § 6 et le corollaire 1 de ce théorème, la congruence

$$ax^2 + by^2 \equiv 0 \pmod{p}$$

a une solution non triviale (disons (x_1, y_0)). Mais alors, la forme $ax^2 + by^2$ est décomposable en facteurs modulo p :

$$ax^2 + by^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}.$$

Ceci est aussi vrai pour la forme (2), i. e. on a une congruence du type

$$ax^2 + by^2 - cz^2 \equiv L^{(p)}(x, y, z)\ M^{(p)}(x, y, z) \pmod{p} \tag{3}$$

dans laquelle $L^{(p)}$ et $M^{(p)}$ sont des formes linéaires à coefficients entiers. On a des congruences analogues pour les diviseurs premiers impairs p des coefficients a et b et aussi pour $p = 2$, puisque

$$ax^2 + by^2 - cz^2 \equiv (ax + by - cz)^2 \pmod 2.$$

Prenons maintenant des formes lintaires $L(x, y, z)$ et $M(x, y, z)$ telles que

$$L(x, y, z) \equiv L^{(p)}(x, y, z) \pmod{p}$$
$$M(x, y, z) \equiv M^{(p)}(x, y, z) \pmod{p}$$

pour tous les diviseurs premiers p de l'un des coefficients a, b, c. Les congruences (3) montrent alors que

$$ax^2 + by^2 - cz^2 \equiv L(x, y, z)\ M(x, y, z) \pmod{abc}. \tag{4}$$

Imposons aux variables x, y, z de prendre des valeurs entières satisfaisant aux conditions

$$0 \leqslant x < \sqrt{bc}, \qquad 0 \leqslant y < \sqrt{ac}, \qquad 0 \leqslant z < \sqrt{ab}. \tag{5}$$

Si nous excluons de cette étude le cas a = b = c = 1 (pour la forme

$$x^2 + y^2 - z^2,$$

le théorème est évident : elle représente zéro dans tout corps), alors, puisque a, b, c sont premiers deux à deux, les nombres $\sqrt{bc}$, $\sqrt{ac}$ et $\sqrt{ab}$ ne sont pas tous entiers. Il en résulte facilement que le nombre des triplets (x, y, z) satisfaisant aux conditions (5) est strictement supérieur à

$$\sqrt{ab}.\sqrt{bc}.\sqrt{ac} = abc.$$

Considérons les valeurs prises par la forme linéaire L(x, y, z) pour ces valeurs des variables. Puisque le nombre des triplets (x, y, z) vérifiant (5) est supérieur au nombre des résidus modulo abc, alors il existe deux triplets distincts (x_1, y_1, z_1) et (x_2, y_2, z_2) tels que l'on ait la congruence

$$L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \pmod{abc}.$$

Il résulte alors de la linéarité de la forme L que

$$L(x_0, y_0, z_0) \equiv 0 \pmod{abc}$$

pour $x_0 = x_1 - x_2$, $y_0 = y_1 - y_2$, $z_0 = z_1 - z_2$.

De la congruence (4) résulte alors

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc}. \tag{6}$$

Puisque les conditions (5) sont réalisées pour les triplets (x_1, y_1, z_1) et (x_2, y_2, z_2) alors

$$|x_0| < \sqrt{bc}, \qquad |y_0| < \sqrt{ac}, \qquad |z_0| < \sqrt{ab},$$

et par suite

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc. \tag{7}$$

L'inégalité (7) est compatible avec la congruence (6) seulement si

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \tag{8}$$

ou bien

$$ax_0^2 + by_0^2 - cz_0^2 = abc. \tag{9}$$

Dans le premier cas nous obtenons une représentation non triviale de zéro par la forme (2); c'est ce qu'il fallait établir. Dans le deuxième cas, nous arriverons au même résultat grâce au lemme suivant.

LEMME 1. — *Si la forme (2) représente abc, alors elle représente aussi zéro.*

Soient x_0, y_0, z_0 satisfaisant à l'égalité (9). Il est alors facile de voir que

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0. \tag{10}$$

Si $z_0^2 = ab \neq 0$, alors cette égalité démontre le lemme. Si maintenant $-ab = z_0^2$, alors la forme $ax^2 + by^2$ représente zéro (cf. appendice, § 1, théorème 10). Mais alors la forme (2) représente aussi zéro et par suite le lemme est encore vérifié dans cc cas.

La démonstration du lemme 1 est très courte, mais elle repose sur un calcul qui utilise l'identité (10). Donnons une autre démonstration plus générale. Si bc est un carré, alors la forme $by^2 - cz^2$ et avec elle la forme (2) représente zéro. Supposons que bc n'est pas un carré. Dans ce cas, la représentabilité de zéro par la forme (2) est équivalente au fait que ac est la norme d'un élément du corps $\mathbf{Q}(\sqrt{bc})$. En effet, l'égalité (8) (dans laquelle on peut supposer $x_0 \neq 0$) entraîne

$$ac = \left(\frac{cz_0}{x_0}\right)^2 - bc\left(\frac{y_0}{x_0}\right)^2 = \mathrm{N}\left(\frac{cz_0}{x_0} + \frac{y_0}{x_0}\sqrt{bc}\right).$$

Réciproquement, si $ac = \mathrm{N}(u + v\sqrt{bc})$, alors

$$ac^2 + b(cv)^2 - cu^2 = 0.$$

Supposons maintenant que l'égalité (9) soit satisfaite. En la multipliant par c, elle prend la forme

$$ac(x_0^2 - bc) = (cz_0)^2 - bcy_0^2$$

ou bien

$$ac\mathrm{N}(\alpha) = \mathrm{N}(\beta),$$

avec

$$\alpha = x_0 + \sqrt{bc}, \qquad \beta = cz_0 + y_0\sqrt{bc}.$$

Mais

$$ac = \mathrm{N}(\gamma), \qquad \gamma = \frac{\beta}{\alpha} \in \mathrm{R}(\sqrt{bc}),$$

et cela, comme nous l'avons vu, signifie aussi que la forme (2) représente zéro dans $\mathbf{Q}$.

Attirons l'attention sur le fait suivant. Dans la démonstration ci-dessus du théorème 1 pour trois variables, nous n'avons utilisé nulle part la résolubilité de l'équation (2) dans le corps des nombres 2-adiques. Par suite, la résolubilité de l'équation (2) dans le corps des nombres réels et dans les corps $\mathbf{Q}_p$ pour tout p impair entraîne sa résolubilité aussi dans le corps Q,. On a une propriété analogue pour tout corps $\mathbf{Q}_q$: si une forme quadratique rationnelle de trois variables représente zéro dans le corps des réels et dans tous les corps $\mathbf{Q}_p$ sauf peut-être dans le corps $\mathbf{Q}_q$, alors elle représente zéro aussi dans le corps $\mathbf{Q}_q$ (et par suite, d'après le théorème, dans le corps Q des nombres rationnels). Essayons d'expliquer ce fait. Considérons pour cela les conditions de représentation de zéro par la forme

$$ax^2 + by^2 - z^2 \tag{11}$$

dans les corps $\mathbf{Q}_p$ et dans le corps des nombres rationnels (ici a et b sont des nombres rationnels non nuls); il est clair que toute forme quadratique rationnelle non singulière de trois variables peut être écrite sous la forme (11) par changement linéaire de variables et multiplication par un nombre rationnel. D'après le point 3) du § 6, la condition de représentabilité de zéro par la forme (11) dans le corps des nombres p-adiques peut s'écrire

$$\left(\frac{a, b}{p}\right) = 1, \tag{12}$$

où $\left(\frac{a, b}{P}\right)$st le symbole de Hilbert dans le corps $\mathbf{Q}_p$. Nous adoptons ici cette notation pour le symbole de Hilbert (a, b) dans le corps $\mathbf{Q}_p$ pour préciser le corps dans lequel nous le considérons, car nous serons amenés à considérer simultanément des symboles de Hilbert pour plusieurs valeurs de p.

Dans le corps des nombres réels, la forme (11) représente zéro si et seulement si au moins un des nombres a, b est positif. Pour écrire cette condi-

tion sous la même forme que (12), étendons les résultats du §6.3 au corps des nombres réels. Utilisons le fait que les corps p-adiques $\mathbf{Q}_p$ et le corps des nombres réels sont tous les complétés du corps Q des nombres rationnels. Ainsi les corps $\mathbf{Q}_p$ correspondent biunivoquement aux nombres premiers *p.* Désirant englober dans cette correspondance le corps des nombres réels, on utilise souvent le symbole ∞ appelé nombre premier éloigné à l'infini et on dit que le corps des nombres réels est le complété du corps Q qui correspond au nombre premier ∞ éloigné à l'infini. Les nombres premiers usuels distincts du symbole ∞ introduit s'appellent alors nombres premiers finis. Par analogie avec la notation $\mathbf{Q}_p$, le corps des nombres réels sera désigné ici par Q_∞.

Pour tout α du groupe multiplicatif de $\mathbf{Q}_\infty$, considérons la forme

$$x^2 - \alpha y^2 \tag{13}$$

et désignons par H_α l'ensemble des nombres $\beta \in \mathbf{Q}_\infty^*$ représentés par cette forme. Si $\alpha > 0$, i. e. $\alpha \in \mathbf{Q}_\infty^{*2}$, alors la forme (13) représente tous les nombres réels et par suite $H_\alpha = \mathbf{Q}_\infty^*$. Si maintenant $\alpha < 0$, i. e. α n'est pas un carré, la forme (13) représente seulement les nombres positifs et par suite, comme dans le théorème 6, § 6, nous avons :

$$(\mathbf{Q}_\infty^* : H,) = 2. \tag{14}$$

Il en résulte que si pour a, $\beta \in \mathbf{Q}_\infty^*$ on pose $(\alpha, \beta) = \pm 1$ suivant que la forme (13) représente ou non le nombre β, alors le symbole (a, β) possède les propriétés (9) à (13) du § 6.

Le théorème 7, § 6 qui permet le calcul du symbole de Hilbert dans le corps $\mathbf{Q}_p$ se réduit ici à

$$\left.\begin{array}{l} (a, \beta) = +1 \text{ si } a > 0 \text{ ou } \beta > 0 \\ (a, \beta) = -1 \text{ si } \alpha < 0 \text{ et } \beta < 0 \end{array}\right\} \tag{15}$$

Pour des nombres rationnels *a, b* nous désignerons par $\left(\frac{a, b}{\infty}\right)$ la valeur du symbole (a, *b)* dans le corps Q,.

En utilisant le symbole $\left(\frac{a, b}{p}\right)$, nous pouvons maintenant énoncer le théorème 1 pour les formes de 3 variables sous la forme suivante :

La forme $ax^2 + by^2 - z^2$, ***a, b étant des rationnels différents de zéro, représente zéro dans le corps des nombres rationnels si et seulement si, pour tout*** p ***(y compris*** $p = \infty$***) l'égalité***

$$\left(\frac{a, b}{p}\right) = 1 \tag{16}$$

est satisfaite

Pour tous les rationnels a et b différents de zéro, le symbole $\left(\frac{a, b}{p}\right)$ est différent de $+1$ seulement pour un nombre fini de valeurs de p. En effet, si $p \neq 2, \infty$ et si p ne figure pas dans la décomposition de a et b (cela signifie que a et b sont des unités p-adiques), alors, d'après le corollaire 2 du théorème 3, § 6, la forme (11) représente zéro dans $\mathbf{Q}_p$ et, par suite, pour toutes ces valeurs de p, $\left(\frac{a, b}{p}\right) = 1$. Par ailleurs, les valeurs du symbole $\left(\frac{a, b}{p}\right)$ pour a, b fixés satisfont à d'autres conditions. Ainsi, le nombre des valeursp (y compris $p = \infty$) pour lesquels $\left(\frac{a, b}{p}\right) = -1$ est toujours pair. On peut aussi exprimer ce résultat sous la forme suivante :

$$\prod_p \left(\frac{a, b}{p}\right) = 1 \tag{17}$$

où p parcourt tous les nombres premiers et le symbole ∞. En effet, le produit formel infini ci-dessus contient seulement un nombre fini de facteurs différents de + 1 et le fait que ce produit est égal à 1 est équivalent à la parité du nombre des p tels que $\left(\frac{a, b}{p}\right) = -1$.

Démontrons (17). Représentant a et b comme produit de puissances de nombres premiers et utilisant les formules (9) à (13) du § 6 (également vérifiées pour $p = \infty$), il est facile de démontrer la formule (17) dans les cas particuliers suivants :

1) a = - 1 , b = - 1

2) $a = q$ b = - 1 (q premier);

3) $a = q$, $b = q'$ (q et q' premiers, $q \neq q'$).

D'après le théorème 7, § 6 et les formules (15), nous obtenons

$$\prod_p \left(\frac{-1, -1}{p}\right) = \left(\frac{-1, -1}{2}\right)\left(\frac{-1, -1}{\infty}\right) = (-1)\cdot(-1) = 1 ;$$

$$\prod_p \left(\frac{2, -1}{p}\right) = \left(\frac{2, -1}{2}\right)\left(\frac{2, -1}{\infty}\right) = 1\cdot 1 = 1 ;$$

$$\prod_p \left(\frac{q, -1}{p}\right) = \left(\frac{q, -1}{q}\right)\left(\frac{q, -1}{2}\right) = \left(\frac{-1}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{-1-1}{2}} = 1 ;$$

$$\prod_p \left(\frac{2, q}{p}\right) = \left(\frac{2, q}{q}\right)\left(\frac{2, q}{2}\right) = \left(\frac{2}{q}\right)(-1)^{\frac{q^2-1}{8}} = 1 ;$$

$$\prod_p \left(\frac{q, q'}{p}\right) = \left(\frac{q, q'}{q}\right)\left(\frac{q, q'}{q'}\right)\left(\frac{q, q'}{2}\right) = \left(\frac{q'}{q}\right)\left(\frac{q}{q'}\right)(-1)^{\frac{q'-1}{2}\cdot\frac{q-1}{2}} = 1.$$

Les nombres premiers q et q' dans ces formules sont impairs et distincts et cela démontre la formule (17).

Remarquons que, dans cette démonstration, nous avons utilisé la loi de réciprocité quadratique de Gauss. Il est facile de voir, d'autre part, à l'aide de l'expression explicite du symbole de Hilbert donnée dans le théorème 7, § 6, que l'on peut déduire de la formule (17) la loi de réciprocité. Ainsi la formule (17) est équivalente à la loi de réciprocité de Gauss.

Supposons maintenant que la forme (11) représente zéro dans tous les corps $\mathbf{Q}_p$ sauf peut-être dans le corps $\mathbf{Q}_q$. L'égalité (17) et les conditions $\left(\frac{a, b}{p}\right) = +1$ pour tout $p \neq q$ nous donnent alors que $\left(\frac{a, b}{p}\right) = 1$. En d'autres termes, on a démontré l'affirmation suivante.

LEMME 2. — *Si une forme quadratique rationnelle de 3 variables représente zéro dans tous les corps $\mathbf{Q}_p$ (p parcourt tous les nombres premiers et le symbole ∞) sauf peut-être dans le corps $\mathbf{Q}_q$, elle représente aussi zéro dans le corps $\mathbf{Q}_q$.*

3) Formes de 4 variables

Nous considérerons les formes

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \tag{18}$$

où les a_i sont des entiers ne contenant pas de facteurs au carré. La forme étant non définie, il est clair que nous pouvons supposer $a_1 > 0$ et $a_4 < 0$. Nous considérerons en même temps que la forme (18) les formes

$$g = a_1x_1^2 + a_2x_2^2 \quad \text{et} \quad h = -a_3x_3^2 - a_4x_4^2.$$

L'idée de la démonstration du théorème de Minkowski-Hasse pour les formes de 4 variables est la suivante.

Utilisant le fait que la forme (18) représente zéro dans les corps $\mathbf{Q}_p$, nous montrerons qu'il existe un entier rationnel $a \neq 0$ représentable simultanément par les formes g et h dans les rationnels. Cela nous donne immédiatement une représentation rationnelle de zéro par la forme (18).

Soient $p_1, \ldots, p_s$ les diviseurs premiers impairs distincts des coefficients a_1, a_2, a_3, a_4. Pour tout p égal à un des $p_1, \ldots, p_s$ et pour $p = 2$ choisissons dans le corps $\mathbf{Q}_p$ une représentation de zéro

$$a_1\xi_1^2 + a_2\xi_2^2 + a_3\xi_3^2 + a_4\xi_4^2 = 0,$$

telle que tous les ξ_i soient différents de zéro (cf. appendice § 1, théorème 8) et posons

$$b_p = a_1\xi_1^2 + a_2\xi_2^2 = -a_3\xi_3^2 - a_4\xi_4^2.$$

Il est facile de voir qu'on peut choisir les ξ_i tels que $b_p \neq 0$, soit un nombre entier p-adique non divisible par p^2 (si $b_p = 0$, les formes g et h représentent zéro dans $\mathbf{Q}_p$ et d'après le théorème 5, § 1 de l'appendice, représentent tous les nombres de $\mathbf{Q}_p$). Considérons le système des congruences

$$\left.\begin{aligned} a &\equiv b_2 \pmod{16} \\ a &\equiv b_{p_1} \pmod{p_1^2} \\ &\cdot \\ a &\equiv b_{p_s} \pmod{p_s^2} \end{aligned}\right\} \tag{19}$$

L'entier rationnel a satisfaisant à ces congruences est dtfini de manière unique modulo $m = 16p_1^2, \ldots, p_s^2$. Puisque b_{p_i} n'est pas divisible par p_i^2, alors $b_{p_i}a^{-1}$ est une unité pi-adique et par suite $b_{p_i}a^{-1} \equiv 1 \pmod{p_i}$. D'après le corollaire 1 du théorème 1, § 6, le nombre $b_{p_i}a^{-1}$ est un carré dans le corps $\mathbf{Q}_{p_i}$. De la même manière, puisque b_2 n'est pas divisible par 2^2, alors $b_2a^{-1} \equiv 1 \pmod 8$ et par suite (théorème 2, § 6) b_2a^{-1} est un carré dans $\mathbf{Q}_2$.

Du fait que b_p et a ne diffèrent que par un carré, pour tout p -2, $p_1, \ldots, p_s$, les formes

$$-ax_0^2 + g \quad \text{et} \quad -ax_0^2 + h \tag{20}$$

représentent zéro dans $\mathbf{Q}_p$. Si a a été choisi > 0, alors, d'après les conditions $a_1 > 0$ et $-a_4 > 0$, les formes (20) représentent aussi zéro dans le corps des nombres réels. Si maintenant $p \neq 2, p_1, \ldots, p_s$ et ne figure pas dans a, i. e. si p impair ne divise pas les coefficients des formes (20), alors ces formes représentent zéro dans $\mathbf{Q}_p$ d'après le corollaire 2 du théorème 3, § 6. Supposons que le nombre a contient un seul facteur premier q différent des nombres $p_1, \ldots, p_s$ (on montrera ci-dessous que l'on peut toujours choisir a ainsi); nous pouvons alors appliquer le lemme 2 aux formes (20) et conclure (d'après le théorème de Minkowski-Hasse pour les formes de 3 variables) que les formes (20) représentent zéro dans le corps des nombres rationnels. Mais alors, nous obtiendrons pourlenombre a les représentations

$$a = a_1c_1^2 + a_2c_2^2, \qquad a = -a_3c_3^2 - a_4c_4^2,$$

les c_i étant rationnels, d'où

$$a_1c_1^2 + a_2c_2^2 + a_3c_3^2 + a_4c_4^2 = 0$$

et le théorème est démontré.

Montrons que l'on peut toujours trouver $a > 0$ satisfaisant aux congruences (19) et possédant la propriété remarquable utilisée ci-dessus. Nous appliquerons le théorème de Dirichlet sur les nombres premiers dans une progression arithmétique (ce théorème sera démontré dans le chapitre V, § 3-2)). Ce théorème affirme que si la raison et le premier terme d'une progression arithmétique infinie sont premiers entre eux, alors cette progression contient une infinité de nombres premiers. Soit $a^* > 0$ une des valeurs de a satisfaisant aux congruences (19). Désignons par d le plus grand diviseur commun de a^* et m. Puisque $\frac{a^*}{d}$ et $\frac{m}{d}$ sont premiers entre eux, il existe, d'après le théorème de Dirichlet, un nombre $k \geqslant 0$ tel que $\frac{a^*}{d} + k\frac{m}{d} = q$ soit premier. Nous prendrons alors pour a le nombre

$$a = a^* + km = dq.$$

Puisque d contient certains des nombres premiers 2, $p_1, \ldots, p_s$, alors ce choix de a permet de terminer la démonstration du théorème 1 pour les formes de 4 variables.

4) Les formes de 5 variables et plus

Soit une forme quadratique rationnelle non définie de 5 variables réduite à une somme de carrés

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 \qquad (21)$$

où tous les a_i sont entiers et sans carrés. Nous pouvons supposer $a_1 > 0$ et $a_5 < 0$. Posons

$$g = a_1x_1^2 + a_2x_2^2, \qquad h = a_3x_3^2 - a_4x_4^2 - a_5x_5^2.$$

En raisonnant comme dans le cas $n = 4$, nous déterminerons au moyen du théorème de Dirichlet un nombre entier rationnel $a > 0$ représentable par g et h dans le corps des nombres réels et dans tous les corps $\mathbf{Q}_p$ sauf peut-être dans le corps $\mathbf{Q}_q$, q étant un nombre premier impair ne figurant pas dans les coefficients a_i. Mais alors g et h représentent a aussi dans le corps Q,, Pour la forme g, cela s'établit de même que plus haut à l'aide du lemme 2. Pour la forme h, elle représente zéro dans $\mathbf{Q}_q$ (corollaire 2 du théorème 3, § 6) et par suite représente tous les nombres q-adiques (cf. appendice, § 1, théorème 5). D'après le corollaire du théorème de Minkowski-Hasse (cf. fin de 1), qui a été déjà été démontré pour 3 et 4 variables, nous obtenons que les formes g et h représentent a également dans le corps des nombres rationnels, d'où, comme ci-dessus, résulte facilement que la forme (21) représente rationnellement zéro.

Pour démontrer le théorème 1 dans le cas $n > 5$, il suffit de remarquer que toute forme quadratique rationnelle non définie fréduite à une somme de carrés peut se représenter sous la forme $f = f_0 + f_1$, où f_0 est une forme non définie de 5 variables. D'après ce qui précède la forme f_0 et par suite la formefreprésentent zéro dans le corps des nombres rationnels. Le théorème de Minkowski-Hasse est complètement démontré.

5) Équivalence rationnelle

Le théorème de Minkowski-Hasse permet de résoudre l'importante question de l'équivalence des formes quadratiques rationnelles.

THÉORÈME 2. — ***Pour que deux formes quadratiques non singulières à coefficients rationnels soient équivalentes sur le corps des nombres rationnels, il faut et il suffit qu'elles soient équivalentes sur le corps des nombres réels et sur tous les corps $\mathbf{Q}_p$ de nombres p-adiques.***

DÉMONSTRATION. — La nécessité est triviale. La suffisance se démontre par récurrence sur le nombre n de variables. Soit $n = 1$. L'équivalence des formes ax^2 et bx^2 sur un corps signifie que $\frac{a}{b}$ est un carré dans ce corps. Mais si $\frac{a}{b}$ est un carré dans le corps des nombres réels et dans tous les corps $\mathbf{Q}_p$, alors, comme nous l'avons vu dans 1), $\frac{a}{b}$ est également un carré dans le corps Q des nombres rationnels. Ainsi le théorème 2 est démontré pour $n = 1$.

Soit maintenant $n > 1$. Choisissons un nombre rationnel $a \neq 0$ représentable par la formef(sur le corps Q). Puisque des formes équivalentes représentent les mêmes nombres, alors la forme g représente a dans le corps des nombres réels et dans tous les corps $\mathbf{Q}_p$. Mais alors, d'après le corollaire du théorème de Minkowski-Hasse, la forme g représente également a dans le corps Q. En utilisant le théorème 2, § 1 de l'appendice, nous concluons alors que $f \sim ax^2 + f_1$, $g \sim ax^2 + g_1$, où f_1 et g_1 sont des formes quadratiques de $(n - 1)$ variables sur le corps Q (le signe $\sim$ signifie ici équivalence sur $\mathbf{Q}$). De l'équivalence des formes $ax^2 + f_1$ et $ax^2 + g_1$ dans le corps des nombres réels et dans les corps $\mathbf{Q}_p$, il résulte que les formes f_1 et g_1 sont également équivalentes dans tous ces corps (cf. appendice § 1, théorème 4). Par hypothèse de récurrence& et g_1 sont équivalentes sur le corps Q des nombres rationnels. Mais alors f et g sont aussi équivalentes sur Q et le théorème 2 est démontré.

Comme exemple, étudions la question de l'équivalence des formes quadratiques binaires. Le discriminant d(f) d'une forme rationnelle non singulière s'écrit de manière unique

$$d(f) = d_0(f)c^2$$

oh $d_0(f)$ est un nombre entier sans carrés. D'après le théorème 1, § 1 de l'appendice, par le passage à une forme équivalente, la valeur $d_0(f)$ ne change pas et cela signifie que c'est un invariant de la classe des formes rationnellement équivalentes.

Soit a un nombre rationnel quelconque non nul représentable par une forme binaire non singulière f. Pour tout nombre premier p (y compris $p = \infty$), posons

$$e_p(f) = \left(\frac{a, -d(f)}{p}\right).$$

D'après le théorème 8, § 6 (qui est aussi vrai, c'est évident, pour le corps des nombres réels Q,), la valeur $e_p(f)$ ne dépend pas du choix de a. Par suite, c'est également un invariant de la forme f pour l'équivalence rationnelle des formes. Réunissant le théorème 2 au théorème 9 du § 6 (vrai aussi pour le corps Q,), nous obtenons le critère suivant d'équivalence rationnelle des formes quadratiques binaires.

THÉORÈME *3. — Deux formes quadratiques binaires f et g sont rationnellement équivalentes si et seulement si*

$$d_0(f) = d_0(g), \qquad e_p(f) = e_p(g) \qquad \textit{pour tout } p.$$

Remarquons que si l'équivalence des formes est définie par le système infini des invariants e,(f), le nombre de ces invariants est en fait fini puisque e,(f) $\neq +1$ seulement pour un nombre fini d'entiers p.

6) Remarques sur les formes de degré supérieur

On se propose ici d'étudier une extension éventuelle du théorème de Minkowski-Hasse à des formes d'autres degrés : est-il vrai qu'une forme rationnelle représente zéro dans le corps des nombres rationnels dès qu'elle représente zéro dans le corps réel et dans les corps $\mathbf{Q}_p$? Il est facile de construire des contre-exemples. Par exemple, si q, l, q', l' sont des nombres premiers distincts tels que $\left(\frac{l}{q}\right) = -1$, $\left(\frac{l'}{q'}\right) = -1$ et si la forme $x^2 + qy^2 - lz^2$ représente zéro dans le corps des nombres 2-adiques, alors la forme de degré 4

$$(x^2 + qy^2 - lz^2)(x^2 + q'y^2 - l'z^2) \tag{22}$$

représentera zéro dans tous les corps $\mathbf{Q}_p$ et dans le corps des nombres réels, mais ne représentera pas zéro dans le corps des nombres rationnels. En effet, dans le corps $\mathbf{Q}_2$, le premier facteur représente zéro par hypothèse. Si p impair est différent de q et l, alors le premier facteur représente zéro dans le corps $\mathbf{Q}_p$ d'après le corollaire 2 du théorème 3, § 6. Dans ces corps $\mathbf{Q}_q$ et $\mathbf{Q}_l$, le deuxième facteur représente ztro pour la même raison. Pourtant, aucun de ces facteurs ne représente zéro dans R puisque le premier facteur ne représente pas zéro dans $\mathbf{R}_q$ et la deuxième dans $\mathbf{R}_{q'}$ (puisque $\left(\frac{l}{q}\right) = -1$ et $\left(\frac{l'}{q'}\right) = -1$). Comme exemple numtrique on a la forme

$$(x^2 + 3y^2 - 17z^2)\,(x^2 + 5y^2 - 7z^2).$$

Cet exemple peut sembler peu convaincant car la forme (22) est décomposée et on pourrait croire que c'est ce qui explique ce phénomène. Selmer a donné un exemple encore plus simple sans ce handicap (E. S. Selmer, The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 1951, 85, n° 3-4, 203-362). Il a montré en particulier que la forme $3x^3 + 4y^3 + 5z^3$ représente zéro dans tout corps $\mathbf{Q}_p$ de nombres p-adiques et dans le corps des réels mais ne représente pas zéro dans le corps des nombres rationnels. Le fait que cette forme représente zéro dans tous les corps $\mathbf{Q}_p$ est facile à démontrer (exercice 8, § 5). La non-représentabilité de zéro dans le corps des nombres rationnels est de démonstration plus délicate (cf. exercice 23, § 7, chap. 3).

L'analogue du théorème de Minkowski-Hasse pour des formes de degré supérieur n'est pas vrai même dans le cas où le nombre de variables est grand. Par exemple, la forme

$$(x_1^2 + \ldots + x_n^2)^2 - 2(y_1^2 + \ldots + y_n^2)^2$$

pour $n \geqslant 5$ représente zéro à la fois dans le corps des nombres réels et dans les corps p-adiques mais ne représente zéro dans le corps des nombres rationnels pour aucune valeur de n. On a le même résultat pour la forme

$$3(x_1^2 + \ldots + x_n^2)^3 + 4(y_1^2 + \ldots + y_n^2)^3 - 5(z_1^2 + \ldots + z_n^2)^3,$$

qui, elle, est absolument irréductible.

Dans les exemples ci-dessus, les formes introduites sont de degré pair. On ne connaît pas encore actuellement d'exemples de formes de degré impair possédant ces propriétés. On a donc émis la conjecture que l'analogue du théorème de Minkowski-Hasse est vrai pour les formes de degré impair d'un nombre assez grand de variables. Rappelons le théorème de Brauer : les formes d'un nombre suffisamment grand de variables représentent zéro

dans tous les corps de nombres p-adiques (nous avons déjà énonce ce théorème au § 6-5)); nous arrivons donc à la conjecture suivante :

Une forme rationnelle de degré impair et d'un nombre suffisamment grand de variables représente rationnellement zéro.

C'est à Artin que l'on doit la forme la plus précise de cette conjecture : une forme rationnelle de degré r impair à n variables représente zéro dans le corps des nombres rationnels si $n > r^2$.

Les exemples connus jusqu'à présent, de formes de degré pair, infirmant la conjecture d'Artin sont toutes obtenues par le même procédé, la substitution d'une forme dans un autre. Il est possible que la conjecture d'Artin soit vraie également pour les formes de degré pair en excluant les formes de ce type et les produits de ces formes.

L'unique résultat général vers la conjecture d'Artin est dû à Birch (B. J. Birch, Homogeneous forms of odd degree in a large number of variables. *Mathematika*, 1957, 4, nº 8, 102-105), qui a démontré qu'une forme de degré impair représente zéro dans le corps des nombres rationnels si le nombre de ses variables est suffisamment grand par rapport à son degré. La conjecture d'Artin n'est encore démontrée pour aucune valeur de r (sauf r = 2). Le cas le plus simple est relatif à r = 3 et affirme qu'une forme cubique de 10 variables représente zéro dans le corps des nombres rationnels.

EXERCICES

1. Demontrer le théorème suivant, dû à Legendre : si a, b, c sont des entiers rationnels premiers deux à deux, sans carrés et non tous de même signe, alors l'équation

$$ax^2 + by^2 + cz^2 = 0$$

admet une solution non nulle dans les nombres rationnels si et seulement si les trois congruences ci-dessous sont résolubles :

$$x^2 \equiv -bc \pmod{a};$$
$$x^2 \equiv -ca \pmod{b};$$
$$x^2 \equiv -ab \pmod{c}.$$

2. Les formes 3x* + $5y^2 - 7z^2$ et $3x^2 - 5y^2 - 7z^2$ représentent-elles zéro dans le corps des nombres rationnels ?

3. Quels sont les nombres premiers rationnels représentés par les formes x^2 + y*, $x^2 + 5y^2$, $x^2 - 5y^2$?

4. Donner une description de tous les nombres rationnels qui sont représentables par la forme $2x^2 - 5y^2$.

5. Quels sont les nombres rationnels qui sont représentés par la forme

$$2x^2 - 6y^2 + 15z^2 ?$$

6. Soit f une forme quadratique non singulière sur le corps des nombres rationnels, dont le nombre de variables n'est pas égal à 4. Montrer que f représente tous les nombres rationnels si et seulement si elle représente zéro.

7. Pour quels entiers rationnels à la forme $x^2 + 2y^2 - az^2$ représente-t-elle zéro dans le corps des nombres rationnels ?

8. Trouver toutes les solutions rationnelles de l'équation $x^2 + y^2 - 2z^2 = 0$.

9. On considère les formes

$$x^2 - 2y^2 + 5z^2, \qquad x^2 - y^2 + 10z^2, \qquad 3x^2 - y^2 + 30z^2;$$

quelles sont celles qui sont équivalentes entre elles sur le corps des nombres rationnels ?

10. Supposons que la forme $ax^2 + by^2 - z^2$, où a et b sont des entiers rationnels sans carré et $|a| > |b|$, représente zéro dans tous les corps de nombres p-adiques. Montrer qu'il existe alors des entiers rationnels a_1 et c tels que

$$aa_1 = c^2 - b, \qquad |a_1| < |a|$$

(l'égalité $aa_1 + b - c^2 = 0$ montre que la forme $aa_1x^2 + by^2 - z^2$ représente zéro rationnellement).

11. Considérant les formes du type $ax^2 + by^2 - z^2$, où a et b sont des entiers sans carres, démontrer le théorème de Minkowski-Hasse pour trois variables par récurrence sur le nombre $m = \max(|a|, |b|)$ (utiliser l'exercice 10 et l'exercice 3 du § 1 de l'appendice).

CHAPITRE II

REPRÉSENTATION DES NOMBRES RATIONNELS PAR DES FORMES DÉCOMPOSABLES

Nous avons étudié dans le chapitre précédent l'existence et la recherche des solutions rationnelles des équations. Ce chapitre est consacré à l'étude des solutions en nombres entiers. Nous commencerons par l'étude d'un exemple simple.

Considérons le problème de la recherche de toutes les solutions en nombres entiers de l'équation

$$x^2 - 2y^2 = 7. \tag{1}$$

Nous nous limiterons aux solutions $x > 0$, $y > 0$ (les autres s'obtiennent par changement de signe). L'équation admet les solutions $(3,1)$ et $(5,3)$. On peut obtenir à partir de ces deux solutions une infinité d'autres solutions, en effectuant la remarque suivante : si (x, y) est une solution de l'équation (1), alors, comme on le vérifie facilement $(3x + 4y, 2x + 3y)$ est encore une solution. Partant de la solution $(x_0, y_0) = (3, 1)$, nous obtenons ainsi une suite infinie (x_n, y_n) de solutions définies par les formules de récurrence

$$\begin{cases} x_{n+1} = 3x_n + 4y_n \\ y_{n+1} = 2x_n + 3y_n. \end{cases} \tag{2}$$

Partant de la solution $(x'_0, y'_0) = (5,3)$ nous obtenons par les mêmes formules une autre suite infinie (x'_n, y'_n) de solutions. On peut démontrer que ces deux suites épuisent toutes les solutions (x, y) de l'tquation (1) telles que

$$x > 0, \qquad y > 0.$$

Cette résolution élémentaire de l'équation (1) repose sur des formules et des calculs. Nous pouvons la relier à des notions plus générales et préparer ainsi le terrain pour des généralisations ultérieures.

Remarquons que la forme $x^2 - 2y^2$ est irréductible sur le corps Q des nombres rationnels mais se décompose en facteurs linéaires $(x + y\sqrt{2})$

$(x - y\sqrt{2})$ dans le corps plus grand $\mathbf{Q}(\sqrt{2})$. Si on utilise la notion de norme de l'extension $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ (voir appendice § 2-2)), l'équation (1) peut aussi s'écrire sous la forme

$$N(\xi) = N(x + y\sqrt{2}) = 7. \tag{3}$$

On est donc amené à rechercher dans le corps $\mathbf{Q}(\sqrt{2})$ les nombres

$$\xi = x + y\sqrt{2},$$

x, y entiers rationnels, dont la norme est égale à 7. Si la norme du nombre $\varepsilon = u + v\sqrt{2}$ (u, v entiers rationnels) est égale à 1, alors, d'après la multiplicativité de la norme tous les nombres de la forme $\xi\varepsilon^n$ satisfont en même temps que ξ à l'équation (3). Puisque $N(3 + 2\sqrt{2}) = 1$, nous pouvons prendre $\varepsilon = 3 + 2\sqrt{2}$. Le passage de ξ à $\xi\varepsilon$ correspond au passage de la solution (x, y) à la solution $(3x + 4y, 2x + 3y)$. Les deux suites infinies de solutions décrites par les formules récurrentes (2) peuvent alors s'écrire :

$$\left.\begin{aligned} x_n + y_n\sqrt{2} &= (3 + \sqrt{2})(3 + 2\sqrt{2})^n \\ x'_n + y'_n\sqrt{2} &= (5 + 3\sqrt{2})(3 + 2\sqrt{3})^n \end{aligned}\right\} \quad n \geqslant 0$$

La possibilité d'obtenir à partir d'une solution de l'équation (1) une infinité d'autres solutions repose sur l'existence de nombres $\varepsilon = u + v\sqrt{2}$, u, v entiers, tels que $N(\varepsilon) = 1$. Les nombres de cette forme sont à leur tour liés, comme nous allons le montrer, à la notion arithmétique fondamentale de nombre algébrique. Considérons l'ensemble de tous les nombres de la forme $x + y\sqrt{2}$, x, y entiers; cet ensemble forme un anneau que nous désignerons par $\mathfrak{D}$. L'arithmétique de cet anneau joue un grand rôle dans la suite; en particulier, ses unités, i. e. les nombres $a \in \mathfrak{D}$ tels que $a^{-1} \in \mathfrak{D}$. Il est facile de montrer qu'un nombre a est une unité de l'anneau $\mathfrak{D}$ si et seulement si $N(a) = \pm 1$. Cela donne une caractérisation très intéressante des nombres $\varepsilon \in \mathfrak{D}$ dont la norme est égale à 1 : ces nombres, réunis à ceux dont la norme est égale à -1, constituent toutes les unités de l'anneau $\mathfrak{D}$.

Dans ce chapitre, nous considérerons une théorie générale dont l'équation (1) constitue un des exemples les plus simples. Le succès obtenu dans la résolution de l'équation (1) repose sur le fait que la forme $x^2 - 2y^2$ est irréductible sur le corps des nombres rationnels mais se décompose en facteurs linéaires dans le corps $\mathbf{Q}(\sqrt{2})$ et par suite cette équation s'écrit sous la forme (3). Nous étudierons plus généralement les formes qui se décomposent en produit de formes linéaires dans une extension convenable du corps des nombres rationnels.

Bien que notre but ultime soit l'étude d'équations dont les coefficients et les solutions cherchées sont des nombres entiers, il convient de considérer le cas plus général de formes à coefficients rationnels. Les valeurs des variables seront par contre toujours supposées entières.

§ 1. — FORMES DÉCOMPOSABLES

1) Formes équivalentes sur Z

DÉFINITION. — ***Deux formes*** $F(x_1, \ldots, x_m)$ et $G(y_1, \ldots, y_l)$ à ***coefficients rationnels et de même degré n sont dites équivalentes sur*** Z ***si chacune d'elles peut être transformée en l'autre par une transformation linéaire des variables à coefficients entiers rationnels.***

Ainsi, les formes $x^2 + 7y^2 + z^2 - 6xy - 2xz + 6yz$ et $2u^2 - v^2$ sont équivalentes puisque, par les transformations linéaires,

$$\left.\begin{array}{l} x = 3v \\ y = u + v \\ z = -u + v \end{array}\right\} \quad \left\{\begin{array}{l} u = -x + 2y + z \\ v = x - y - z \end{array}\right.$$

elles sont transformées l'une de l'autre. Dans le cas de formes dépendant du même nombre de variables, la condition d'équivalence est qu'une des formes se transforme en l'autre par une transformation linéaire des variables de matrice unimodulaire (i. e. une matrice à coefficients entiers dont le déterminant est égal à ± 1).

Si les formes F et G sont équivalentes, alors connaissant toutes les solutions entières de $F = a$, nous obtenons facilement toutes les solutions entières de $G = a$ et *vice versa.* Ainsi, pour la recherche des solutions de l'équation $F = a$, on peut remplacer la forme F par une forme équivalente.

LEMME 1. — ***Toute forme de degré n est équivalente à une forme dans laquelle une des variables figure au*** $n^{\text{ième}}$ ***degré avec un coefficient non nul.***

DÉMONSTRATION. — Soit $F(x_1, \ldots, x_m)$ la forme de degré n. Montrons qu'il existe des nombres entiers rationnels $a_2, \ldots, a_m$ tels que

$$F(1, a_2, \ldots, a_m) \neq 0.$$

Nous procéderons par récurrence sur m. Pour $m = 1$, la forme F s'écrit Ax_1^n avec $A \neq 0$; par suite $F(1) \neq 0$. Supposons le lemme démontré pour les formes de m — 1 variables ($m \geqslant 2$). Écrivons la forme F :

$$F = G_0 x_m^n + G_1 x_m^{n-1} + \ldots + G_n,$$

oh $G_k(0 \leqslant k \leqslant n)$ est soit nul, soit une forme de degré k des variables $x_1, \ldots, x_{n-1}$ (nous considérons que les formes de degrés nuls sont des constantes différentes de zéro). Tous les G_k ne peuvent pas être nuls puisque F qui est une forme de degré n a au moins un coefficient non nul, Par récurrence, il existe des nombres entiers $a_2, \ldots, a_{m-1}$ tels que

$$G_k(1, a_2, \ldots a_{m-1}) \neq 0$$

pour au moins un indice k. Puisque le polynôme $F(1, a_2, \ldots, a_{m-1}, x_m)$ de la variable x_m n'est pas identiquement nul, prenant pour a, un nombre entier différent de ses racines, on aura $F(1, a_2, \ldots, a,) \neq 0$.

Effectuons maintenant la transformation linéaire suivante des variables :

$$\left.\begin{aligned} x_1 &= y_1 \\ x_2 &= a_2 y_1 + y_2 \\ &\vdots \\ x_m &= a_m y_1 + y_m \end{aligned}\right\}.$$

La forme F est transformée en la forme

$$G(y_1, \ldots, y_m) = F(y_1, a_2 y_1 + y_2, \ldots, a_m y_1 + y_m).$$

Puisque la matrice de notre transformation linéaire est entière et de déterminant égal à 1, les formes F et G sont équivalentes ; d'autre part, le coefficient de y_1^n est égal à

$$G(1, 0, \ldots, 0) = F(1, a_2, \ldots, a_m)$$

qui est non nul. Ainsi le lemme 1 est démontré.

2) Structure des formes décomposables

DÉFINITION. — ***Une forme*** $F(x_1, \ldots, x_m)$ ***à coefficients dans le corps Q des nombres rationnels est dite décomposable si elle se décompose en facteurs linéaires dans une extension*** $\Omega/\mathbf{Q}$.

Un tel exemple de forme décomposable est la forme

$$F(x, y) = a_0 x^n + a_1 x^{n-1} y + \ldots + a_n y^n,$$

de deux variables ($a_n \neq 0$). En effet, si Ω est un corps de décomposition du polynôme $F(x, 1)$ et $\alpha_1, \ldots, \alpha_n$ ses racines, alors on a dans Ω la décomposition

$$F(x, y) = a_0(x - \alpha_1 y) \ldots (x - \alpha_n y).$$

Parmi les formes quadratiques non singulières considérées dans le premier chapitre, les formes d'une ou deux variables sont décomposables (exercice 1).

Il est évident que, simultanément avec F, toutes les formes équivalentes sont aussi décomposables.

Dans la définition d'une forme décomposable, on ne précise pas dans quel corps Ω la forme se décompose en facteurs linéaires. Nous montrerons ici qu'on peut toujours prendre pour Ω une extension finie du corps Q des nombres rationnels. Cette question est liée de manière fondamentale à la théorie des extensions finies des corps. Les principales propriétés utiles ici des extensions finies des corps sont rappelées dans le § 2 de l'appendice.

DÉFINITION. — ***Les extensions finies du corps des nombres rationnels sont appelées corps de nombres algébriques et leurs éléments nombres algébriques.***

THÉORÈME 1. — ***Toute forme rationnelle décomposable est décomposable en facteurs linéaires dans un certain corps de nombres algébriques.***

DÉMONSTRATION. — D'après le lemme 1, nous pouvons supposer que la forme décomposable s'écrit

$$F = (\alpha_{11}x_1 + \ldots + \alpha_{1m}x_m) \ldots (\alpha_{n1}x_1 + \ldots + \alpha_{nm}x_m), \qquad \alpha_{ij} \in \Omega,$$

le coefficient de x_1^n étant non nul; ainsi, les coefficients α_{i1} $(1 \leqslant i \leqslant n)$ sont différents de zéro. Par suite, la forme peut s'écrire

$$F = A(x_1 + \beta_{12}x_2 + \ldots + \beta_{1m}x_m) \ldots (x_1 + \beta_{n2}x_2 + \ldots + \beta_{nm}x_m), \qquad (1)$$

avec $A = \alpha_{11} \ldots \alpha_{n1}$ et $\beta_{ij} = \alpha_{ij}\alpha_{i1}^{-1}$. Le nombre A qui est le coefficient de x_1^n est rationnel. Pour tout j $(2 \leqslant j \leqslant m)$, faisons $x_j - 1$ dans la dernière décomposition et donnons la valeur 0 à toutes les autres variables sauf x_1. Nous obtenons :

$$F(x_1, 0, \ldots, 1, \ldots, 0) = A(x_1 + \beta_{1j}) \ldots (x_1 + \beta_{nj}).$$

Puisque le terme de gauche est un polynôme de degré n à coefficients rationnels, les β_{ij} sont des nombres algébriques. Désignons par L le sous-corps du corps Ω obtenu à partir de Q par adjonction de tous les β_{ij}. L'extension L/Q est finie (cf. appendice § 2-1)), i. e. L est un corps de nombres algébriques.

Nous nous limiterons dans ce qui suit aux formes décomposables irréductibles sur le corps des nombres rationnels. Précisons la structure des formes décomposables irréductibles.

Considérons un corps K quelconque de nombres algébriques, de degré n, et un élément primitif θ du corps K sur Q, i. e. tel que $K = R(\theta)$ (cf. appendice § 2-3)). Le polynôme minimal $\varphi(t)$ du nombre θ sur le corps Q est de degré n. Construisons une extension L/K dans laquelle $\varphi(t)$ se décompose en facteurs linéaires :

$$\varphi(t) = (t - \theta^{(1)}) \ldots (t - \theta^{(n)}), \qquad \theta^{(1)} = \theta$$

(on peut supposer que $L = R(\theta^{(1)}, \ldots, \theta^{(n)})$). Pour tout nombre

$$a = f(\theta) \in K$$

(f(t) polynôme à coefficients rationnels), posons

$$\alpha^{(l)} = f(\theta^{(l)}) \in R(W) \subset L.$$

La norme $N(\alpha) = N_{K/Q}(\alpha)$ est alors donnée par la formule

$$N(a) = \alpha^{(1)}\alpha^{(2)} \ldots \alpha^{(n)}$$

(cf. appendice, § 2-3)).

Soient maintenant $\mu_1, \ldots, \mu_m$, m nombres non nuls du corps K. Ces nombres définissent la forme

$$F(x_1, \ldots, x_m) = \prod_{i=1}^{n} (x_1\mu_1^{(i)} + \ldots + x_m\mu_m^{(i)}) \qquad (2)$$

Puisque $\mu_k^{(i)} = f_k(\theta^{(i)})$ $(1 \leqslant k \leqslant m)$, $f_k(t)$ polynômes à coefficients rationnels, les coefficients de la forme (2) sont des fonctions symétriques de $\theta^{(1)}, \ldots, \theta^{(n)}$ et par suite s'expriment rationnellement en fonction des coefficients du polynôme $\varphi(t)$. Ainsi les coefficients de la forme (2) sont rationnels. Si nous substituons des nombres rationnels quelconques aux variables $x_1, \ldots, x_m$, alors, puisque

$$x_1\mu_1^{(i)} + \ldots + x_m\mu_m^{(i)} = (x_1\mu_1 + \ldots + x_m\mu_m)^{(i)},$$

le produit (2) est la norme du nombre $x_1\mu_1 + \ldots + x_n\mu_n$ (pour l'extension K/Q). Par suite, la forme (2) s'écrit

$$F(x_1, \ldots, x_m) = N(x_1\mu_1 + \ldots + x_m\mu_m). \qquad (3)$$

Une forme du type (2) n'est pas toujours irréductible. Ainsi, si on prend, dans le corps $Q(\sqrt{2}, \sqrt{3})$, $\mu_1 = \sqrt{2}$, $\mu_2 = \sqrt{3}$, la forme correspondante est $(2x_1^2 - 3x_2^2)^2$. Cependant, on a le théorème suivant.

THÉORÈME 2. — *Si les nombres $\mu_2, \ldots, \mu_m$ engendrent le corps K,* i. e. $K = Q(\mu_2, \ldots, \mu_m)$, *alors la forme*

$$F(x_1, \ldots, x_m) = N(x_1 + x_2\mu_2 + \ldots + x_m\mu_m) \qquad (4)$$

est irréductible (sur le corps des nombres rationnels). Inversement, toute forme irréductible décomposable est équivalente, à un facteur constant près, à une forme du type (4).

DÉMONSTRATION. — Supposons que

$$F = G \cdot H,$$

où les facteurs G et H sont à coefficients rationnels. Puisque dans l'anneau des polynômes à m variables, la décomposition en facteurs irréductibles est unique (à des facteurs constants près), chacune des formes linéaires

$$L_i = x_1 + x_2\mu_2^{(i)} + \ldots + x_m\mu_m^{(i)}$$

divise soit H soit G. Soit $L_1 = x_1 + x_2\mu_2 + \ldots + x_m\mu_m$ un diviseur de G, i. e.

$$G = L_1M_1.$$

Remplaçons dans cette dernière égalité tous les coefficients par leurs images dans l'isomorphisme $\alpha \to \alpha^{(i)}$ du corps $K = Q(\theta)$ sur le corps $Q(\theta^{(i)})$. Puisque les coefficients de la forme G sont rationnels, elle est invariante par cette substitution et nous obtenons l'égalité

$$G = L_iM_i;$$

ainsi G est divisible par L_i pour $i = 1, \ldots, n$ ($n = (K : Q)$).

Remarquons maintenant que l'isomorphisme $a \to \alpha^{(i)}$ $(a \in R(\mu_2, \ldots, \mu_m))$ est complètement défini par la donnée des images $\mu_2^{(i)}, \ldots, \mu_m^{(i)}$ des nombres $\mu_2, \ldots, \mu_m$. Il en résulte que les ensembles de nombres

$$\mu_2^{(i)}, \ldots, \mu_m^{(i)} \qquad (1 \leqslant i \leqslant n)$$

sont distincts (puisque les isomorphismes $a \to \alpha^{(i)}$ sont distincts); par suite, les formes $L_1, \ldots, L_n$ sont distinctes. Le coefficient de x_1 est égal à 1 pour toutes les formes L_i et par suite deux quelconques de ces formes ne sont pas proportionnelles. Utilisant à nouveau l'unicité de la décomposition, nous en concluons que G est divisible par le produit $L_1 \ldots L_n$, i. e. est divisible par F. Le facteur H est donc une constante et la première partie du théorème est démontrée.

Démontrons la réciproque. Soit $F^*(x_1, \ldots, x_m)$ une forme décomposable irréductible de degré n. D'après le lemme 1, on peut supposer que le coefficient de x_1^n est non nul; F* admet alors une décomposition du type (1), où les β_{ij} sont des nombres algébriques. Posons $\beta_{1j} = \mu_j$ $(2 \leqslant j \leqslant m)$ et considérons le corps $K = Q(\mu_2, \ldots, \mu_m)$; soit r le degré de cette extension. D'après ce qui précède, la forme

$$F = N(x_1 + x_2\mu_2 + \ldots + x_m\mu_m)$$

est irréductible et, par suite, un de ses facteurs linéaires

$$L_1 = x_1 + x_2\mu_2 + \ldots + x_m\mu_m$$

divise aussi la forme F*. Par suite, en transformant tous les coefficients de l'égalité $F^* = L_1M_1$ par l'isomorphisme $\alpha \to \alpha^{(i)}$ ($\alpha \in K$, $1 \leqslant i \leqslant r$), nous obtenons la décomposition $F^* = L_iM_i$. Comme nous l'avons vu, deux quelconques des formes $L_1, \ldots, L_r$ ne sont pas proportionnelles; ainsi, F^* est divisible par leur produit $L_1 \ldots L_r = F$. Puisque F^* est irréductible, on a donc $F^* = AF$, où A est une constante. Ceci termine la démonstration du théorème (on a démontré aussi que $r = n$).

3) Modules

Il est clair que la résolution en nombres entiers de l'équation

$$F(x_1, \ldots, x_m) = a,$$

où F est la forme (3), équivaut à la recherche dans le corps K des nombres 4 de la forme

$$\xi = x_1\mu_1 + \ldots + x_m\mu_m, \tag{5}$$

$x_1, \ldots, x_m$ entiers rationnels, tels que $N(E) = a$. Cela nous conduit à l'étude des nombres de la forme (5).

DÉFINITION. — *Soient* K *un corps de nombres algébriques et* $\mu_1, \ldots, \mu_m$ *un ensemble fini de nombres de* **K.** *L'ensemble* **M** *de toutes les combinaisons linéaires*

$$c_1\mu_1 + \ldots + c_m\mu_m$$

à coefficients c_i *entiers rationnels* ($1 \leqslant i \leqslant m$); *est appelé un module du corps* K. *Les nombres* $\mu_1, \ldots, \mu_m$ *sont appelés des générateurs du module* M.

Bien entendu, un même module M peut être défini par des systèmes distincts de générateurs. Si $\mu_1, \ldots, \mu_m$ est un système de générateurs du module M, on écrira $M = \{\mu_1, \ldots, \mu_m\}$.

Étudions le comportement de la forme (3), si on remplace $\mu_1, \ldots, \mu_m$ par un autre système de nombres $\rho_1, \ldots, \rho_l$ définissant le même module M. Nous avons

$$\rho_j = \sum_{k=1}^{m} c_{jk}\mu_k, \qquad (1 \leqslant j \leqslant l)$$

c_{jk} entiers. Soit

$$G(y_1, \ldots, y_l) = N(y_1\rho_1 + \ldots + y_l\rho_l).$$

Puisque

$$\sum_{i=1}^{l} y_j\rho_j = \sum_{k=1}^{m}\Big(\sum_{j=1}^{l} c_{jk}y_j\Big)\mu_k,$$

la forme F est transformée en G par la transformation linéaire

$$x_k = \sum_{j=1} c_{jk}\mu_j \qquad (1 \leqslant k \leqslant m).$$

Puisque les systèmes de générateurs μ_k et ρ_j du module M jouent un rôle symétrique, il existe aussi une transformation linéaire à coefficients entiers des variables transformant G en F. Ainsi, à des systèmes distincts de générateurs du même module M correspondent des formes équivalentes i. e. à tout module du corps K correspond une classe de formes décomposables équivalentes.

Pour tout module $M = \{\mu_1, \ldots, \mu_m\}$ et $\alpha \in K$, nous désignerons par αM l'ensemble de tous les produits $\alpha\xi$, ξ parcourant M. Il est évident que αM coïncide avec l'ensemble des combinaisons linéaires à coefficients entiers des nombres $\alpha\mu_1, \ldots, \alpha\mu_m$, i. e. $\alpha M = \{\alpha\mu_1, \ldots, \alpha\mu_m\}$.

DÉFINITION. — ***Deux modules*** M ***et*** M_1 ***d'un corps*** K ***de nombres algébriques sont dits semblables si*** $M_1 = \alpha M$ ***pour un certain élément*** $\alpha \neq 0$ ***de*** K.

Des formes correspondant à des modules semblables M et αM diffèrent entre elles seulement par le facteur constant N(u). C'est pourquoi, si on considère les formes à un facteur constant près, on peut toujours remplacer M par un module semblable; ainsi, on peut supposer qu'un des générateurs du module, disons μ_1, est égal à 1. Ce qui précède permet de formuler ainsi le problème de la représentation des nombres par des formes décomposables irréductibles. Si la forme F est écrite

$$F(x_1, \ldots, x_m) = AN(x_1\mu_1 + \ldots + x_m\mu_m)$$

(après avoir choisi le corps K), la résolution en nombres entiers de l'équation $F(x_1, \ldots, x_m) = a$ est équivalente à la recherche dans le module

$$M = \{\mu_1, \ldots, \mu_m\}$$

de tous les nombres α dont la norme N(u) est égale au nombre rationnel $\frac{a}{A}$. Nous nous occuperons donc dans la suite de la recherche, dans un module donné, des nombres dont la norme est un nombre donné. Comme nous l'avons vu, ce problème est équivalent à la recherche dans tout module semblable μM des nombres de norme $N(\mu)\frac{a}{A}$; ainsi on peut remplacer le module donné par tout module semblable.

Si le degré d'un corps de nombres algébriques K est égal à n, tout module M de K contient au plus n nombres linéairement indépendants (sur le corps $\mathbf{Q}$).

DÉFINITION. — ***Si le module*** M ***d'un corps de nombres algébriques*** K ***de degré n contient n nombres linéairement indépendants (sur le corps des nombres rationnels), il est dit complet et incomplet dans le cas contraire. Les formes décomposables liées au module*** M ***seront simultanément dites complètes ou incomplètes.***

Par exemple, si le nombre entier rationnel d n'est pas un cube, les nombres 1, $\sqrt[3]{d}$, $\sqrt[3]{d^2}$ forment une base du corps $Q(\sqrt[3]{d})$ sur Q ; par suite, la forme

$$N(x + y\sqrt[3]{d} + z\sqrt[3]{d^2}) = x^3 + dy^3 + d^2z^3 - 3dxyz$$

est complète. Comme exemple de forme incomplète, on peut prendre

$$N(x + y\sqrt[3]{d}) = x^3 + dy^3.$$

Si $\{1, \mu_2, \ldots, \mu_m\}$ est un module complet du corps K, alors il est clair que $K = \mathbf{Q}(\mu_2, \ldots, \mu_m)$. D'après le théorème 1, il en résulte facilement que toute forme complète est irréductible.

La question de la représentation des nombres par des formes irréductibles incomplètes est très compliquée et on ne connaît pas actuellement de théorie générale satisfaisante. Nous en étudierons un cas particulier dans le chapitre IV.

Le problème de la représentation des nombres rationnels par des formes complètes est entièrement résolu et nous l'étudierons dans ce chapitre. Comme nous l'avons remarqué, ce problème est équivalent à la recherche de tous les nombres de norme donnée appartenant à un module donné d'un corps K de nombres algébriques.

EXERCICES

1. Démontrer qu'une forme quadratique rationnelle est décomposable si et seulement si son rang est $\leqslant 2$.

2. Demontrer que la forme liée à un module quelconque d'un corps K de nombres algébriques est une puissance d'une forme irréductible.

3. Démontrer que dans le corps $\mathbf{Q}$ des nombres rationnels, tout module est de la forme $a\mathbf{Z}$, avec $a \in \mathbf{Q}$ ($\mathbf{Z}$ est l'anneau de tous les nombres entiers rationnels).

§ 2. — LES MODULES COMPLETS ET LEURS ANNEAUX DE STABILISATEURS

1) Base d'un module

DÉFINITION. — ***Un système de générateurs $\alpha_1, \ldots, a_{,,,}$ d'un module M est appelé une base s'il est linéairement indépendant sur l'anneau des nombres entiers,*** i. ***e. si l'égalité***

$$a_1\alpha_1 + \ldots + a_m\alpha_n = 0, \qquad a_i \in \mathbf{Z}$$

entraîne $a_i = 0$ pour tout i.

Il est évident que si $\alpha_1, \ldots,$ a, est une base du module M, alors tout nombre $a \in$ M admet une représentation et une seule du type

$$a = c_1\alpha_1 + \ldots + c_m\alpha_m, \qquad c_i \in \mathbf{Z}. \tag{1}$$

Montrons pour commencer que tout module admet une base. La démonstration n'utilise pas le fait que les éléments du module appartiennent à un corps de nombres algébriques mais seulement les faits suivants : pour l'addition, un module est un groupe abélien dont aucun élément n'est d'ordre fini et dont tout élément s'exprime comme une combinaison linéaire à coefficients entiers d'un nombre fini d'éléments (existence d'un système de générateurs). Nous démontrerons donc ce résultat dans le cadre des groupes abéliens. Nous utiliserons la terminologie suivante. Nous dirons que des éléments $\alpha_1, \ldots, \alpha_m$ d'un groupe abélien M (en notation additive) forment un système de générateurs si tout élément a $\in$ M s'écrit sous la forme (1); nous écrirons alors M = $\{\alpha_1, \ldots, \alpha_m\}$. Si le système $\alpha_1, \ldots,$ a,,, satisfait à la définition donnée ci-dessus, nous dirons que c'est une base du groupe M.

THÉORÈME 1. — ***Si un groupe abélien dont aucun élément n'est d'ordrejïni possède un système fini de générateurs, alors il possède une base.***

DÉMONSTRATION. — Désignons par $\alpha_1, \ldots, \alpha_s$ un système de générateurs du groupe M. Remarquons tout d'abord que si nous ajoutons à un de ces générateurs le produit d'un autre générateur par un nombre entier quelconque, le nouveau système d'éléments est encore un système de générateurs. En effet, soit par exemple, $\alpha_1' = \alpha_1 + k\alpha_2$. Alors, pour tout a $\in$ M, nous avons

$$a = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_s\alpha_s = c_1\alpha_1' + (c_2 - kc_1)\alpha_2 + \ldots + c_s\alpha_s,$$

oh tous les coefficients sont entiers; ainsi M = $\{\alpha_1', \alpha_2, \ldots, a, \}$.

Si les éléments $\alpha_1, \ldots, a$, sont linéairement indépendants, alors c'est une base de M. Supposons qu'ils soient linéairement dépendants, i. e. il existe des entiers c_i non tous nuls tels que :

$$c_1\alpha_1 + c_2\alpha_2 + \ldots + c_s\alpha_s = 0. \tag{2}$$

Choisissons parmi les coefficients c_i non nuls un de ceux dont la valeur absolue est minimum, disons c_1. Considérons tout d'abord le cas où c_1 ne divise pas un des autres coefficients, disons c_2 et posons

$$c_2 = c_1q + c', \qquad 0 < c' < |c_1|.$$

Si nous prenons pour nouveau système de générateurs

$$\alpha_1' = \alpha_1 + q\alpha_2, \alpha_2, \ldots, \alpha_s,$$

la relation (2) devient

$$c_1\alpha_1' + c'\alpha_2 + \ldots + c_s\alpha_s = 0,$$

avec $0 < c' < |c_1|$. Ainsi, si des générateurs $\alpha_1, \ldots, a$, sont liés par la relation non triviale (2) dans laquelle un des plus petits coefficients en valeur absolue ne divise pas un des autres, il existe un autre système de générateurs liés par une relation non triviale à coefficients entiers pour laquelle le plus petit coefficient (non nul) en valeur absolue est strictement inférieur (en valeur absolue) au coefficient correspondant de la relation (2) initiale, Au bout d'un nombre fini d'opérations nous obtenons un système de générateurs $\beta_1, \ldots, \beta_s$ tels que

$$k_1\beta_1 + k_2\beta_2 + \ldots + k_s\beta_s = 0, \tag{3}$$

les k_i étant des nombres entiers tels que l'un d'eux, soit par exemple k_1, divise tous les autres. Divisant la relation (3) par k_1 (c'est possible puisque, par hypothèse, 0 est le seul élément d'ordre fini de M), nous obtenons alors

$$\beta_1 + l_2\beta_2 + \ldots + l_s\beta_s = 0, \tag{4}$$

pour des entiers $l_2, \ldots, l_s$. Par suite, on peut exclure β_1 du système de générateurs considéré, i. e. $M = \{\beta_2, \ldots, \beta_s\}$.

On a donc démontré que si un système de générateurs de M est linéairement dépendant, on peut trouver un nouveau système de générateurs contenant un élément de moins. Répétant ce raisonnement, nous obtenons finalement un système de générateurs linéairement indépendants qui est donc une base du groupe M.

COROLLAIRE. — ***Tout module dans un corps K de nombres algébriques admet une base.***

Le nombre m d'éléments d'une base d'un module M est égal, c'est clair,

au nombre maximum d'éléments de M linéairement indépendants (sur Q). Par suite, ce nombre m est le même pour toutes les bases et s'appelle le rang du module M. Le rang du module réduit à 0 est égal à 0.

Soient $\omega_1, \ldots, \omega_m$ et $\omega'_1, \ldots, \omega'_m$ deux bases d'un module M de rang m. Il est clair que la matrice C de passage de la première base à la seconde est à coefficients entiers. Par symétrie, la matrice de passage de la deuxième base à la première, i. e. la matrice C^{-1}, est également à coefficients entiers. Par suite $\det C = \pm 1$. Nous obtenons ainsi que la matrice de passage d'une base d'un module de rang m à une autre base est une matrice unimodulaire de rang m.

Si le degré du corps K/Q est égal à n, le rang de tout module de K ne dépasse pas n. Il est évident que le rang d'un module est égal à n si et seulement si ce module est complet. Ainsi, les modules incomplets sont caractérisés par le fait que leur rang est strictement plus petit que le degré n du corps.

Tout système de générateurs d'un module de rang m contient au moins m éléments. Il en résulte que parmi les formes liées à ce module il existe des formes à m variables mais il n'existe pas de formes d'un plus petit nombre de variables. Les formes complètes de degré n peuvent donc être définies comme étant les formes décomposables irréductibles qui ne sont équivalentes à aucune forme de moins de n variables.

THÉORÈME 2. — *Soit* M *un groupe abélien sans élément d'ordre fini et possédant un nombre fini de générateurs. Tout sous-groupe N a alors aussi un nombre fini de générateurs et par suite possède une base. Pour toute base* $\omega_1, \ldots, \omega_m$ *du groupe* M *(ordonnée de manière convenable), il existe une base du groupe N de la forme*

$$\left.\begin{aligned} \eta_1 &= c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1k}\omega_k + \ldots + c_{1m}\omega_m \\ \eta_2 &= \quad c_{22}\omega_2 + \ldots + c_{2k}\omega_k + \ldots + c_{2m}\omega_m \\ &\vdots \\ \eta_k &= \quad + c_{kk}\omega_k + \ldots + c_{km}\omega_m \end{aligned}\right\}$$

où les c_{ij} *sont des entiers,* $c_{ii} > 0$, $k \leqslant m$.

DÉMONSTRATION. — Nous démontrerons le théorème par récurrence sur le rang m du groupe N, i. e. sur le nombre d'éléments d'une base. Pour $m=0$, le théorème est trivial. Soit $m \geqslant 1$. Si N est réduit à $\{0\}$, alors $k = 0$ et le théorème est démontré. Soit maintenant $\alpha \in N$, $\alpha \neq 0$; on a

$$\alpha = c_1\omega_1 + \ldots + c_m\omega_m \tag{5}$$

où un au moins des coefficients c_i n'est pas nul; changeant éventuellement l'ordre des éléments de la base, nous pouvons supposer $c_1 \neq 0$. Si $c_1 < 0$,

alors le coefficient de — a relatif à ω_1 est positif. Choisissons dans le groupe N un élément

$$\eta_1 = c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1m}\omega_m,$$

dont le coefficient c_{11} relatif à ω_1 soit > 0 et le plus petit possible.

Pour tout $a \in$ N, le coefficient c_1 est divisible par c_{11}; en effet, si

$$c_1 = q c_{11} + c', \qquad 0 \leqslant c' < c_{11} \qquad (q \text{ entier}),$$

alors l'élément $a - q\eta_1$ s'écrit

$$a - q\eta_1 = c'\omega_1 + c'_2\omega_2 + \ldots + c'_m\omega_m,$$

d'où $c' = 0$ d'après la minimalité de c_{11}. Considérons maintenant dans M le sous-groupe $\mathbf{M}_0 = \{\omega_2, \ldots, \omega_m\}$. Puisque l'intersection $\mathbf{M}_0 \cap$ N est un sous-groupe du groupe $\mathbf{M}_0$, alors, par hypothèse de récurrence, il existe une base de $\mathbf{M}_0 \cap$ N de la forme

$$\left.\begin{aligned} \eta_2 &= c_{22}\omega_2 + c_{23}\omega_3 + \ldots + c_{2k}\omega_k + \ldots + c_{2m}\omega_m \\ \eta_3 &= \quad c_{33}\omega_3 + \ldots + c_{3k}\omega_k + \ldots + c_{3m}\omega_m \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_k &= \quad c_{kk}\omega_k + \ldots + c_{km}\omega_m \end{aligned}\right\}$$

oh les c_{ij} sont des entiers, $c_{ii} > 0$, $k - 1 \leqslant m - 1$ (pour un ordre convenable des éléments $\omega_2, \ldots, \omega_m$). Démontrons que N est l'ensemble des combinaisons linéaires à coefficients *entiers* des éléments $\eta_1, \eta_2, \ldots, \eta_k$. Soit a un élément quelconque de N. Si on le représente sous la forme (5), alors, d'après ce qui a été démontré, $c_1 = c_{11}q_1$, q_1 entier et par suite

$$a - q_1\eta_1 = c'_2\omega_2 + \ldots + c'_m\omega_2$$

appartient à l'intersection $\mathbf{M}_0 \cap$ N. D'après l'hypothèse de récurrence, nous avons

$$\alpha - q_1\eta_1 = q_2\eta_2 + \ldots + q_k\eta_k$$

q entiers, d'où $a = q_1\eta_1 + \ldots + q_k\eta_k$. Cela démontre que

$$\mathbf{N} = \{\eta_1, \eta_2, \ldots, \eta_k\}.$$

Les générateurs $\eta_1, \ldots, \eta_k$ étant linéairement indépendants sur $\mathbf{Z}$, comme il est facile de le voir, forment la base de N cherchée.

La démonstration ci-dessus du théorème 2 utilise la méthode de Gauss pour éliminer des inconnues dans les systèmes d'équations linéaires, avec des modifications dues au fait que les coefficients n'appartiennent pas à un corps mais à l'anneau $\mathbf{Z}$ des nombres entiers.

COROLLAIRE. — ***Tout sous-groupe N d'un module*** M ***d'un corps*** K ***de nombres algébriques est encore un module (sous-module du module*** M).

2) Anneaux de stabilisateurs

DÉFINITION. — ***Un nombre*** α ***d'un*** corps K ***de nombres algébriques est appelé un stabilisateur d'un module complet*** M ***du corps*** K ***si*** $\alpha M \subset M$, i. e. ***si pour tout*** $\xi \in M$ ***le produit*** $\alpha\xi$ ***appartient aussi à M.***

L'ensemble $\mathfrak{D}_M$ de tous les stabilisateurs du module M est un anneau. En effet, si $\alpha, \beta \in \mathfrak{D}_M$, nous avons, pour tout $\xi \in M$:

$$(\alpha - \beta)\xi = \alpha\xi - \beta\xi \in M$$

et $(\alpha\beta)\xi = \alpha(\beta\xi) \in M$, i. e. $\alpha - \beta \in \mathfrak{D}_M$ et $\alpha\beta \in \mathfrak{D}_M$. L'anneau $\mathfrak{D}_M$ est appelé ***l'anneau des stabilisateurs du module complet*** M. Puisque $1 \in \mathfrak{D}_M$, $\mathfrak{D}_M$ est un anneau avec unité.

Pour savoir si un nombre donné $\alpha \in K$ appartient à l'anneau $\mathfrak{D}_M$, il n'est pas nécessaire de vérifier que le produit $\alpha\xi$ appartient à M pour tout $\xi \in M$; il suffit de vérifier cette propriété pour les éléments d'une base $\mu_1, \ldots, \mu_n$ du module M. En effet, si $\alpha\mu_i \in M$ pour tout $i = 1, \ldots, n$, alors pour tout $\xi = c_1\mu_1 + \ldots + c_n\mu_n \in M$, on aura

$$\alpha\xi = c_1(\alpha\mu_1) + \ldots + c_n(\alpha\mu_n) \in M.$$

Démontrons que l'anneau des stabilisateurs $\mathfrak{D}_M$ est un module complet de K. Soit y un nombre non nul de M; puisque $\alpha\gamma \in M$ pour tout $a \in \mathfrak{D}_M$, alors $\gamma\mathfrak{D}_M \subset M$. L'ensemble $\gamma\mathfrak{D}_M$ est un groupe pour l'addition; par suite, d'après le corollaire du théorème 2, $\gamma\mathfrak{D}_M$ est un module. Mais alors

$$\mathfrak{D}_M = \gamma^{-1}(\gamma\mathfrak{D}_M)$$

est aussi un module. 11 reste à montrer que ce module est complet. Soit a un nombre non nul de K et désignons par c le dénominateur commun de tous les nombres rationnels a_{ij} définis par la décomposition

$$\alpha\mu_i = \sum_{j=1}^{n} a_{ij}\mu_j \qquad (1 \leqslant i \leqslant n). \tag{6}$$

Puisque les produits ca_{ij} sont entiers, alors $c\alpha\mu_i \in M$; ainsi, $c\alpha \in \mathfrak{D}_M$. Soit mamtenant $\alpha_1, \ldots, a$, une base du corps K; d'après ce qui précède, il existe des entiers rationnels $c_1, \ldots, c_n$ tels que les produits $c_1\alpha_1, \ldots, c_n\alpha_n$ soient contenus dans $\mathfrak{D}_M$. Ainsi, il existe n nombres linéairement indépendants dans $\mathfrak{D}_M$ et par suite $\mathfrak{D}_M$ est un module complet.

DÉFINITION. — ***Un module*** complet ***d'un*** *corps* K ***de nombres algébriques qui est un sous-anneau de*** K ***contenant le nombre*** 1 ***est appelé un ordre du corps*** K.

Avec cette définition, les résultats que nous venons d'obtenir peuvent s'énoncer sous la forme suivante

THÉORÈME 3. *-L'anneau des stabilisateurs d'un module complet d'un corps de nombres algébriques est un ordre de ce corps.*

La réciproque est vraie : tout ordre $\mathfrak{D}$ du corps K est l'anneau des stabilisateurs d'un certain module complet, par exemple lui-même (puisque $1 \in \mathfrak{D}$, l'inclusion $\alpha\mathfrak{D} \subset \mathfrak{D}$ est équivalente à $a \in \mathfrak{D}$). On dira qu'un module complet M est *associé* à un ordre $\mathfrak{D}$ s'il admet cet ordre pour anneau de stabilisateurs.

Pour un nombre $y \neq 0$ de K, la condition $\alpha\xi \in M$ équivaut à la condition $\alpha(\gamma\xi) \in \gamma M$ (ici $\xi \in M$); il en résulte que des modules semblables M et γM ont le même anneau de stabilisateurs i. e.

$$\mathfrak{D}_{\gamma M} = \mathfrak{D}_M.$$

Soient $\mu_1, \ldots, \mu_n$ une base du module M et $\omega_1, \ldots, \omega_n$ une base de son anneau de stabilisateurs 9,. Pour tout $i = 1, \ldots, n$, nous avons

$$\mu_i = \sum_{j=1}^{n} b_{ij}\omega_j,$$

où les b_{ij} sont des nombres rationnels. Si b est le dénominateur commun de tous les coefficients b_{ij}, les nombres $b\mu_i$ s'expriment comme combinaisons linéaires à coefficients entiers des nombres de la base de l'ordre $\mathfrak{D}_M$, i. e. appartiennent à $\mathfrak{D}_M$. Le module $b\mathbf{M}$ vérifie donc l'inclusion $b\mathbf{M} \subset \mathfrak{D}_M$.

Formulons les résultats obtenus.

LEMME 1. — *Les anneaux de stabilisateurs de deux modules complets semblables coïncident. Pour tout module complet, il existe un module semblable qui est contenu dans son anneau de stabilisateurs.*

3) unités

Revenons à l'étude des représentations entières des nombres rationnels par des formes décomposables complètes.

Dans le § 1-3), nous avons vu que cela revient à chercher dans un module complet M les nombres μ tels que

$$N(\mu) = a. \tag{7}$$

Pour tout ω de l'anneau de stabilisateurs $\mathfrak{D} = \mathfrak{D}_M$, le produit $\omega\mu$ appartient à M, d'où, d'après la multiplicativité de la norme,

$$N(\omega\mu) = N(\omega)a.$$

Si $N(\omega) = 1$, le produit $\omega\mu$ est, de même que μ, une solution de l'équation (7). Ainsi, les stabilisateurs ω dont la norme est égale à 1 permettent d'obtenir une classe de nouvelles solutions de l'équation (7) à partir d'une solution particulière. Ce fait est à la base de la méthode de résolution de l'équation (7) que nous allons exposer.

Démontrons que les nombres $\omega \in \mathfrak{D}$ tels que $N(w) = 1$ doivent être cherchés parmi les nombres ε de l'anneau $\mathfrak{D}$ tels que $\varepsilon^{-1} \in \mathfrak{D}$. Ces nombres ε sont appelés des ***unités*** de l'anneau $\mathfrak{D}$ (cf. appendice § 4-l)). Puisque les inclusions $EM \subset M$ et $\varepsilon^{-1}M \in M$ équivalent à l'égalité $EM = M$, les unités de l'anneau $\mathfrak{D} = \mathfrak{D}_M$ sont les nombres $\alpha \in K$ tels que $\alpha M = M$.

LEMME *2.* — ***Pour tout nombre α appartenant à un ordre $\mathfrak{D}$, les polynômes caractéristique et minimal de a sont à coefficients entiers. En particulier, la norme $N(a) = N_{K/Q}(\alpha)$ et la trace $Tr\ (a) = Tr_{K/Q}(\alpha)$ sont des nombres rationnels.***

DÉMONSTRATION. — Soit un ordre $\mathfrak{D}$ qui est l'anneau de facteurs d'un module $M = \{\mu_1, \ldots, \mu_n\}$ (on peut prendre par exemple $M = \mathfrak{D}$). Si $\alpha \in \mathfrak{D}$, alors les coefficients a_{ij} dans l'égalité (6) sont des entiers et par suite le polynôme caractéristique du nombre a (pour l'extension K/Q) est à coefficients entiers. Le reste du lemme est trivial.

THÉORÈME 4. — ***Soit $\mathfrak{D}$ un ordre quelconque d'un corps K de nombres algébriques. Pour qu'un nombre $\varepsilon \in \mathfrak{D}$ soit une unité de l'anneau $\mathfrak{D}$, il faut et il suffit que $N(\varepsilon) = \pm 1$.***

DÉMONSTRATION. — Montrons tout d'abord que la norme *N(a)* de tout $a \in \mathfrak{D}$, $a \neq 0$, est divisible par a dans l'anneau $\mathfrak{D}$. D'après le lemme 2, le polynôme caractéristique $\varphi(t) = t^n + c_1 t^{n-1} + \ldots + c_n$ du nombre a est à coefficients entiers; puisque $\varphi(\alpha) = 0$, alors

$$\frac{N(\alpha)}{a} = \frac{(-1)^n c_n}{\alpha} = (-1)^{n-1}(\alpha^{n-1} + c_1\alpha^{n-2} + \ldots + c_{n-1}).$$

Le quotient $\frac{N(\alpha)}{\alpha}$ appartient ainsi à $\mathfrak{D}$ et cela signifie que ***N(a) est*** divisible par ***a*** dans $\mathfrak{D}$.

Si maintenant $N(a) = \pm 1$, alors 1 est divisible par ***a***, i. e. a est une unité de l'anneau $\mathfrak{D}$. Réciproquement, si ε est une unité de l'anneau $\mathfrak{D}$, i. e. $\varepsilon\varepsilon' = 1$ pour un certain $\varepsilon' \in \mathfrak{D}$, alors, puisque $N(E)$ et $N(E')$ sont entiers, l'égalité $N(E)N(E') = 1$ entraîne $N(E) = \pm 1$. Le théorème 4 est démontré.

La recherche des stabilisateurs $\omega \in \mathfrak{D}$ tels que $N(\omega) = 1$ revient à caractériser parmi toutes les unités de $\mathfrak{D}$ celles dont la norme est égale à $+1$.

Deux nombres μ_1 et μ_2 d'un module complet M sont dits ***associés*** si leur

quotient $\frac{\mu_1}{\mu_2} = \varepsilon$ est une unité de l'anneau de stabilisateurs $\mathfrak{D} = \mathfrak{D}_M$. Il est clair que si M = $\mathfrak{D}$, cette notion coïncide avec la notion habituelle d'éléments associés dans un anneau commutatif unitaire (cf. appendice § 4-l)). On voit facilement que cette relation possède les propriétés habituelles des relations d'équivalence; ainsi toutes les solutions de l'équation (7) sont décomposables en classes de solutions associées. Si μ_1 et μ_2 sont deux solutions associées, i. e. $\mu_1 = \mu_2\varepsilon$, oh ε est une unité de l'anneau $\mathfrak{D}$, alors N(E) = 1. Réciproquement, pour toute unité ε de $\mathfrak{D}$ de norme + 1 et toute solution μ, le produit $\mu\varepsilon$ et μ sont des solutions associées. Ainsi, toutes les solutions d'une même classe de solutions associées sont obtenues à partir de l'une d'entre elles par multiplication par toutes les unités de norme + 1. Nous allons montrer que le nombre de ces classes de solutions est fini.

THÉOREME 5. — *Dans tout ordre $\mathfrak{D}$, il existe seulement un nombre fini d'éléments non associés deux à deux ayant pour norme un nombre donné.*

DÉMONSTRATION. — Soient $\omega_1, \ldots, \omega_n$ une base de l'ordre $\mathfrak{D}$ et $c > 1$ un entier naturel donné. En liaison avec la définition de l'appendice § 4-1), nous dirons que deux nombres α et β de $\mathfrak{D}$ sont congrus modulo c si la différence $\alpha - \beta$ est divisible par c (dans l'anneau $\mathfrak{D}$). Il est évident que tout $\alpha \in \mathfrak{D}$ est congru modulo c à un et un seul des nombres

$$x_1\omega_1 + \ldots + x_n\omega_n, \qquad 0 \leqslant x_i < c \qquad (1 \leqslant i \leqslant n).$$

Tous les nombres de $\mathfrak{D}$ se repartissent donc en c^n classes de nombres congrus entre eux modulo c. Soient maintenant α et β deux nombres appartenant à la même classe et tels que $|N(\alpha)| = |N(\beta)| = c$; de l'égalité $\alpha - \beta = cy$, $y \in \mathfrak{D}$, résulte que $\frac{\alpha}{\beta} = 1 \pm \frac{N(\beta)}{\beta} y \in \mathfrak{D}$ $\left(\text{car } \frac{N(\beta)}{\beta} \in \mathfrak{D}, \text{ cf. le début de la}\right.$ démonstration du théorème 4) et de même $\frac{\beta}{\alpha} = 1 \pm \frac{N(\alpha)}{\alpha} y \in \mathfrak{D}$. Ainsi les nombres α et β sont divisibles l'un par l'autre et cela signifie qu'ils sont associés dans l'anneau $\mathfrak{D}$. Cela démontre qu'il existe dans $\mathfrak{D}$ au plus c^n nombres non associés deux à deux dont la valeur absolue de la norme est égale à un nombre donné c.

COROLLAIRE. — *Parmi les nombres de norme donnée d'un module complet* M *d'un corps K, il existe seulement un nombre fini de nombres non associés deux à deux.*

En effet, soit $\mathfrak{D}$ l'anneau des stabilisateurs du modulo M. Alors pour un certain entier b, le module $b\mathfrak{M}$ est contenu dans $\mathfrak{D}$. Si $\gamma_1, \ldots, \gamma_k$ sont des nombres de M de norme c et non associés deux à deux, alors les nombres $b\gamma_1, \ldots, b\gamma_k$ de $\mathfrak{D}$ sont de norme $b^n c$ et ne sont pas associés deux à deux dans $\mathfrak{D}$. Le nombre k ne peut donc pas être arbitrairement grand.

Remarque. — La démonstration du théorème 5 montre que dans l'anneau $\mathfrak{D}$ (et aussi dans le module M) il existe un ensemble fini de nombres de norme donnée c tel que tout nombre de $\mathfrak{D}$ (ou de M) de norme c soit associé à l'un d'entre eux. Cependant cette démonstration ne permet pas de trouver effectivement ces nombres mais donne seulement une majoration de la quantité de ces nombres.

Le problème fondamental de la recherche de toutes les solutions de l'équation (7) est ainsi ramené aux deux problèmes suivants :

1° trouver dans l'anneau $\mathfrak{D}$ toutes les unités ε de norme $N(\varepsilon) = +1$;

2° trouver dans le module M des nombres $\mu_1, \ldots, \mu_k$ de norme a, non associés deux à deux, et tels que tout $\mu \in M$ de norme a soit associé à l'un d'entre eux, i. e. soit de la forme $\mu = \mu_i \varepsilon$ pour un i, $1 \leqslant i \leqslant k$ et ε unité de l'anneau $\mathfrak{D}$.

Si nous résolvons ces deux problèmes nous aurons également résolu le problème de la représentation entière des nombres rationnels par des formes décomposables complètes.

4) Ordre maximum

Dans le point 2), nous avons introduit la notion d'ordre. Il est naturel de chercher à comparer les différents ordres d'un même corps K de nombres algébriques. Nous montrerons ici qu'il existe dans le corps K un ordre maximum contenant tous les autres ordres. D'après le lemme 2, le polynôme minimal de tout nombre appartenant à un ordre quelconque est à coefficients entiers. Nous montrerons ci-dessous (théorème 6) que l'ordre maximum du corps K est égal à l'ensemble $\tilde{\mathfrak{D}}$ de tous les nombres de K dont le polynôme minimal est à coefficients entiers.

LEMME 3. — ***Si*** $\alpha \in \tilde{\mathfrak{D}}$, i. ***e. si le polynôme minimal*** $t^m + c_1 t^{m-1} + \ldots + c_n$ ***du nombre a est à coefficients entiers, alors le module*** $M = \{1, a, \ldots, \alpha^{m-1}\}$ ***est un anneau.***

DÉMONSTRATION. — Il est clair qu'il suffit de démontrer que toutes les puissances α^k, $k \geqslant 0$, du nombre a appartiennent à M. Par définition de M, c'est vrai pour $k \leqslant m-1$; de plus, $\alpha^m = -c_1\alpha^{m-1} - \ldots - c_m$, c_i ***entiers,*** et par suite $\alpha^m \in M$. Soit $k > m$ et supposons que l'on ait démontré que $\alpha^{k-1} \in M$ i. e. $\alpha^{k-1} = a_1\alpha^{m-1} + \ldots + a_m$, a_i entiers ; alors

$$\alpha^k = \alpha\alpha^{k-1} = a_1\alpha^m + a_2\alpha^{m-1} + \ldots + a_m\alpha.$$

Puisque tous les termes de la somme de droite appartiennent à M, alors $\alpha^k \in M$. Le lemme 3 est démontré .

LEMME 4. — *Si $\mathfrak{D}$ est un ordre quelconque du corps* K *et $a \in \tilde{\mathfrak{D}}$, alors l'anneau $\mathfrak{D}[\alpha]$ de tous les polynômes en α à coefficients dans $\mathfrak{D}$ est un ordre du corps* K.

DÉMONSTRATION. — Puisque $\mathfrak{D} \subset \mathfrak{D}[\alpha]$, alors dans l'anneau $\mathfrak{D}[\alpha]$ il existe $n = (K : R)$ éléments linéairement indépendants sur R. Il suffit donc de démontrer que $\mathfrak{D}[\alpha]$ est un module (i. e. possède un système fini de générateurs). Soient $\omega_1, \ldots, \omega_n$ une base de l'ordre $\mathfrak{D}$. D'après le lemme 3, toutes les puissances α^k de a s'écrivent sous la forme

$$a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1},$$

a_i entiers rationnels; il en résulte facilement que tout nombre de $\mathfrak{D}[\alpha]$ est une combinaison linéaire à coefficients entiers des produits

$$\omega_i\alpha^j \qquad (1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant m-1).$$

Ainsi $\mathfrak{D}[\alpha]$ est un module.

Par application répétée du lemme 4, nous obtenons :

COROLLAIRE. — *Si $\mathfrak{D}$ est un ordre et $\alpha_1, \ldots, \alpha_\rho \in \tilde{\mathfrak{D}}$, alors l'anneau*

$$\mathfrak{D}[\alpha_1, \ldots, \alpha_\rho]$$

de tous les polynômes en $\alpha_1, \ldots, \alpha_\rho$ à coefficients dans $\mathfrak{D}$ est aussi un ordre.

THÉORÈME 6. — *L'ensemble de tous les nombres de* K *dont les polynômes minimaux sont à coefficients entiers rationnels est un ordre du corps* K *qui est maximum.*

DÉMONSTRATION. — Soit $\mathfrak{D}$ un ordre quelconque de K et α et $\beta \in \tilde{\mathfrak{D}}$. D'après le corollaire du lemme 4, l'anneau $\mathfrak{D}[\alpha, \beta]$ est un ordre et par suite il est contenu dans $\mathfrak{D}$ (lemme 2). Mais alors la différence $a - \beta$ et le produit $\alpha\beta$ appartiennent aussi à $\tilde{\mathfrak{D}}$. Cela démontre que $\tilde{\mathfrak{D}}$ est un anneau. Puisque $\mathfrak{D} \subset \tilde{\mathfrak{D}}$, alors $\tilde{\mathfrak{D}}$ contient n nombres linéairement indépendants; il suffit de vérifier que $\mathfrak{D}$ est un module.

Soit $\omega_1, \ldots, \omega$ une base de l'ordre $\mathfrak{D}$ et soit $\omega_1^*, \ldots, \omega_n^*$ la base duale dans le corps K (cf. appendice § 2-3)). Montrons que l'anneau $\tilde{\mathfrak{D}}$ est contenu dans le module $\mathfrak{D}^* = \{\omega_1^*, \ldots, \omega_n^*\}$. Soit $\alpha \in \mathfrak{D}$ et représentons-le sous la forme

$$a = c_1\omega_1^* + \ldots + c_n\omega_n^*,$$

c_i nombres rationnels. Multipliant cette égalité par ω_i et prenant la trace, nous obtenons

$$c = \mathrm{Tr}\,(\alpha\omega_i) \qquad (1 \leqslant i \leqslant n)$$

(nous utilisons le fait que $\mathrm{Tr}\,(\omega_i\omega_i^*) = 1$ et $\mathrm{Tr}\,(\omega_i\omega_j^*) = 0$ pour $i \neq j$). Tous les produits $\alpha\omega_i$ sont contenus dans l'ordre $\mathfrak{D}[\alpha]$ et par suite, d'après le lemme 2, tous les nombres c_i sont entiers, d'où $\alpha \in \mathfrak{a})^*$. Ainsi $\tilde{\mathfrak{D}} \subset \mathfrak{a})^*$. Appliquant maintenant le corollaire du théorème 2, nous concluons que $\tilde{\mathfrak{D}}$ est un module, ce qui termine la démonstration du théorème 6.

La démonstration ci-dessus du fait que $\tilde{\mathfrak{D}}$ est un anneau se généralise sans difficulté (avec des variantes sans importance) dans le cadre de la théorie des anneaux commutatifs sans diviseur de zéro. Les notions correspondantes dans le cas général sont étudiées dans le § 4 de l'appendice. En appliquant cette terminologie, on peut dire que l'ordre maximum d'un corps K de nombres algébriques est la fermeture intégrale de l'anneau Z des entiers rationnels dans le corps K. En liaison avec ce fait, les nombres de l'ordre maximum $\tilde{\mathfrak{D}}$ sont souvent appelés ***nombres entiers du corps*** K; l'anneau $\tilde{\mathfrak{D}}$ est alors appelé ***l'anneau des entiers du corps*** K.

Les unités de l'ordre maximal $\tilde{\mathfrak{D}}$ ***sont*** appelées ***unités du corps*** K ***de nombres algébriques.***

5) Discriminant d'un module complet

Soient $\mu_1, \ldots, \mu_n$ et $\mu_1', \ldots, \mu_n'$ deux bases d'un module complet M d'un corps K de nombres algébriques. Comme nous le savons (cf. 1)), la matrice de passage de la première base à la seconde est unimodulaire (i. e. est une matrice à coefficients entiers de déterminant ± 1). Il en résulte que les discriminants $D(\mu_1, \ldots, \mu_n)$ et $D(\mu_1', \ldots, \mu_n')$ sont égaux (cf. appendice § 2-3), formule (12)). Toutes les bases du module M ont ainsi le même discriminant, qui est un nombre rationnel; nous appellerons ce nombre rationnel le ***discriminant du module*** M.

Tout ordre du corps K est un module complet de K et par suite on peut parler du discriminant d'un ordre quelconque. Puisque la trace de tout nombre d'un ordre est un entier, le discriminant d'un ordre est toujours un entier rationnel (c'est déjà vrai pour tout module complet qui est contenu dans $\tilde{\mathfrak{D}}$).

Une base de l'ordre maximum $\tilde{\mathfrak{D}}$ d'un corps K de nombres algébriques est souvent appelée une ***base fondamentale*** de K et son discriminant le

discriminant du corps K. Le discriminant d'un corps de nombres algébriques est une caractéristique arithmétique très importante qui jouera dans la suite un rôle essentiel.

EXERCICES

1. Soient $\omega_1, \omega_2, \omega_3$ des nombres linéairement indépendants d'un corps K de nombres algébriques. Montrer que tous les nombres de K de la forme

$$a\omega_1 + b\omega_2 + c\omega_3,$$

a, *b,* c entiers rationnels quelconques, forment un module et trouver une base de ce module.

2. Trouver l'anneau des stabilisateurs du module $\left\{2, \frac{\sqrt{2}}{2}\right\}$ dans le corps $\mathbf{Q}(\sqrt{2})$. Montrer de plus que le module $\{1, \sqrt{2}\}$ est l'ordre maximum du corps $\mathbf{Q}(\sqrt{2})$.

3. Montrer que dans le corps Q des nombres rationnels il existe un ordre unité qui est l'anneau de tous les nombres entiers rationnels.

4. Démontrer que dans l'ordre $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ du corps $\mathbf{Q}(\sqrt[3]{2})$, tout nombre de norme 2 est associé à $\sqrt[3]{2}$.

5. Montrer que l'intersection de deux modules complets est aussi un module complet.

6. Démontrer que tout module (d'un corps de nombres algébriques) qui est un anneau est contenu dans l'ordre maximum du corps.

7. Soient $M = \{\gamma_1, \ldots, \alpha_\eta\}$ et $N = \{\beta_1, \ldots, \beta_n\}$ deux modules complets du corps K. Le module engendré par les produits $\alpha_i\beta_j$ ne dépend pas du choix des bases α_i et β_j et s'appelle le produit des modules M et N; on le désigne par MN. Montrer que les anneaux de stabilisateurs de M et N sont contenus dans l'anneau des stabilisateurs de leur produit MN.

8. Soit M un module complet contenu dans l'ordre maximum $\mathfrak{D}$ d'un corps K de nombres algébriques. Montrer que si le discriminant du module M n'est pas divisible par le carré d'un nombre entier $(\neq 1)$, alors M coïncide avec $\mathfrak{D}$.

9. Soit θ un élément primitif d'un corps K de nombres algébriques de degré n, contenu dans l'ordre maximum. Montrer que si le discriminant du polynôme minimal de θ n'est pas divisible par un carré, alors les nombres $1, \theta, \ldots, \theta^{n-1}$ forment une base fondamentale du corps K.

10. Trouver une base fondamentale et le discriminant du corps $\mathbf{Q}(\sqrt{2})$.

11. Trouver une base fondamentale et le discriminant du corps Q(p), où ρ racine de l'équation $x^3 - x - 1 = 0$.

12. Soit M un module complet d'un corps K de nombres algébriques. Montrer que l'ensemble M* des nombres $\xi \in K$ tels que $\mathrm{Tr}(\alpha\xi) \in \mathbf{Z}$ pour tout $a \in M$ est aussi un module complet du corps K; le module M* est appelé module dual du module M. Montrer de plus que si $\mu_1, \ldots, \mu_n$ est une base de M, alors la base duale $\mu_1^*, \ldots, \mu_n^*$ dans le corps K (par rapport à $\mathbf{Q}$) est une base de M*.

13. Démontrer que (M*)* = M, i. e. que le module dual de $\mathbf{M}^*$ est égal à M.

14. Démontrer qu'un module M et son module dual M* ont le même anneau de stabilisateurs.

15. Soient $\mathbf{M}_1$ et $\mathbf{M}_2$ des modules complets. Montrer que les inclusions $\mathbf{M}_1 \subset \mathbf{M}_2$ et $\mathbf{M}_1^* \supset \mathbf{M}_2^*$ sont équivalentes.

16. Soit θ un élément primitif d'un corps K de nombres algébriques de degré n; on suppose que θ appartient à l'ordre maximum $\tilde{\mathfrak{D}}$ de K et soit f(t) son polynôme minimal sur Q. Montrer que le module dual M* du module

$$\mathbf{M} = \{1, \theta, \ldots, \theta^{n-1}\}$$

(qui est d'ailleurs un ordre) est égal à $\frac{1}{f'(\theta)}$ M.

17. Soient M un module complet dans K et $\mathfrak{D}$ son anneau de stabilisateurs. Démontrer que le produit MM* (cf. exercice 7) est égal à a)*.

18. Montrer que dans le corps Q(0), $\theta^3 = 2$, l'anneau des stabilisateurs du module M = { 4, θ, θ^2 } est égal à l'ordre { 1, 2θ, $2\theta^2$ } et celui du module

$$\mathbf{M}^2 = \{2, 2\theta, \theta^2\}$$

à l'ordre maximum { 1, θ, θ^2 }.

19. Un polynôme $t^n + a_1 t^{n-1} + \ldots + a_n$ à coefficients entiers rationnels, est appelé un polynôme d'Eisenstein relativement à un nombre premier p si tous les coefficients $a_1, \ldots, a_n$ sont divisibles par p et si le terme constant a_n (qui est divisible par p) n'est pas divisible par p^2.

Soient K un corps de nombres algébriques, de degré n et θ un entier algébrique qui soit un élément primitif de K; montrer que si θ est racine d'un polynôme d'Eisenstein relatif au nombre p, alors

$$\mathbf{N}(c_0 + c_1\theta + \ldots + c_{n-1}\theta^{n-1}) \equiv c_0^n \pmod{p}$$

pour tous les entiers rationnels $c_0, c_1, \ldots, c_{n-1}$.

20. Soit θ un élément primitif d'un corps K de nombres algébriques, de degré n; l'indice de l'ordre { 1, $\theta, \ldots, \theta^{n-1}$ } dans l'ordre maximum est appelé aussi l'indice du nombre θ. Montrer que si θ est racine d'un polynôme d'Eisenstein relatif à un nombre premier p, alors l'indice du nombre θ n'est pas divisible par p.

21. Démontrer que, dans chacun des trois corps cubiques

$$\begin{aligned} \mathbf{K}_1 &= \mathbf{Q}(\theta), & \theta^3 - 18\theta - 6 &= 0, \\ \mathbf{K}_2 &= \mathbf{Q}(\theta), & \theta^3 - 36\theta - 78 &= 0, \\ \mathbf{K}_3 &= \mathbf{Q}(\theta), & \theta^3 - 54\theta - 150 &= 0, \end{aligned}$$

toute base fondamentale est une puissance de la base 1, θ, θ^2. Vérifier de plus que ces trois corps ont le même discriminant, égal à $22\,356 = 23 \cdot 2^2 \cdot 3^5$ (Les corps $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$ sont distincts, comme cela résulte de l'exercice 14, § 7, chap. III).

22. Montrer que pour le corps cubique $\mathbf{Q}(\theta)$, $\theta^3 - \theta - 4 = 0$, la base 1, θ, $\frac{\theta + \theta^2}{2}$ est une base fondamentale.

23. Soient a et b des entiers naturels sans carrés et premiers entre eux. Posons $k = ab$ si $a^2 \equiv b^2 \pmod 9$ et $k = 3ab$ si $a^2 \not\equiv b^2 \pmod 9$. Montrer que le discriminant du corps $\mathbf{Q}\sqrt[3]{(ab^2)}$ est $D = -3k^2$.

24. Montrer que les nombres 1, $\sqrt[3]{6}$, $(\sqrt[3]{6})^2$ forment une base fondamentale du corps $\mathbf{Q}(\sqrt[3]{6})$.

§ 3. — MÉTHODES GÉOMÉTRIQUES

La résolution des deux problèmes formulés à la fin du § 2, 3) exige l'introduction de nouvelles techniques de nature géométrique. Ces méthodes reposent sur une représentation des nombres algébriques comme points d'un espace n-dimensionnel, analogue à la représentation des nombres complexes dans le plan de Cauchy.

1) Représentation géométrique des nombres algébriques

Si un corps K de nombres algébriques est de degré n sur le corps Q des nombres rationnels, alors il existe n isomorphisme, distincts de ce corps dans le corps C de tous les nombres complexes (cf. appendice § 2, 3)).

DÉFINITION. — *Si l'image d'un corps* K *par un isomorphisme* $\sigma : K \to C$ *est contenue dans le corps des nombres réels, nous dirons que I?somorphisme* σ *est réel. Il est dit complexe dans le cas contraire.*

Par exemple, pour le corps cubique K = R(B), où $\theta^3 = 2$, l'isomorphisme

$$Q(e) \to \mathbf{Q}(\sqrt[3]{2})$$

tel que $\theta \to \sqrt[3]{2}$ est réel (pour $\sqrt[3]{2}$ on prend ici la détermination réelle de ce nombre) ; les deux autres isomorphismes

$$\mathbf{Q}(\theta) \to \mathbf{Q}(\varepsilon\sqrt[3]{2}) \quad \text{et} \quad Q(e) \to \mathbf{Q}(\varepsilon^2\sqrt[3]{2}) \qquad \left(\varepsilon = \cos\frac{2x}{2} + i\sin\frac{2x}{3}\right)$$

sont complexes. Si d est un nombre rationnel qui n'est pas un carré, pour le corps $\mathbf{Q}(\theta)$, $\theta^2 = d$, *les* deux isomorphismes sont réels pour $d > 0$ et complexes pour $d < 0$. En général, si, dans un corps K de nombres algébriques, on choisit un élément primitif θ racine d'un polynôme $\varphi(t)$ irréductible sur Q et si $\theta_1, \ldots, \theta_n$ sont les racines de $\varphi(t)$ dans le corps C, alors l'isomorphisme

$$\mathbf{K} = \mathbf{Q}(\theta) \to \mathbf{Q}(\theta_i) \subset \mathbf{C}, \qquad \theta \to \theta_i \tag{1}$$

est réel si la racine θ_i est réelle et complexe dans le cas contraire.

Pour tout nombre complexe $y = x + iy$ (x et y réels), nous désignerons par $\bar{\gamma}$ le nombre complexe conjugué $x - y_i$.

Soit σ : K → C un isomorphisme complexe. Il est évident que l'application $\bar{\sigma}$: K → C définie par l'égalité

$$G(a) = a(a) \qquad \alpha \in \mathbf{K},$$

est aussi un isomorphisme complexe de K dans C. Cet isomorphisme $\bar{\sigma}$ est appelé conjugué de σ. Puisque $\bar{\sigma} \neq \sigma$ et $\bar{\bar{\sigma}} = \sigma$, tous les isomorphismes complexes de K dans C se répartissent en isomorphismes conjugués deux à deux. En particulier, le nombre des isomorphismes complexes est toujours pair. Deux isomorphismes complexes de la forme (1) sont conjugués entre eux si et seulement si dans la correspondance des racines θ_i et θ_j sont des nombres complexes conjugués.

Supposons que parmi les isomorphismes de K dans C il en existe s réels $\sigma_1, \ldots, \sigma_s$ et $2t$ complexes, tels que $s + 2t = n = (K : R)$. Dans chaque paire d'isomorphismes complexes conjugués choisissons l'un d'entre eux; soit $\sigma_{s+1}, \ldots, \sigma_{s+t}$ le système d'isomorphismes complexes ainsi obtenus. Le système de tous les isomorphismes du corps K dans le corps C s'écrit alors sous la forme

$$\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \bar{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \bar{\sigma}_{s+t}.$$

Nous supposerons dans la suite que les isomorphismes ont été ainsi classés. Pour certains corps, il peut ne pas y avoir d'isomorphismes réels ($s = 0$) ou pas d'isomorphismes complexes ($t = 0$).

Considérons l'ensemble $\mathfrak{L}^{s,t}$ des lignes de la forme

$$x = (x_1, \ldots, x_s ; x_{s+1}, \ldots, x_{s+t}) \tag{2}$$

dont les 5 premiéres composantes $x_1, \ldots, x_s$ sont réelles et dont les autres $x_{s+1}, \ldots, x_{s+t}$ sont des nombres complexes. Définissons l'addition et la multiplication de ces lignes entre elles par un nombre réel, composante par composante. Pour ces opérations, il est clair que $\mathfrak{L}^{s,t}$ est un anneau commutatif à unité (1, . . . 1) et un espace vectoriel réel. Nous appellerons les lignes (2) vecteurs ou points de l'espace $\mathfrak{L}^{s,t}$.

Comme base de l'espace $\mathfrak{L}^{s,t}$ sur le corps des nombres réels, il est clair que l'on peut prendre les vecteurs

$$\left.\begin{array}{l}(1, \ldots, 0 ; 0, \ldots, 0)\\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot\\ (0, \ldots, 1 ; 0, \ldots, 0)\end{array}\right\} s$$
$$\left.\begin{array}{l}(0, \ldots, 0 ; 1, \ldots, 0)\\ (0, \ldots, 0 ; i, \ldots, 0)\\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot\\ (0, \ldots, 0 ; 0, \ldots, 1)\\ (0, \ldots, 0 ; 0, \ldots, i)\end{array}\right\} 2t \tag{3}$$

Ainsi, l'espace vectoriel $\mathfrak{L}^{s,t}$ est de dimension $n = s + 2t$. Si nous posons

$$x_{s+j} = y_j + iz_j \qquad (j = 1, \ldots, t),$$

le vecteur (2) a pour coordonnées, dans la base (3)

$$(x_1, \ldots, x_s ; y_1, z_1, \ldots, y_t, z_t), \tag{4}$$

Si on considère $\mathfrak{L}^{s,t}$ seulement comme un espace vectoriel réel, nous le désignerons par $\mathfrak{R}^n$.

Soit x un point fixé de $\mathfrak{L}^{s,t}$. L'application $x' \to xx'$ ($x' \in \mathfrak{L}^{s,t}$), i. e. la multiplication dans $\mathfrak{L}^{s,t}$ par x est une transformation linéaire de l'espace réel $\mathfrak{L}^{s,t} = \mathfrak{R}^n$. Dans la base (3), la matrice de cette transformation est

$$\begin{vmatrix} x_1 & & & & & & & \\ & \ddots & & & & & & \\ & & x_s & & & & & \\ & & & y_1 & -z_1 & & & \\ & & & z_1 & y_1 & & & \\ & & & & & \ddots & & \\ & & & & & & y_t & -z_t \\ & & & & & & z_t & y_t \end{vmatrix}$$

tous les éléments non écrits étant nuls. Le déterminant de cette matrice est égal à

$$x_1 \ldots x_s(y_1^2 + z_1^2) \ldots (y_t^2 + z_t^2) = x_1 \ldots x_s \,|\, x_{s+1} \,|^2 \ldots |\, x_{s+t} \,|^2.$$

Cela suggère la définition suivante. Nous prendrons pour ***norme d'un point*** $x = (x_1, \ldots, x_{s+t}) \in \mathfrak{L}^{s,t}$ la quantité

$$N(x) = x_1 \ldots x_s \,|\, x_{s+1} \,|^2 \ldots |\, x_{s+t} \,|^2.$$

Ainsi la norme N(x) de x est le déterminant de la matrice de la transformation linéaire $x' \to x'x$.

Il est clair que la norme ainsi introduite possède la propriété de **multiplicativité**

$$N(xx') = N(x)N(x').$$

Précisons maintenant comment on peut représenter les nombres du corps K par des points de l'espace $\mathfrak{S}^{s,t}$. A tout nombre α de K, associons le point

$$x(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)) \tag{5}$$

de $\mathfrak{L}^{s,t}$. Ce point est la représentation géométrique du nombre a.

Si α et β sont des nombres distincts de K, alors, pour tout

$$k = 1, \ldots, s + t,$$

les nombres $\sigma_k(\alpha)$ et $\sigma_k(\beta)$ sont distincts et en particulier $x(\alpha) \neq x(\beta)$. Ainsi, l'application

$$\alpha \to x(\alpha), \qquad \alpha \in \mathbf{K}$$

est **injective** (bien entendu elle n'est pas **surjective,** i. e. tout point de $\mathfrak{L}^{s,t}$ n'est pas l'image d'un point de K).

Puisque $\sigma_k(\alpha + \beta) = \sigma_k(\alpha) + \sigma_k(\beta)$ et $\sigma_k(\alpha\beta) = \sigma_k(\alpha)\sigma_k(\beta)$, alors

$$x(\alpha + \beta) = x(\alpha) + x(\beta) \tag{6}$$

$$x(\alpha\beta) = x(\alpha)x(\beta) \tag{7}$$

i. e. l'application $a \to$ x(a) est un homomorphisme. De plus, si a est un nombre rationnel, $\sigma_k(a\alpha) = \sigma_k(a)\sigma_k(\alpha) = a\sigma_k(\alpha)$; d'où

$$x(a\alpha) = ax(\alpha). \tag{8}$$

Puisque, d'après le § 2-3) de l'appendice, nous avons

$$\begin{aligned} \mathbf{N}(\alpha) &= \mathbf{N}_{\mathbf{K}/\mathbf{Q}}(\alpha) \\ &= \sigma_1(\alpha) \ldots \sigma_s(\alpha)\sigma_{s+1}(\alpha)\bar{\sigma}_{s+1}(\alpha) \ldots \sigma_{s+t}(\alpha)\bar{\sigma}_{s+t}(\alpha) \\ &= \mathrm{q(a)} \ldots \sigma_s(\alpha) \mid \sigma_{s+1}(\alpha) \mid^2 \ldots \mid \sigma_{s+t}(\alpha) \mid^2, \end{aligned}$$

la norme N(x(a)) du point $x(\alpha)$ coïncide avec la norme N(a) du nombre a :

$$\mathbf{N}(x(\alpha)) = \mathbf{N}(\alpha), \qquad \alpha \in \mathbf{K}.$$

Considérons deux exemples simples. Soit d un nombre rationnel > 0 qui n'est pas un carré. Alors, pour le corps quadratique réel $\mathbf{Q}(\theta)$, $\theta^2 = d$, la représentation géométrique du nombre a = a + $b\theta$ (a et b rationnels) est le point $x(\alpha) = (a + b\sqrt{d}$, a $- b\sqrt{d})$. Dans le cas du corps quadratique imaginaire Q(q), $\eta^2 = -d$, la représentation du nombre β = a + $b\eta$ est le point du plan complexe de coordonnées (a, $b\sqrt{d}$) (dans ce cas, la base (3) est formée des nombres 1 et i).

Montrons que pour une base quelconque $\alpha_1, \ldots, a$, (du corps $\mathbf{K}/\mathbf{Q}$), les vecteurs correspondants $x(\alpha_1), \ldots, x(\alpha_n)$ de $\mathfrak{L}^{s,t} = \mathfrak{R}^n$ sont **linéairement** indépendants (sur le corps réel). En effet, posons

$$\sigma_k(\alpha_l) = x_k^{(l)}, \qquad 1 \leqslant k \leqslant s,$$

$$\sigma_{s+j}(\alpha_l) = y_j^{(l)} + iz_j^{(l)}, \qquad 1 \leqslant j \leqslant t.$$

Puisque le vecteur

$$x(\alpha_l) = (xl', \ldots, x_s^{(l)}; y_1^{(l)} + iz_1^{(l)}, \ldots, y_t^{(l)} + iz_t^{(l)})$$

a pour composantes, dans la base (3),

$$(\mathrm{xl''}, \ldots, x_s^{(l)}; y_1^{(l)}, z_1^{(l)}, \ldots, y_t^{(l)}, z_t^{(l)}),$$

il suffit, pour démontrer notre affirmation, de vérifier que le déterminant

$$d = \begin{vmatrix} x_1^{(1)} \dots x_s^{(1)} y_1^{(1)} z_1^{(1)} \dots y_t^{(1)} z_t^{(1)} \\ \dots \\ x_1^{(n)} \dots x_s^{(n)} y_1^{(n)} z_1^{(n)} \dots y_t^{(n)} z_t^{(n)} \end{vmatrix}$$

est différent de zéro. Considérons, à la place de d, un autre déterminant

$$d^* = \begin{vmatrix} x_1^{(1)} \dots x_s^{(1)} y_1^{(1)} + iz_1^{(1)} y_1^{(1)} - iz_1^{(1)} \dots \\ \dots \\ x_1^{(n)} \dots x_s^{(n)} y_1^{(n)} + iz_1^{(n)} y_1^{(n)} - iz_1^{(n)} \dots \end{vmatrix},$$

qui peut aussi s'écrire

$$d^* = \begin{vmatrix} \sigma_1(\alpha_1) \dots \sigma_s(\alpha_1) \sigma_{s+1}(\alpha_{11}) \bar{\sigma}_{s+1}(\alpha_1) \dots \\ \dots \\ \sigma_1(\alpha_n) \dots \sigma_s(\alpha_n) \sigma_{s+1}(\alpha_n) \bar{\sigma}_{s+1}(\alpha_n) \dots \end{vmatrix}$$

Dans le déterminant d^* ajoutons à la $(s+1)^{\text{ème}}$ colonne la colonne suivante et mettons 2 en facteur dans le déterminant obtenu; soustrayons cette nouvelle colonne de la $(s+2)^{\text{ème}}$ et mettons $-i$ en facteur. Appliquant ces opérations aux couples de colonnes suivantes, nous obtenons l'égalité

$$d^* = (-2i)^t d. \tag{9}$$

Dans le \$2, 3) de l'appendice, on a montré que

$$d^{*2} = \mathrm{D}, \tag{10}$$

où $\mathrm{D} = \mathrm{D}(\alpha_1, \dots, \alpha_n)$ est le discriminant de la base $\alpha_1, \dots, \alpha_n$ (dans l'extension $\mathbf{K}/\mathbf{Q}$). Puisque $\mathrm{D} \neq 0$, il résulte de (9) et (10) que $d \neq 0$.

Supposons maintenant que $\alpha_1, \dots, a_n$ est la base d'un module complet M du corps K. D'après (6) et (8), tout $a = a_1\alpha_1 + \dots + a_n\alpha_n$ de M ($a_1, \dots, a_n$ entiers rationnels) a pour représentation géométrique dans $\mathcal{R}^n$ le vecteur $x(a) = a_1 x(\alpha_1) + \dots + a_n x(\alpha_n)$. Nous avons obtenu le résultat suivant.

THÉORÈME 1. — *Dans la représentation géométrique des nombres d'un corps* K *de degré* $n = s + 2t$*par des points de l'espace* $\mathcal{R}^n$*, l'image d'un module complet* $\mathrm{M} = \{\alpha_1, \dots, a_n\}$ *est l'ensemble de toutes les combinaisons linéaires, à coefficients entiers, des vecteurs linéairement indépendants (dans l'espace* $\mathcal{R}^n$*)*

$$x(\alpha_1), \dots, x(\alpha_n).$$

2) Lattices

L'étude géométrique des modules complets repose sur le théorème 1. Nous considérerons donc dans $\mathcal{R}^n$ des ensembles de vecteurs d'un type particulier.

DÉFINITION. — *Soient* $e_1, \ldots, e_m$, $m \leqslant n$, *un système de vecteurs linéairement indépendants de l'espace* $\mathcal{R}^n$. *L'ensemble* $\mathcal{M}$ *de tous les vecteurs de la forme*

$$a_1e_1 + \ldots + a_me_m$$

où les a_i *parcourent indépendamment les uns des autres l'ensemble des entiers rationnels est appelé un lattice m-dimensionne1 dans* $\mathcal{R}^n$ *et les vecteurs* $e_1, \ldots, e_m$ *sont appelés la base du lattice. Si* $m = n$, *le lattice est dit complet; il est dit incomplet dans le cas contraire.*

Le contenu du théorème 1 est donc que l'image géométrique d'un module complet est un lattice complet.

Il est facile de voir que deux systèmes de vecteurs linéairement indépendants $e_1, \ldots, e_m$ et $f_1, \ldots, f_m$ définissent un même lattice si et seulement si on passe de l'un à l'autre par une transformation unimodulaire, i. e. si

$$f_i = \sum_{j=1}^{m} c_{ij}e_j \qquad (1 \leqslant i \leqslant m),$$

où (c_{ij}) est une matrice à coefficients entiers de determinant ± 1.

L'étude des lattices repose sur des considérations métriques dans l'espace $\mathcal{R}^n$. Introduisons dans $\mathfrak{L}^{s,t} = \mathcal{R}^n$ un produit scalaire pour lequel les vecteurs (3) forment une base orthonormée. Si les vecteurs x et x' ont respectivement pour coordonnées dans la base (3) $(x_1, \ldots, x_n)$ et $(x_1', \ldots, x_n')$, le produit scalaire $(x,$ x') est défini par la formule

$$(x, x') = x_1x_1' + \ldots + x_nx_n'.$$

On désignera par $\| x \|$ la longueur du vecteur x.

Soit r un nombre réel > 0. Nous dtsignerons par $U(r)$ l'ensemble de tous les points x de coordonnées $(x_1, \ldots, x_n)$ dans la base (3), tels que

$$\| x \| = \sqrt{x_1^2 + \ldots + xl,} < r.$$

Cet ensemble U(r) est appelé la boule (ouverte) de centre d'origine et de rayon r.

Un ensemble de points de $\mathcal{R}^n$ est dit *borné* s'il est contenu dans une boule U(r).

Un ensemble de points de l'espace $\mathcal{R}^n$ est dit *discret* si pour tout $r > 0$, il y a seulement un nombre fini de points de cet ensemble dans la boule U(r).

LEMME 1. — *L'ensemble des points d'un lattice quelconque* $\mathcal{M}$ *de* $\mathcal{R}^n$ *est discret.*

DÉMONSTRATION. — Puisque tout lattice incomplet est contenu dans un lattice complet, il suffit de considérer le cas d'un lattice complet $\mathcal{M}$. Choisissons une base $e_1, \ldots, e_n$ de $\mathcal{M}$. Les conditions

$$(x, e_2) = 0, \ \ldots, (x, e_n) = 0$$

forment un système linéaire homogène de $(n - 1)$-équations à n inconnues. Puisque ce système admet une solution non nulle, il existe un vecteur x non nul orthogonal aux vecteurs $e_2, \ldots, e_n$. Si on avait aussi $(x, e_1) = 0$, le vecteur x serait orthogonal à tous les vecteurs de l'espace $\mathcal{R}^n$, ce qui est impossible. Ainsi $(x, e_1) \neq 0$. Le vecteur $f_1 = \frac{x}{(x, e_1)}$ est orthogonal à tous les vecteurs $e_2, \ldots, e_n$ et $(f_1, e_1) = 1$. Ainsi, pour tout i $(1 \leqslant i \leqslant n)$, on peut trouver un vecteur f_i tel que

$$(f_i, e_j) = \begin{cases} 1 & \text{si} \quad j = i \\ 0 & \text{si} \quad j \neq i. \end{cases}$$

Soit maintenant $z = a_1 e_1 + \ldots + a_n e_n$ un vecteur de $\mathcal{M}$ (a_i entier rationnel) appartenant à la boule U(r), i. e. $\| z \| < r$. Puisque $a_k = (z, f_k)$, alors, d'après l'inégalité de Cauchy, on a

$$| a_k | = | (z, f_k) | \leqslant \| z \| \cdot \| f_k \| < r \| f_k \|,$$

où $r \| f_k \|$ est indépendant de z. Ainsi il y a seulement un nombre fini de valeurs possibles pour les nombres a_k; cela signifie qu'il n'existe qu'un nombre fini de $z \in \mathcal{M}$ tel que $\| z \| < r$. Le lemme 1 est dtmontré.

Soit X un ensemble quelconque de points de l'espace $\mathcal{R}^n$ et z un point de $\mathcal{R}^n$. L'ensemble des points de la forme x + z, où x parcourt tous les points de X, s'appelle l'ensemble translaté de l'ensemble X par le vecteur z; nous le désignerons par X + z.

DÉFINITION. — *Soit $e_1, \ldots, e_m$ une base d'un lattice $\mathcal{M}$. L'ensemble* T *des points de la forme*

$$\alpha_1 e_1 + \ldots + \alpha_m e_m$$

où $\alpha_1, \ldots, \alpha_m$ parcourent, indépendamment l'un de l'autre les nombres réels du segment [0,1 [, i. *e.* $0 \leqslant \alpha_i < 1$, *est appelé un parallélépipède fondamental du lattice $\mathcal{M}$.*

Un parallélépipède fondamental n'est pas défini de manière unique par la donnée du lattice; il dépend du choix de la base.

LEMME 2. — *Si* T *est un parallélépipède fondamental d'un lattice complet $\mathcal{M}$, les ensembles*

$$T_z = T + z,$$

où z parcourt les points de $\mathcal{M}$, sont disjoints deux à deux et remplissent tout l'espace $\mathcal{R}^n$.

DÉMONSTRATION. — Soit $e_1, \ldots, e_n$ la base du lattice $\mathcal{M}$ sur laquelle est construite le parallélépipède T. On veut montrer que tout point

$$x = x_1e_1 + \ldots + x_ne_n$$

de $\mathcal{R}^n$ appartient à un ensemble T_z et un seul. Pour tout i, *écrivons* le nombre réel x_i sous la forme $x_i = k_i + \alpha_i$, k_i entier rationnel et α_i tel que $0 \leqslant \alpha_i < 1$. Posant $z = k_1e_1 + \ldots + k_ne_n$ et $u = \alpha_1e_1 + \ldots + \alpha_ne_n$, on a

$$x = u + z \qquad (u \in T, \quad z \in \mathcal{M}),$$

et ainsi $x \in T_z$. Si maintenant $x \in T_{z'}$, i. e. $x = u' + z'$ ($u' \in T$, $z' \in A$), alors égalant les coefficients de e_i dans l'égalité $u + z = u' + z'$, on obtient facilement $z = z'$. Le lemme 2 est démontre.

LEMME *3.* — ***Pour tout nombre réel $r > 0$, il existe seulement un nombre fini d'ensembles*** T_z (cf. le lemme 2) ***qui rencontrent la boule*** U(r).

DÉMONSTRATION. — Soit $e_1, \ldots, e_n$ la base du lattice $\mathcal{M}$ sur laquelle est construite le parallélépipède T. Si nous posons $d = \| e_1 \| + \ldots + \| e_n \|$, alors, pour tout vecteur $u = \alpha_1e_1 = \ldots + \alpha_ne_n \in T$, on aura

$$\| u \| \leqslant \| \alpha_1e_1 \| + \ldots + \| \alpha_ne_n \| = | \alpha_1 | \| e_1 \| + \ldots + | \alpha_n | \| e_n \| < d.$$

Supposons que l'ensemble T_z ($z \in \mathcal{M}$) rencontre U(r). Cela signifie qu'il existe un vecteur $x = u + z$, $u \in T$, $z \in \mathcal{M}$ tel que $\| x \| < r$. Puisque $z = x - u$, alors

$$\| z \| \leqslant \| x \| + \| -u \| < r + d,$$

i. e. le point z appartient à la boule U($r + d$). D'après le lemme 1; il existe seulement un nombre fini de tels points $z \in \mathcal{M}$ et le lemme est démontré.

Il est clair que les vecteurs du lattice forment un groupe pour l'addition; ainsi, tout lattice est un sous-groupe du groupe $\mathcal{R}^n$. Le lemme 1 montre cependant que ce n'est pas un sous-groupe quelconque; donnons une réciproque du lemme 1.

LEMME 4. — ***Tout sous-groupe discret $\mathcal{M}$ du groupe $\mathcal{R}^n$ est un lattice.***

DÉMONSTRATION. — Désignons par $\mathfrak{S}$ le plus petit sous-espace vectoriel de l'espace $\mathcal{R}^n$ contenant l'ensemble $\mathcal{M}$ et par m la dimensions de $\mathfrak{S}$. Nous pouvons alors choisir, dans $\mathcal{M}$, m vecteurs $e_1, \ldots, e_m$ formant une base du sous-espace $\mathfrak{S}$; soit $\mathcal{M}_0$ le lattice de base $e_1, \ldots, e_m$. Il est clair que $\mathcal{M}_0 \subset \mathcal{M}$.

Démontrons que l'indice $(\mathcal{M} : \mathcal{M}_0)$ est fini. En effet, tout vecteur $x \in \mathcal{M}$ s'écrit

$$x = u + z, \tag{11}$$

$z \in \mathcal{M}_0$, et u appartient au parallélépipède fondamental T du lattice $\mathcal{M}_0$ construit sur la base $e_1, \ldots, e_m$. Par hypothèse, $x \in \mathcal{M}$ et $z \in \mathcal{M}_0 \subset \mathcal{M}$; puisque $\mathcal{M}$ est un groupe, alors $u \in \mathcal{M}$. Mais T est un ensemble borné qui contient seulement un nombre fini de vecteurs de $\mathcal{M}$ (car $\mathcal{M}$ est discret). Ainsi le nombre de vecteurs u obtenu dans la décomposition (11) pour tout $x \in \mathcal{M}$ est fini ; cela signifie que l'indice $(\mathcal{M} : \mathcal{M}_0) = j$ est fini. Puisque l'ordre de tout élément du groupe quotient $\mathcal{M}/\mathcal{M}_0$ est un diviseur de j, alors $jx \in \mathcal{M}_0$ pour tout $x \in \mathcal{M}$; ainsi x s'exprime comme combinaison linéaire à coefficients entiers des vecteurs $\frac{1}{j} e_1, \ldots, \frac{1}{j} e_m$, i. e. $\mathcal{M}$ est contenu dans le lattice $\mathcal{M}^*$ de base $\frac{1}{j} e_1, \ldots, \frac{1}{j} e_m$. Le théorème 2 du § 2 montre maintenant que le sous-groupe $\mathcal{M}$ du groupe $\mathcal{M}^*$ possède une base $f_1, \ldots, f_l$, $l \leqslant m$. Pour démontrer que $\mathcal{M}$ est un lattice, il suffit donc de démontrer que les vecteurs $f_1, \ldots, f_l$ sont linéairement indépendants sur le corps des nombres réels et cela résulte du fait qu'ils engendrent le sous-espace vectoriel $\mathfrak{S}$ de dimension m. Le lemme 4 est démontré.

3) Espace logarithmique

Parallèlement à la représentation géométrique du corps K que nous venons d'étudier, où l'addition des nombres correspond à l'addition des vecteurs correspondants dans $\mathcal{R}^n$, nous avons besoin d'une autre représentation géométrique qui nous permette d'interpréter simplement la multiplication des nombres de K.

Supposons que parmi les isomorphismes du corps K de nombres algébriques dans le corps C des nombres complexes il en existe s réels et $2t$ complexes; nous les supposerons ordonnés comme dans 1).

Considérons l'espace vectoriel réel $\mathcal{R}^{s+t}$ de dimension $s + t$ constitué par les lignes $(\lambda_1, \ldots, \lambda_{s+t})$ dont les composantes sont réelles. Pour tout point $x \in \mathfrak{L}^{s,t}$ de la forme (2) dont toutes les composantes sont différentes de zéro, posons

$$\left.\begin{aligned} l_k(x) &= \operatorname{Log} |x_k| \quad \text{pour } k = 1, \ldots, s \\ l_{s+j}(x) &= \operatorname{Log} |x_{s+j}|^2 \quad \text{pour } j = 1, \ldots, t \end{aligned}\right\} \tag{12}$$

Associons maintenant à tout point $x \in \mathfrak{L}^{s,t}$ le vecteur

$$l(x) = (l_1(x), \ldots, l_{s+t}(x)) \tag{13}$$

de l'espace $\mathcal{R}^{s+t}$. Puisque pour des points x' et x de $\mathfrak{L}^{s,t}$ dont toutes les composantes sont différentes de zéro, on a

$$l_k(xx') = l_k(x) + l_k(x'), \qquad 1 \leqslant k \leqslant s+t,$$

alors

$$l(xx') = \mathrm{Z}(x) + l(x'). \tag{14}$$

Tous les points $x \in \mathfrak{L}^{s,t}$ de la forme (2) et à composantes non nulles (i. e. tels que $\mathrm{N}(x) \neq 0$) forment un groupe pour la multiplication composante par composante. L'égalité (14) exprime que l'application $x \to l(x)$ est un homomorphisme de ce groupe multiplicatif dans le groupe additif des vecteurs de l'espace $\mathcal{R}^{s+t}$.

Rapprochant l'égalité (2) de la définition de la norme N(x) d'un point $x \in \mathfrak{L}^{s,t}$ nous obtenons facilement la formule

$$\sum_{k=1}^{s+t} l_k(x) = \mathrm{Log} \mid \mathrm{N}(x) \mid, \tag{15}$$

pour la somme des composantes $l_k(x)$ du vecteur $l(x)$.

Soit maintenant $\alpha \neq 0$ un nombre du corps K. Posons

$$l(\alpha) = l(x(\alpha)),$$

ou $x(a) \in \mathfrak{L}^{s,t}$ est l'image de a dans la représentation étudiée dans 1). D'après (5), (12), (13), on a

$$l(\alpha) = (\log \mid \sigma_1(\alpha) \mid, \ldots, \log \mid \sigma_s(\alpha) \mid, \log \mid \sigma_{s+1}(\alpha) \mid^2, \ldots, \log \mid \sigma_{s+t}(\alpha) \mid^2).$$

Le vecteur $Z(a) \in \mathcal{R}^{s+t}$ sera appelé la ***représentation logarithmique du nombre*** $a \neq 0$ de K; l'espace $\mathcal{R}^{s+t}$ sera appelé ***espace logarithmique du corps*** K.

De (7) et (14) découle

$$l(\alpha\beta) = l(\alpha) + l(\beta) \qquad (\alpha \neq 0, \beta \neq 0). \tag{16}$$

L'application $a \to \mathrm{Z}(a)$ est donc un homomorphisme du groupe multiplicatif du corps K dans le groupe additif des vecteurs de l'espace $\mathcal{R}^{s+t}$. Il en résulte en particulier que

$$l(\alpha^{-1}) = -Z(a), \qquad a \neq 0.$$

Pour la somme des composantes $l_k(\alpha) = l_k(x(\alpha))$ $(1 \leqslant k \leqslant s+t)$ du vecteur $Z(a)$, on a la formule

$$\sum_{k=1}^{s+t} l_k(\alpha) = \mathrm{Log} \mid \mathrm{N}(\alpha) \mid. \tag{17}$$

En effet, la somme de gauche est égale au logarithme du module du produit

$$\sigma_1(\alpha) \dots \sigma_s(\alpha)\sigma_{s+1}(\alpha)\overline{\sigma_{s+1}(\alpha)} \dots \sigma_{s+t}(\alpha)\overline{\sigma_{s+t}(\alpha)},$$

qui est égal, d'après l'appendice § 2, 3), à la norme $N(a)$ (dans l'extension K/Q).

4) Représentation géométrique des unités

Soit maintenant $\mathfrak{D}$ un certain ordre du corps K. Considérons dans l'espace logarithmique $\mathcal{R}^{s+t}$ les vecteurs $l(\varepsilon)$ pour toutes les unités ε de l'anneau $\mathfrak{D}$. L'application $\varepsilon \to I(E)$ n'est pas injective. En effet, si une unité $\eta \in \mathfrak{D}$ est une racine de 1, i. e. $\eta^m = 1$ pour un certain entier m, alors $|\sigma_k(\eta)| = 1$ pourtoutk= 1, ... $s + t$ et par suite $l(\eta)$ est le vecteur nul ; ainsi, toutes les racines de 1 (et il en existe au moins deux dans l'ordre $\mathfrak{D}$, + 1 et — 1) ont pour image le même vecteur (nul). Pour analyser la structure du groupe des unités de l'ordre $\mathfrak{D}$ au moyen de l'homomorphisme $\varepsilon \to I(E)$, nous devrons rtsoudre les deux problèmes suivants :

1° Quelles sont les unités $\varepsilon = \mathfrak{D}$ qui ont pour image le vecteur nul ?

2° Nature de l'ensemble de tous les vecteurs I(E)?

Étudions la première question. Soit W l'ensemble des nombres $a \in \mathfrak{D}$ tels que Z(a) = 0. D'après (16), le produit de deux nombres de W appartient encore à W; puisque la condition I(a) = 0 équivaut aux égalités

$$|\sigma_k(\alpha)| = 1, \qquad 1 \leqslant k \leqslant s + t.$$

L'ensemble des points $x(a) \in \mathcal{R}_n = \mathfrak{L}^{s,t}$ pour a ∈ W est borné, i. e. est contenu dans une certaine boule U(r). Appliquant le lemme 1, nous obtenons que W est un ensemble fini. Pour tout nombre $\alpha \in$ W, considérons les puissances successives 1, a, . . . , α^k,... Puisque toutes ces puissances appartiennent à W, certaines d'entre elles sont égales, par exemple $\alpha^k = \alpha^l$, $l > k$. Mais alors, posant $m = l - k$, nous obtenons $a^m = 1$; ainsi tous les nombres de W sont des racines de 1 et par suite W est un sous-groupe fini du groupe des unités de l'anneau $\mathfrak{D}$.

Puisque le groupe W contient un sous-groupe d'ordre 2 (formé de + 1 et — 1), il est d'ordre pair. De plus, tout sous-groupe fini du groupe multiplicatif d'un corps est toujours cyclique (cf. appendices 3)); le groupe W est donc cyclique.

Nous résumerons sous forme d'un théorème les résultats obtenus.

THÉORÈME 2. — *Les unités ε d'un ordre $\mathfrak{D}$ telles que I(E) soit le vecteur nul forment un groupe cyclique fini d'ordre pair. Ce groupe est l'ensemble des racines de 1 contenues dans $\mathfrak{D}$.*

Passons à la deuxième question, i. e. précisons la structure de l'ensemble $\mathfrak{G} \subset \mathcal{R}^{s+t}$ des vecteurs Z(E) quand ε parcourt toutes les unités de l'anneau $\mathfrak{D}$.

D'après le théorème 4 du § 2, la norme de toute unité $\varepsilon \in \mathfrak{D}$ est égale à ± 1; par suite Log $|\mathrm{N}(\varepsilon)| = 0$. D'après l'égalité (17), on a donc

$$\sum_{k=1}^{s+t} l_k(\varepsilon) = 0 \ ; \tag{18}$$

cela signifie que tous les points Z(E) appartiennent au sous-espace $\mathfrak{L} \subset \mathcal{R}^{s+t}$ des points $(\lambda_1, \ldots, \lambda_{s+t}) \in \mathcal{R}^{s+t}$ tels que $\lambda_1 + \ldots + \lambda_{s+t} = 0$. Ce sous-espace $\mathfrak{L}$ est de dimension $s + t - 1$.

Démontrons que $\mathfrak{G}$ est un lattice. Puisque $\mathfrak{G}$ est un sous-groupe du groupe additif des vecteurs de l'espace $\mathcal{R}^{s+t}$ alors, d'après le lemme 4, il suffit de vérifier que l'ensemble $\mathfrak{G}$ est discret (comme base orthonormale dans $\mathcal{R}^{s+t}$, on prend l'ensemble des vecteurs dont une composante est égale à 1 et toutes les autres nulles). Soit r un nombre positif quelconque et supposons $\| l(\varepsilon) \| < r$. Puisque $l_k(\varepsilon) \leqslant |\, l_k(\varepsilon) \,| \leqslant \| l(\varepsilon) \|$, alors

$$l_k(\varepsilon) < r \qquad (1 \leqslant k \leqslant s + t),$$

d'où

$$|\, \sigma_k(\varepsilon) \,| < e^r, \qquad k = 1, \ldots, s,$$

$$|\, \sigma_{s+j}(\varepsilon) \,|^2 < e^r, \qquad j = 1, \ldots, t.$$

Il en résulte que si $\varepsilon \in \mathfrak{D}$ parcourt toutes les unités telles que $\| Z(\varepsilon) \| < r$, les points $x(\varepsilon)$ sont bornés. Puisque les vecteurs x(a) $\in \mathcal{R}^n$ pour $a \in \mathfrak{D}$ forment un lattice (théorème 1), le nombre de telles unités ε est fini (lemme 1). Par suite, il n'existe qu'un nombre fini de vecteurs $l(\varepsilon)$ tels que $\| Z(\varepsilon) \| < r$ et l'ensemble $\mathfrak{G}$ est donc discret.

Puisque le lattice $\mathfrak{G}$ est contenu dans le sous-espace $\mathfrak{L}$, sa dimension ne dépasse pas $s + t - 1$.

THÉORÈME 3. — *Dans la représentation géométrique d'un ordre $\mathfrak{D}$ dans l'espace logarithmique $\mathcal{R}^{s+t}$, les images Z(E) des unités $\varepsilon \in \mathfrak{D}$ forment un Zattice de dimension $r \leqslant s + t - 1$.*

5) Premiers résultats sur le groupe des unités

Les théorèmes 2 et 3 fournissent déjà d'importants renseignements sur la structure du groupe des unités d'un ordre $\mathfrak{D}$. Il en résulte notamment qu'il existe dans $\mathfrak{D}$ des unités $\varepsilon_1, \ldots, \varepsilon_r$, $r \leqslant s + t - 1$, telles que toute unité de $\mathfrak{D}$ s'écrive de manière unique sous la forme

$$\varepsilon = \zeta \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}, \tag{19}$$

où $a_1, \ldots,$ a, sont des entiers rationnels et ζ une certaine racine de 1 contenue dans $\mathfrak{D}$. Montrons que le groupe des unités de l'ordre $\mathfrak{D}$ est le produit d'un groupe fini et de r groupes cycliques infinis.

Pour ce résultat, choisissons une base $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ du lattice $\mathfrak{G}$ et montrons que les unités $\varepsilon_1, \ldots, \varepsilon_r$ possèdent la propriété ci-dessus. Soit ε une unité de l'ordre $\mathfrak{D}$. Puisque $l(\varepsilon) \in \mathfrak{G}$, alors

$$l(\varepsilon) = a_1 l(\varepsilon_1) + \ldots + a_r l(\varepsilon_r),$$

où les a_j sont des nombres entiers. Considérons l'unité

$$\zeta = \varepsilon \varepsilon_1^{-a_1} \ldots \varepsilon_r^{-a_r}.$$

D'après la formule (16), nous avons, pour cette unité,

$$l(\zeta) = \mathrm{Z}(c) - a_1 l(\varepsilon_1) - \ldots - a_r l(\varepsilon_r) = 0;$$

par suite, d'après le théorème 2, c'est une racine de 1. Ainsi l'unité ε admet la représentation (19). Montrons l'unicité : soit $\varepsilon = \zeta' \varepsilon_1^{b_1} \ldots \varepsilon_r^{b_r}$ une autre représentation de ε; puisque les vecteurs $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ sont linéairement indépendants, l'égalité $l(\varepsilon) = b_1 l(\varepsilon_1) + \ldots + b_r l(\varepsilon_r)$ entraîne

$$a_1 = b_1, \ldots, a_r = b_r.$$

Mais alors nous avons aussi $\zeta = \zeta'$, ce qui termine la démonstration.

Il reste à préciser la valeur du nombre r, dont nous savons seulement qu'il est inférieur ou égal à $s + t - 1$. Nous montrerons dans le paragraphe suivant que, en fait, $r = s + t - 1$; avec les méthodes de ce chapitre, nous ne pouvons même pas affirmer que $r > 0$ (dans le cas $s + t - 1 > 0$, bien entendu).

D'après le théorème 3, l'affirmation ci-dessus est équivalente au fait que le lattice $\mathfrak{G}$ des représentants des unités de l'ordre $\mathfrak{D}$ dans l'espace logarithmique est de dimension égale à $s + t - 1$.

EXERCICES

1. Démontrer que tous les représentants $x(\alpha) \in \mathcal{R}^n$ des nombres α d'un corps K de nombres algébriques de degré n forment un sous-ensemble partout dense dans l'espace $\mathcal{R}^n$.

2. Montrer que si $s \neq 0$ (i. e. s'il existe au moins un isomorphisme réel parmi les isomorphismes du corps K dans le corps des nombres complexes), les seules racines de 1 qui appartiennent à K sont les nombres $+1$ et -1 (ce fait a toujours lieu si le degré de K est impair).

3. Définir toutes les racines de 1 qui peuvent appartenir à un corps de nombres algébriques de degré 4.

4. Déterminer toutes les unités du corps $\mathbf{Q}(\sqrt{3})$.

5. Montrer que dans le corps $\mathbf{Q}(\sqrt[3]{2})$ toutes les unités sont de la forme

$$\pm (1 + \sqrt[3]{2})^k.$$

6. Soit $\mathbf{K}$ un corps de nombres algébriques contenant une racine complexe de 1. Montrer qu'alors la norme de tout $\alpha \neq 0$ de K est positive.

§ 4. — LE GROUPE DES UNITÉS

1) Critère de complétude d'un lattice

Dans ce paragraphe, nous poursuivrons (et terminerons) l'étude de la structure du groupe des unités d'un ordre d'un corps algébrique. Le résultat fondamental que nous allons démontrer a déjà été énoncé à la fin du précédent paragraphe : le lattice $\mathfrak{G}$ dont les vecteurs sont les représentants des unités d'un ordre $\mathfrak{D}$ dans la représentation logarithmique est de dimension $s + t - 1$ (les notations sont celles du paragraphe précédent).

Le lattice $\mathfrak{G}$ est situé dans le sous-espace S de l'espace $\mathcal{R}^{s+t}$ formé des vecteurs $(A_{,}, \ldots, \lambda_{s+t})$ tels que $\lambda_1 + \ldots + \lambda_{s+t} = 0$. Puisque la dimension de S est égale à $s + t - 1$, il suffit de montrer que $\mathfrak{G}$ est un lattice complet de l'espace S. Nous Ctablirons ce résultat dans 3), en utilisant le critère ci-dessous de complétude d'un lattice.

THÉORÈME 1. — ***Un lattice $\mathcal{M}$ d'un espace vectoriel S est complet si et seulement s'il existe dans S un ensemble borné $\mathbf{U}$ dont les translatés par tous les vecteurs de $\mathcal{M}$ remplissent tout l'espace S (en se coupant éventuellement).***

DÉMONSTRATION. — Si le lattice $\mathcal{M}$ est complet, alors on peut prendre pour U un de ses parallélépipèdes fondamentaux : d'après le lemme 2 du § 3, tous les translatés d'un parallélépipède fondamental par les vecteurs d'un lattice complet remplissent l'espace. Supposons maintenant que le lattice $\mathcal{M}$ n'est pas complet et soit U un sous-ensemble borné quelconque de l'espace S. Montrons que les translatés de l'ensemble U par les vecteurs de $\mathcal{M}$ ne peuvent pas remplir tout l'espace S. Puisque U est borné, il existe un nombre réel $r > 0$ tel que $\| u \| < r$ pour tout $u \in$ U. Désignons par S le sous-espace engendré par les vecteurs du lattice $\mathcal{M}$; puisque le lattice $\mathcal{M}$ n'est pas complet, $\mathfrak{L}'$ est un sous-espace propre et par suite il existe des vecteurs $y \in$ S de longueur aussi grande que l'on veut orthogonaux au sous-espace S' (et par suite à tous les vecteurs de A). Montrons que ces vecteurs y tels que $\| y \| \geqslant r$ n'appartiennent pas aux translatés de U par les vecteurs de $\mathcal{M}$. En effet, si le vecteur y (orthogonal à S') est contenu dans un

certain translaté, alors il est de la forme y = $u + z$, $u \in U$, $z \in \mathcal{M}$. Mais alors d'après l'inégalité de Cauchy, nous avons

$$\| y \|^2 = (y, y) = (y, u) \leqslant \| y \| \, \| u \| < r \| y \|,$$

d'où $\| y \| < r$. Le **théorème** 1 est démontré (l'idée géométrique de la démonstration est que les translatés de l'ensemble U par les vecteurs d'un lattice incomplet sont dans la bande formée par les points dont la distance au sous-espace S' est inférieure ou égale à r).

Remarque. — En termes topologiques, la complétude du lattice $\mathcal{M}$ dans l'espace S est équivalente, comme on le voit facilement, à la **compacité** du groupe quotient $\mathfrak{L}/\mathcal{M}$ (S groupe topologique pour l'addition).

2) Lemme de Minkowski

La démonstration de l'existence de $s + t - 1$ unités indépendantes utilise un argument géométrique simple qui a de nombreuses applications en théorie des nombres. La formulation et la démonstration de ce résultat utilisent la notion de volume dans un espace n-dimensionne1 et ses **propriétés.**

Le volume $v(X)$ d'un sous-ensemble X d'un espace n-dimensionne1 $\mathcal{R}^n$ peut être défini comme la valeur de l'intégrale multiple

$$u(X) = \int \ldots \int dx_1 \, dx_2 \ldots dx_n,$$

étendue à l'ensemble X (ici, nous nous écarterons des notations (4) du § 3, en écrivant sous la forme $(x_1, \ldots, x_n)$ les coordonnées d'un point $x \in \mathcal{R}^n$). Nous n'étudierons pas ici les conditions d'existence du volume; dans les cas qui nous intéressent, l'ensemble X sera défini par des inégalités simples et l'existence du volume s'établira élémentairement. Remarquons les propriétés très simples suivantes du volume qui résultent des **propriétés** des intégrales (on suppose que tous les volumes considérés existent)

1° si $X \subset X'$, alors

$$v(X) \leqslant v(X') ;$$

2° si les ensembles X et X' sont disjoints

$$v(X \cup X') = u(X) + v(X') ;$$

3° par translation les ensembles conservent leur volume, i. e.

$$v(X + z) = v(X);$$

4° Soit α un nombre réel > 0. Désignons par αX l'ensemble des points de la forme ax pour $x \in X$ (l'ensemble αX est dit l'homothétique de X). Alors

$$v(\alpha X) = \alpha^n v(X).$$

Calculons le volume du parallélépipède fondamental T d'un lattice $\mathcal{M}$ construit sur la base e,, . . . , e_n. Soient

$$e_j = (a_{1j}, \ldots, a_{nj}) \qquad (1 \leqslant j \leqslant n).$$

Montrons que l'on a

$$v(T) = |\det (a_{ij})|. \tag{1}$$

Dans l'intégrale

$$v(T) = \int_{(T)} \ldots \int dx, \ldots dx_n,$$

faisons le changement de variable défini par les formules

$$x_i = \sum_{j=1}^{n} a_{ij} x'_j \qquad (1 \leqslant i \leqslant n).$$

Le jacobien de la transformation est égal au déterminant det (a_{ij}) qui est différent de zéro puisque les vecteurs e,, . . . , e_n sont indépendants. Puisque l'ensemble T a pour image par cette transformation l'ensemble T_0 des points $(x'_1, \ldots, x'_n)$ tels que $0 \leqslant x'_i < 1$ $(i = 1, \ldots, n)$, alors

$$v(T) = \int_{(T_0)} \ldots \int |\det (a_{ij})| \, dx'_1 \ldots dx'_n$$

$$= |\det (a_{ij})| \int_0^1 \ldots \int_0^1 dx'_1 \ldots dx'_n = |\det (a_{ij})|,$$

ce qui démontre la formule (1).

Soumettons l'espace $\mathbb{R}^n$ à une transformation linéaire régulière $x \to x'$. Le lattice $\mathcal{M}$ a pour image par cette transformation le lattice $\mathcal{M}'$ (qui est encore complet) et le parallélépipède fondamental T de $\mathcal{M}$ a pour image un parallélépipède T' du lattice $\mathcal{M}'$. Il est clair que le parallélépipède est construit sur les images $e'_1, \ldots, e'_n$ des vecteurs de la base e,, . . . , e,. Si

$$e'_j = (b_{1j}, \ldots, b_{nj}) \qquad (1 \leqslant j \leqslant n),$$

alors, d'après ce qui précède, le volume $v(T')$ est égal à $|\det (b_{ij})|$. Soit $C = (c_{ij})$ la matrice de la transformation linéaire $x \to x'$ dans la base $e_1, \ldots, e_n$, 1. e.

$$e'_j = \sum_{i-1}^{n} c_{ij} e_i \qquad (1 \leqslant j \leqslant n).$$

On voit facilement que $b_{ij} = \sum_{s=1}^{n} a_{is}c_{sj}$, i. e. la matrice (b_{ij}) est le produit de (a_{ij}) par (c_{ij}); on a donc la formule

$$v(\mathrm{T}') = v(\mathrm{T}) . |\det \mathrm{C}|. \qquad (2)$$

Supposons maintenant que $e_1, \ldots, e_n$ et $e'_1, \ldots, e'_n$ sont deux bases d'un même lattice $\mathcal{M}$. Puisque l'on passe de l'une à l'autre de ces bases par une transformation unimodulaire (i. e. dont la matrice C est à coefficients entiers et de déterminant ± 1), on a $v(\mathrm{T}') = \mathrm{u}(\mathrm{T})$, d'après (2). Ainsi le volume d'un parallélépipède fondamental d'un lattice dépend seulement du lattice et non de la base choisie.

Le rapprochement de la formule (1) et des égalités (9) et (10) du § 3 nous conduit à préciser ainsi le théorème 1 du § 3.

THÉORÈME 2. — ***Dans la représentation géométrique des nombres d'un corps*** K ***par les points de l'espace*** $\mathfrak{L}^{s,t} = \mathfrak{R}^n$ ***de dimension*** $n = s + 2t$, ***toutes les images des nombres d'un module complet*** M ***de discriminant*** D ***forment un lattice complet dont le volume d'un parallélépipède fondamental est égal à*** $2^{-t}\sqrt{|\mathrm{D}|}$.

Pour énoncer le résultat essentiel de ce point, nous avons besoin d'introduire deux nouvelles notions géométriques.

Un ensemble $\mathrm{X} \subset \mathfrak{R}^n$ est dit ***symétrique*** si avec tout point x il contient le point — x symétrique par rapport à l'origine.

Un ensemble X est dit convexe si avec tout couple de points x, x' $\in$ X il contient tous les points de la forme $\alpha x + (1 - \alpha)x'$, α étant un nombre réel quelconque tel que $0 \leqslant a \leqslant 1$. En d'autres termes, l'ensemble X est convexe s'il contient tout le segment joignant deux quelconques de ses points.

THÉORÈME 3 (lemme de Minkowski pour un ensemble convexe). — ***Dans l'espace*** $\mathfrak{R}^n$ ***de dimension*** n, ***soit donné un lattice complet*** $\mathcal{M}$ ***dont le volume d'un parallélépipède fondamental est égal à*** A; ***soit X un ensemble symétrique convexe borné, de volume*** $v(X)$. ***Si*** $v(X) > 2^n\Delta$, ***l'ensemble X contient au moins un point du lattice*** $\mathcal{M}$ ***différent de l'origine.***

DÉMONSTRATION. — Nous utiliserons la propriété intuitive suivante : si $\mathrm{Y} \subset \mathfrak{R}^n$ est un ensemble borné dont tous les translatés Y, = Y + z par les vecteurs $z \in \mathcal{M}$ sont disjoints, alors $v(\mathrm{Y}) \leqslant$ A. Pour démontrer ce résultat, choisissons un parallélépipède fondamental T du lattice $\mathcal{M}$ et considérons les intersections Y $\cap$ T-, de l'ensemble Y avec les translatés T_{-z} = T — z du parallélépipède T; il est clair que

$$v(y) = \sum_{z \in \mathcal{M}} v(y \cap \mathrm{T}\text{-}3$$

(dans cette somme, il y a seulement un nombre fini de termes non nuls puisque l'ensemble Y borné rencontre seulement un nombre fini des parallélépipèdes $\mathbf{T}_{-z}$, cf. lemme 3, § 3). Le translate de l'ensemble Y n $\mathbf{T}_{-z}$ par le vecteur z est égal à Y, $\cap$ T, c'est pourquoi $v(\mathrm{Y}\ n\ \mathbf{T}_{-z}) = v(\mathrm{Y}_z \cap \mathrm{T})$, d'où

$$v(\mathrm{Y}) = \sum_{z \in \mathcal{M}} v(\mathrm{Y}_z \cap \mathrm{T}).$$

Si maintenant les translatés Y, sont deux à deux disjoints, alors les intersections Y, n T sont deux à deux disjointes et puisqu'elles sont contenues dans T, la somme de la partie droite de l'égalité ci-dessus ne peut pas dépasser v(T). Par suite $v(\mathrm{Y}) \leqslant$ u(T), ce qui démontre notre argument.

Considérons maintenant l'ensemble $\frac{1}{2}\mathbf{X}$ (obtenu à partir de X par une homothétie de rapport $\frac{1}{2}$). Les conditions du théorème entraînent que

$$v\left(\frac{1}{2}\mathrm{X}\right) = \frac{1}{2^n} v(\mathrm{X}) > \Delta.$$

Si tous les translatés $\frac{1}{2}$ X + z par les vecteurs z $\in \mathcal{M}$ étaient deux à deux disjoints, alors, d'après ce qui précède, nous aurions $v\left(\frac{1}{2}\mathrm{X}\right) \leqslant$ A, ce qui n'est pas. Ainsi, pour certains vecteurs distincts z_1 et z_2 de $\mathcal{M}$, les ensembles $\frac{1}{2}\mathbf{X} + z_1$ et $\frac{1}{2}$ X + z_2 ont un point commun :

$$\frac{1}{2}x' + z_1 = \frac{1}{2}x'' + z^2 \qquad (x', x'' \in \mathrm{X}).$$

Écrivons cette égalité sous la forme

$$z_1 - z_2 = \frac{1}{2}x'' - \frac{1}{2}x',$$

Puisque l'ensemble X est symétrique, — x' $\in$ X et, d'après la convexité, nous avons aussi

$$\frac{1}{2}x'' - \frac{1}{2}x' = \frac{1}{2}x'' + \frac{1}{2}(-x') \in \mathrm{X}.$$

Ainsi le point $z_1 - z_2$ de $\mathcal{M}$, différent de l'origine appartient à l'ensemble X. C. Q. F. D.

Le raisonnement de la première partie de la démonstration du théorème 3 entraîne facilement le résultat suivant (qui sera utile au § 5).

LEMME 1. — *Si les translatés d'un ensemble Y par les vecteurs d'un lattice $\mathcal{M}$ remplissent tout l'espace $\mathcal{R}^n$, alors v(Y) $\geqslant$ A.*

En effet, les intersections $Y_z \cap T$ remplissent complètement le parallélépipède T (avec éventuellement des intersections non vides) et par suite

$$v(Y) = \sum_{z \in \mathcal{M}} v(Y_z \cap T) \geqslant v(T) = A.$$

Pour étudier le groupe des unités, nous appliquerons le lemme de Minkowski à un lattice de l'espace $\mathfrak{L}^{s,t}$ et à l'ensemble X formé des points x de la forme (2) du § 3 tels que

$$|x_1| < c_1, \ldots, |x_s| < c_s ; \qquad |x_{s+1}|^2 < c_{s+1}, \ldots, |x_{s+t}|^2 < c_{s+t},$$

$c_1, \ldots, c_{s+t}$ étant des nombres réels > 0. La symétrie et la convexité de cet ensemble X sont claires. Utilisant les notations (4) du § 3 pour les coordonnées de x, nous obtenons

$$v(X)^2 = \int_{-c_1}^{c_1} dx_1 \ldots \int_{-c_s}^{c_s} dx_s \iint\limits_{y_1^2+z_1^2<c_{s+1}} dy_1 dz_1 \ldots \iint\limits_{y_t^2+z_t^2<c_{s+t}} dy_t dz_t = 2^s \pi^t \prod_{i=1}^{s+t} c_i.$$

L'application du lemme de Minkowski à l'ensemble X donne le résultat suivant :

THÉORÈME 4. — *Si le volume d'un parallélépipède fondamental d'un lattice complet $\mathcal{M}$ de l'espace $\mathfrak{L}^{s,t}$ est égal à A et si les nombres réels positif $c_1, \ldots, c_{s+t}$ sont tels que $\prod_{i=1}^{s+t} c_i > \left(\frac{4}{\pi}\right)^t A$, alors il existe dans le lattice $\mathcal{M}$ un vecteur non nul tel que*

$$|x_1| < c_1, \ldots, |x_s| < c_s ; \quad |x_{s+1}|^2 < c_{s+1}, \ldots, |x_{s+t}|^2 < c_{s+t} \qquad (3)$$

3) Structure du groupe des unités

Nous pouvons maintenant préciser la structure du groupe des unités d'un ordre quelconque.

THÉORÈME 5 (théorème de Dirichlet). — *Soit $\mathfrak{D}$ un ordre d'un corps K de nombres algébriques de degré $n = s + 2t$. Il existe alors dans $\mathfrak{D}$ des unités*

$\varepsilon_1, \ldots, \varepsilon_r$, $r = s + t - 1$, telles que toute unité $\varepsilon \in \mathfrak{D}$ s'écrive de manière unique sous la forme

$$\varepsilon = \zeta \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r},$$

où $a_1, \ldots, a_r$ sont des entiers rationnels et ζ une racine de 1 contenue dans $\mathfrak{D}$.

DÉMONSTRATION. — Comme on l'a dit à la fin du paragraphe précédent et au début de celui-ci, il suffit d'établir que le lattice $\mathfrak{G}$ qui représente les unités de l'ordre $\mathfrak{D}$ dans l'espace $\mathfrak{L}$ (de dimension égale à $s + t - 1$) est complet. D'après le théorème 1, il suffit de montrer qu'il existe dans $\mathfrak{L}$ un ensemble borné U dont les translatés par tous les vecteurs de $\mathfrak{G}$ remplissent tout l'espace $\mathfrak{L}$.

Il est évident que tout point $(\lambda_1, \ldots, \lambda_{s+t})$ de $\mathfrak{L}$ (et aussi de $\mathfrak{R}^{s+t}$) est l'image d'un certain point $x \in \mathfrak{L}^{s,t}$ par l'application $x \to l(x)$. De plus, il résulte de manière évidente de la formule (15), § 3 que pour $x \in \mathfrak{L}^{s,t}$ (à composantes non nulles) son image l(x) dans l'espace logarithmique $\mathfrak{R}^{s+t}$ appartient au sous-espace $\mathfrak{L}$ si et seulement si $|\,N(x)\,| = 1$.

Nous désignerons par S l'ensemble de tous les points $x \in \mathfrak{L}^{s,t}$ tels que

$$|\,N(x)\,| = 1.$$

Si $\mathbf{X}_0$ est un sous-ensemble borné quelconque de S, alors son image $I(X_0)$ dans l'espace S est aussi bornée. En effet, pour tout point $x = (x_1, \ldots, x_{s+t})$ de norme ± 1, on a

$$|x_k| < c\,(1 \leqslant k \leqslant s), \qquad |x_{s+j}|^2 < c\,(1 \leqslant j \leqslant t);$$

alors $l_k(x) < \operatorname{Log} c$ pour tout $k = 1, \ldots, s + t$, et de plus

$$l_k(x) = -\sum_{i \neq k} l_i(x) > -(s + t - 1)c,$$

ce qui montre que $I(X_0)$ est borné. D'après la multiplicativité de la norme, pour $x \in S$ et $\mathbf{X}_0 \subset S$, le produit $\mathbf{X}_0 x$ est encore contenu dans S; en particulier, pour toute unité ε de l'ordre $\mathfrak{D}$, nous avons $\mathbf{X}_0 x(\varepsilon) \subset S$ (puisque

$$N(x(\varepsilon)) = N(E) = \pm 1).$$

Si les produits $\mathbf{X}_0 x(\varepsilon)$ remplissent S pour toutes les unités ε, alors les translatés $I(X_0) + l(\varepsilon)$ rempliront tout l'espace $\mathfrak{L}$. Ainsi, nous avons établi que pour démontrer le théorème 5, il suffit de trouver dans S un sous-ensemble borné $\mathbf{X}_0$ dont les translatés « multiplicatifs » $\mathbf{X}_0 x(\varepsilon)$ par les points $X(E)$ remplissent tout S.

Soient y un point quelconque de S et $\mathcal{M}$ le lattice de $\mathfrak{L}^{s,t}$ représentant les nombres de l'ordre $\mathfrak{D}$. Soumettons l'espace $\mathfrak{L}^{s,t}$ à l'application linéaire

$$x \to yx \qquad (x \in \mathfrak{L}^{s,t}).$$

Dans le § 3,1), nous avons vu que le déterminant de la matrice de cette application est égal à N(y), i. e. est égal à $\pm$ 1; ainsi, d'après la formule (2), les volumes des parallélépipèdes fondamentaux des lattices $\mathcal{M}$ et $y\mathcal{M}$ sont égaux; soit A ce volume.

Choisissons maintenant des nombres réels positifs $c_1, \ldots, c_{s+t}$ tels que

$$Q = c_1 \ldots c_{s+t} > \frac{4^t}{0\pi} \Delta,$$

et désignons par X l'ensemble des points $x \in \mathfrak{L}^{s,t}$ défini par les inégalités (3). D'après le théorème 4, il existe dans le lattice $y\mathcal{M}$ un point

$$x = yx(a) \neq 0 \qquad (\alpha \in \mathfrak{D},\ \alpha \neq 0)$$

appartenant à X. Puisque $N(x) = N(y)N(\alpha) = \pm N(a)$ et

$$|N(x)| < c_1 \ldots c_{s+t} = Q,$$

alors $|N(a)| < Q$. D'après le théorème 5 du § 2, il existe seulement dans l'ordre $\mathfrak{D}$ une quantité finie de nombres non associés deux à deux dont la valeur absolue de la norme soit inférieure à Q; soit $\alpha_1, \ldots, \alpha_N$ un système de nombres $\neq 0$ de $\mathfrak{D}$ tels que tout nombre non nul de $\mathfrak{D}$ dont la norme est inférieure à Q soit associé à l'un d'entre eux. Pour un certain i ($1 \leqslant i \leqslant N$), on aura $a(c) = \alpha_i, \varepsilon$ étant une Unité de $\mathfrak{D}$. Le point y peut alors s'écrire

$$y = xx(\alpha_i^{-1})x(\varepsilon). \tag{4}$$

Posons

$$X_0 = S \bigcap \left(\bigcup_{i=1}^{N} Xx(\alpha_i^{-1}) \right). \tag{5}$$

Puisque X est borné, tous les ensembles $Xx(\alpha_i^{-1})$ sont aussi bornés; ainsi X_0 est borné. De plus, le choix des nombres $c_1, \ldots, c_{s+t}$ qui définissent X et du système $\alpha_1, \ldots, \alpha_N$ est indépendant de y; ainsi l'ensemble (5) est défini sans ambiguïté par l'ordre $\mathfrak{D}$. Puisque y et $x(\varepsilon)$ appartiennent S, d'après (4), le point $xx(\alpha_i^{-1})$ appartient aussi à S et par suite à X_0. L'égalité (4) signifie que le point y $\in$ S (qui a été pris arbitrairement) appartient à l'ensemble $X_0 x(\varepsilon)$. Ainsi, quand ε parcourt l'ensemble des unités de $\mathfrak{D}$, les ensembles $X_0 x(\varepsilon)$ recouvrent S, ce qui démontre le théorème 5.

Comme nous l'avons déjà remarqué dans le § 3, 5), le théorème de Dirichlet entraîne que le groupe des unités de tout ordre $\mathfrak{D}$ d'un corps de nombres

algébriques de degré $n = s + 2t$ s'écrit comme produit direct d'un groupe fini et de $r = s + t - 1$ groupes cycliques infinis. Si $s + t = 1$ (c'est le cas du corps des nombres rationnels et de tout corps quadratique imaginaire), alors $r = 0$. Dans ce cas, le lattice $\mathfrak{G}$ est seulement formé du vecteur nul et le groupe des unités d'un ordre $\mathfrak{D}$ est un groupe fini de racines de l'unité.

Les unités $\varepsilon_1, \ldots, \varepsilon_r$ dont le théorème de Dirichlet établit l'existence s'appellent ***les unités fondamentales de l'ordre*** $\mathfrak{D}$. Il résulte du § 3-5) que des unités $\varepsilon_1, \ldots, \varepsilon_r$ sont fondamentales si et seulement si les vecteurs $l(\varepsilon_1), \ldots . l(\varepsilon_r)$ forment une base du lattice $\mathfrak{G}$. Les unités

$$\varepsilon_i' = \zeta_i \varepsilon_1^{a_{i1}} \ldots \varepsilon_r^{a_{ir}} \qquad (1 \leqslant i \leqslant r)$$

(où les ζ_i sont des racines de 1 quelconques contenues dans $\mathfrak{D}$) sont à leur tour fondamentales si et seulement si la matrice à coefficients entiers (a_i) est unimodulaire.

Remarque. — La démonstration du théorème de Dirichlet que nous avons exposée n'est pas « effective », en ce sens qu'elle ne donne pas d'algorithme pour trouver des systèmes d'unités fondamentales de l'ordre $\mathfrak{D}$. Cela résulte en particulier du fait que nous avons utilisé un système complet de nombres $\alpha_1, \ldots . \alpha_N$ non associés dont les normes sont inférieures ou égales à un certain nombre Q; la démonstration de l'existence d'un tel système était déjà non « effective » (théorème 5, § 2). Nous reviendrons sur cette question dans le paragraphe suivant.

Le théorème de Dirichlet (de même que le théorème 2 du $3) est en particulier vérifié pour l'ordre maximum $\mathfrak{D}$ du corps K. Les unités fondamentales de l'ordre maximum $\tilde{\mathfrak{D}}$ sont dites ***unités fondamentales du corps*** K ***de nombres algébriques.***

4) Régulateur

D'après le § 3, 3) et 4), à tout ordre $\mathfrak{D}$ d'un corps K de nombres algébriques de degré $n = s + 2t$ est associé un lattice $\mathfrak{G}$ de dimension $r = s + t - 1$ dans le sous-espace $\mathfrak{L} \subset \mathcal{R}^{s+t}$. Le volume v d'un parallélépipède fondamental de ce lattice ne dépend pas de la base choisie et il est donc complètement défini par l'ordre $\mathfrak{D}$. Calculons ce volume. Soit T_0 le parallélépipède fondamental du lattice $\mathfrak{G}$ construit sur la base $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ (ici $\varepsilon_1, \ldots, \varepsilon_r$ est un système d'unités fondamentales de l'ordre $\mathfrak{D}$). Le vecteur

$$l_0 = \frac{1}{\sqrt{s+t}} \times (1, \ldots, 1) \in \mathcal{R}^{s+t}$$

est orthogonal au sous-espace $\mathfrak{L}$ et de longueur égale à 1. Il est clair que le volume r-dimensionne1 $v = v(T_0)$ est égal au volume $(s + t)$-dimensionne1 du parallélépipède T construit sur les vecteurs $l_0, l(\varepsilon_1), \ldots, l(\varepsilon_r)$. Par suite, d'après la formule (1), le volume v est égal à la valeur absolue du déterminant dont les lignes sont formées par les composantes de ces vecteurs. Si dans ce déterminant nous ajoutons toutes les colonnes à la $i^{\text{ième}}$ colonne, nous obtenons, en appliquant à cette colonne la formule (18) du § 3,

$$v = \sqrt{s + t}\,R$$

où R est la valeur absolue d'un des mineurs d'ordre r de la matrice

$$\begin{pmatrix} l_1(\varepsilon_1) & \ldots & l_{s+t}(\varepsilon_1) \\ \cdot & \cdot & \cdot \\ l_1(\varepsilon_r) & \ldots & l_{s+t}(\varepsilon_r) \end{pmatrix} \tag{6}$$

Il en résulte en particulier que les valeurs absolues de tous les mineurs d'ordre r de la matrice (6) sont égaux entre eux et ne dépendent pas du choix du système $\varepsilon_1, \ldots, \varepsilon_r$ d'unités fondamentales. Le nombre R (de même que Y) dépend seulement de $\mathfrak{D}$ et s'appelle le ***régulateur de Z'ordre*** $\mathfrak{D}$.

Le régulateur de l'ordre maximum $\tilde{\mathfrak{D}}$ est aussi appelé le ***régulateur du corps*** K (dans le cas du corps des nombres rationnels ou d'un corps quadratique imaginaire, le régulateur est par définition égal à 1).

EXERCICES

1. Démontrer qu'il est impossible d'améliorer l'inégalité $o(X) > 2^n\Delta$ dans le lemme de Minkowski. Pour cela, on construira un ensemble X borné, convexe, symétrique par rapport à l'origine et de volume $2^n\Delta$ ne contenant aucun point du lattice à part l'origine.

2. Soit a un nombre réel positif. Démontrer que le volume de l'ensemble $X \subset \mathfrak{L}^{s,t}$ formé des points x tels que

$$|x_1| + \text{a--} + |x_s| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_t^2 + z_t^2} < a$$

(pour les coordonnées (4) du § 3) est égal à

$$u(X) = 2^s \frac{\pi^t}{n!} a_n.$$

Vérifier de plus que X est borne, convexe et symétrique par rapport à l'origine.

3. Soient a et b des entiers naturels qui ne sont pas des carrés. Montrer que toute unité fondamentale de l'ordre $\{1, \sqrt{a}\}$ du corps $\mathbf{Q}(\sqrt{a})$ est aussi une unité fondamentale de l'ordre $\{1, \sqrt{a}, \sqrt{-b}, \sqrt{a}\sqrt{-b}\}$ du corps $\mathbf{Q}(\sqrt{a}, \sqrt{-b})$.

4. Montrer que le groupe des unités d'un ordre $\mathfrak{D}$ est un sous-groupe d'indice fini du groupe des unités de l'ordre maximum $\tilde{\mathfrak{D}}$.

5. Soient $\eta_1, \ldots, \eta_r$ $(r = s + t - 1)$ des unités d'un ordre $\mathfrak{D}$ telles que les vecteurs $l(\eta_1), \ldots, l(\eta_r)$ soient linéairement indépendants. Montrer qu'alors le groupe des unités qui sont de la forme $\eta_1^{c_1} \ldots \eta_r^{c_r}$, où les c_i sont des entiers rationnels, est un sous-groupe d'indice fini du groupe de toutes les unités de l'ordre $\mathfrak{D}$.

6. Soient $c_1, \ldots, c_n$ des nombres réels positifs et (a_{ij}) une matrice réelle régulière d'ordre n. Démontrer que si $c_1 \ldots c_n > d = |\det (a_{ij})|$, alors il existe des entiers rationnels $x_1, \ldots, x_n$ non tous nuls tels que

$$\left| \sum_{j=1}^{n} a_{ij} x_j \right| < c_i \qquad (i = 1, \ldots, n)$$

INDICATION. — Montrer que dans l'espace $\mathfrak{R}^n$, l'ensemble des points $(x_1, \ldots, x_n)$ qui satisfont aux inégalités précédentes est borné, convexe, symétrique par rapport à l'origine et de volume $\frac{1}{d} 2^n c_1 \ldots c_n$. Appliquer alors le lemme de Minkowski.

7. Soient a_{ij} $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant n)$ des entiers rationnels et m_i $(1 \leqslant i \leqslant k)$ des entiers naturels. Démontrer que l'ensemble des points de l'espaces $\mathfrak{R}^n$ à coordonnées entières $(x_1, \ldots, x_n)$ telles que

$$\sum_{j=1}^{n} a_{ij} x_j \equiv 0 \pmod{m_i} \qquad (1 \leqslant i \leqslant k)$$

est un lattice complet dont le volume du parallélépipède fondamental est $\leqslant m_1 \ldots m_k$.

8. Soient a, b, c des nombres entiers rationnels non nuls, premiers entre eux deux à deux, sans carrés, et posons $|abc| = 2^\lambda p_1 \ldots p_s$ (les p_i sont des nombres premiers impairs et λ est égal à 0 ou à 1). On suppose que la forme $ax^2 + by^2 + cz^2$ représente zéro dans tous les corps p-adiques. Démontrer qu'il existe des formes linéaires à coefficients entiers $L_1, \ldots, L_s, L', L''$ de trois variables telles que des nombres entiers u, v, w vérifient la congruence

$$au^2 + bv^2 + cw^2 \equiv 0 \pmod{4\,|abc|}$$

dès que

$$\left.\begin{aligned} &L_i(u, v, w) \equiv 0 \pmod{p_i}, \qquad 1 \leqslant i \leqslant s \\ &L'(u, v, w) \equiv 0 \pmod{2^{1+\lambda}} \\ &L''(u, v, w) \equiv 0 \pmod{2} \end{aligned}\right\} (*)$$

9. Conservant les notations de l'exercice précédent, désignons par $\mathcal{M}$ le lattice des points à coordonnées entières $(u, v, w) \in \mathfrak{R}^3$ qui satisfont aux congruences (*). D'après l'exercice 7, le volume d'un parallélépipède fondamental du lattice $\mathcal{M}$ est inférieur à $4\,|abc|$. Désignons enfin par X l'ellipsoïde

$$|a| x^2 + |b| y^2 + |c| z^2 < 4\,|abc|,$$

dont le volume est égal, comme on le vérifie facilement, à $\frac{32}{3}\pi\,|abc|$. Appliquant le lemme de Minkowski pour un corps convexe à l'ellipsoïde X et au lattice $\mathcal{M}$, démontrer que la forme $ax^2 + by^2 + cz^2$ représente rationnellement zéro (Dans cette démonstration du théorème de Minkowski-Hasse pour une forme de trois variables, on n'a pas utilisé le fait que la forme est non définie).

§ 5. — SOLUTION DU PROBLÈME DES REPRÉSENTATIONS DES NOMBRES RATIONNELS PAR DES FORMES DÉCOMPOSABLES COMPLÈTES

1) Unités de norme + 1

Au § 2, 3), nous avons vu que la recherche dans un certain module complet des nombres de norme donnée conduisait à l'étude des unités de l'anneau de stabilisateurs $\mathfrak{D}$ telles que $N(E) = +1$. Ces unités forment un groupe que nous allons étudier.

Supposons tout d'abord que le degré n du corps K est impair. Dans ce cas, il existe seulement dans l'anneau $\mathfrak{D}$ deux racines de 1 qui sont les nombres ± 1 (exercice 2 du § 3). Si pour une certaine unité $\varepsilon \in \mathfrak{D}$, nous avons $N(E) = -1$, alors

$$N(-\varepsilon) = N(-1)N(\varepsilon) = (-1)^n(-1) = 1.$$

Soient $\varepsilon_1, \ldots, \varepsilon_r$ $(r = s + t - 1)$ un système d'unités fondamentales de l'anneau $\mathfrak{D}$. Il se peut que certaines des unités ε soient de norme -1; remplaçant ces unités ε par $-\varepsilon_i$, nous obtenons un nouveau système $\eta_1, \ldots, \eta_r$ d'unités fondamentales telles que $N(\eta_i) = 1$ pour tout $i = 1, \ldots, r$. La norme d'une unité quelconque

$$\varepsilon = \pm \eta_1^{a_1} \ldots \eta_r^{a_r}$$

est alors égale à $N(\pm 1) = (\pm 1)^n = \pm 1$. Par suite toutes les unités $\varepsilon \in \mathfrak{D}$ telles que $N(E) = 1$ s'écrivent

$$\varepsilon = \eta_1^{a_1} \ldots \eta_r^{a_r} \qquad (a_i \in \mathbf{Z}).$$

Supposons maintenant n pair. Montrons que la norme de toute racine de 1 contenue dans K est égale à + 1. C'est évident pour les racines ± 1; si K contient une racine complexe ζ de 1, alors $s = 0$ et par suite tous les isomorphismes du corps K dans le corps des nombres complexes se décomposent en paires d'isomorphismes complexes conjugués. Pour une telle paire σ et $\bar{\sigma}$ nous avons $\sigma(\zeta)\bar{\sigma}(\zeta) = |\sigma(\zeta)|^2 = 1$. D'après le \$2, 3) de l'appendice, nous obtenons donc bien $N(\zeta) = 1$.

Soit encore $\varepsilon_1, \ldots, \varepsilon_r$ un système d'unités fondamentales de l'anneau $\mathfrak{D}$. Si $N(\varepsilon_i) = 1$ pour tout $i = 1, \ldots, r$, la norme de toute unité $\varepsilon \in \mathfrak{D}$ est égale à + 1. Supposons maintenant que

$$N(\varepsilon_1) = 1, \ldots, N(\varepsilon_k) = 1, \qquad N(\varepsilon_{k+1}) = -1, \ldots, N(E_s) = -1$$

pour $k < r$. Posant

$$\eta_1 = \varepsilon_1, \ldots, \eta_k = \varepsilon_k, \qquad \eta_{k+1} = \varepsilon_{k+1}\varepsilon_r, \ldots, \eta_{r-1} = \varepsilon_{r-1}\varepsilon_r,$$

nous obtenons un nouveau système d'unités fondamentales $\eta_1, \ldots, \eta_{r-1}, \varepsilon_r$ telles que $N(\eta_i) = 1$, $1 \leqslant i \leqslant r - 1$. Cherchons à quelle condition la norme de l'unité $\varepsilon = \zeta\eta_1^{a_1} \ldots \eta_{r-1}^{a_{r-1}}\varepsilon_r^b$ $(a_1, \ldots, a_{r-1}, b \in Z)$ est égale à $+1$. Puisque $N(\varepsilon) = (-1)^b$, $N(\varepsilon) = +1$ si et seulement si l'exposant b est pair, i. e. $b = 2a_r$. Nous avons ainsi obtenu que, pour n pair, une unité quelconque $\varepsilon \in \mathfrak{D}$ de norme $+1$ s'écrit

$$\varepsilon = \zeta\eta_1^{a_1} \ldots \eta_{r-1}^{a_{r-1}}\eta_r^{a} \qquad (a_i \in \mathbf{Z})$$

avec $\eta_r = \varepsilon_r^2$ et ζ racine quelconque de 1 appartenant à $\mathfrak{D}$.

Ainsi, si on connaît un système d'unités fondamentales de l'ordre $\mathfrak{D}$, on peut trouver toutes les unités de norme + 1.

2) Forme générale des solutions de l'équation $N(\mu) = a$

Rapprochant le corollaire du théorème 5, § 2 du résultat ci-dessus, nous pouvons énoncer le théorème suivant qui donne une description complète des solutions de l'équation (7) du § 2.

THÉORÈME 1. — *Soient M un module complet d'un corps K de nombres algébriques de degré $n = s + 2t$, $\mathfrak{D}$ son anneau de stabilisateurs et $a \neq 0$ un nombre rationnel. Il existe dans l'ordre $\mathfrak{D}$ des unités $\eta_1, \ldots, \eta$ $(r=s+t-1)$ de norme $+1$ et dans le module M un système fini (éventuellement vide) de nombres $\mu_1, \ldots, \mu_k$ de normes a, tels que toute solution $\mu \in M$ de l'équation*

$$N(\mu) = a \tag{1}$$

s'écrive de manière unique sous la forme

$$\mu = \mu_i\eta_1^{a_1} \ldots \eta_r^{ar} \qquad \textit{si } n \textit{ impair}$$

$$\mu = \mu_i\zeta\eta_1^{a_1} \ldots \eta_r^{a_r} \qquad \textit{si } n \textit{ pair.}$$

Ici μ_i est un des nombres $\mu_1, \ldots, \mu_k$, ζ est une racine de 1 et $a_1, \ldots, a_r$ sont des entiers rationnels.

Dans le cas n pair, prenant pour nouveau système de nombres μ_i l'ensemble des produits $\mu_i\zeta$, nous obtenons pour μ la même représentation que dans le cas n impair.

Dans tout ordre d'un corps quadratique imaginaire, il existe seulement un nombre fini d'unités (puisque $r = s + t - 1 = 0$). Par suite, dans ce

cas, l'équation (1) a seulement un nombre fini de solutions. Si maintenant K n'est pas un corps quadratique imaginaire (et K différent du corps des nombres rationnels), alors $r > 0$ et par suite l'équation (1) ou bien n'a pas de solutions ou bien a une infinité de solutions.

Remarque. — Le théorème 1 décrit la structure des solutions de l'équation (1) mais ne nous donne pas le moyen de déterminer explicitement toutes ces solutions. Pour résoudre dans la pratique l'équation (1), il faut trouver un système d'unités fondamentales de l'ordre $\mathfrak{D}$ et un système complet de nombres $\mu_1, \ldots, \mu_k$ de M, non associés deux à deux, de norme donnée. Nous montrerons dans les points suivants qu'on peut résoudre effectivement ces deux problèmes par un nombre fini d'opérations; cependant, cette méthode est peu utilisable dans les cas pratiques car les calculs sont très compliqués. Nous exposerons cette méthode dans le cas des corps quadratiques.

3) Recherche effective d'un système d'unités fondamentales

Désignant par $\sigma_1, \ldots, \sigma_n$ les isomorphismes du corps K de nombres algébriques dans le corps des nombres complexes, démontrons tout d'abord le lemme suivant.

LEMME 1. — ***Soient*** $c_1, \ldots, c_n$ ***des nombres réels*** > 0 ***quelconques. Dans tout module complet*** M ***du corps*** K ***il existe seulement un nombre fini d'éléments*** $a \in$ M ***tels que***

$$|\sigma_1(\alpha)| < c_1, \ldots, |\sigma_n(\alpha)| < c_n, \tag{2}$$

et on peut les calculer explicitement.

DÉMONSTRATION. — Soit $\alpha_1, \ldots, a_n$ une base de M (si le module M est défini par un système de générateurs qui ne constituent pas une base, on peut, en un nombre fini d'étapes, construire une base de M; cf. démonstration du théorème 1 du § 2). Tout nombre $a \in$ M peut s'écrire

$$a = a_1\alpha_1 + \ldots + a_n\alpha_n, \tag{3}$$

a_j entiers rationnels. Construisons la base duale $\alpha_1^*, \ldots, \alpha_n^*$ de la base $\alpha_1, \ldots, a_n$ dans le corps K (cf. appendice § 2-3)) et soit A un nombre réel > 0 tel que

$$|\sigma_i(\alpha_j^*)| \leqslant A \tag{4}$$

pour tout i, j. Multipliant (3) par α_j^* et passant à la trace, nous obtenons

$$a_j = \mathrm{Tr}\ \alpha\alpha_j^* = \sum_{i=1}^{n} \sigma_i(\alpha)\,\sigma_i(\alpha_j^*).$$

Si $\alpha \in M$ satisfait à la condition (2), alors on a, d'après (4), la majoration suivante des coefficients a_j :

$$|a_j| \leqslant A\sum_{i=1}^{n} |\sigma_i(\alpha)| < A\sum_{i=1}^{n} c_i. \qquad (5)$$

Par suite, il y a seulement un nombre fini d'entiers a_j possibles. Considérant tous les nombres de la forme (3) qui vérifient (5), nous trouverons alors facilement ceux qui satisfont aux inégalités (2).

Dans la suite et jusqu'à la fin de ce point, nous utiliserons les mêmes notations et notions que dans les deux paragraphes précédents.

La possibilité de construire effectivement un système d'unités fondamentales d'un ordre quelconque d'un corps de nombres algébriques repose sur le théorème suivant.

THÉORÈME. — ***Pour tout ordre $\mathfrak{D}$ d'un corps K de nombres algébriques, on peut trouver un nombre réel $\rho > 0$ tel que la boule de rayon ρ de l'espace logarithmique R^{s+t} contienne au moins une base du lattice $\mathfrak{G}$*** (représentant les unités de l'ordre $\mathfrak{D}$).

Montrons que ce théorème donne « effectivement » une méthode de construction d'un système d'unités fondamentales de l'ordre $\mathfrak{D}$. Si la représentation logarithmique I(E) d'une unité $\varepsilon \in \mathfrak{D}$ est contenue dans la boule de rayon ρ, alors

$$|\sigma_k(\varepsilon)| < e^{\rho} \ (1 \leqslant k \leqslant s), \qquad |\sigma_{s+j}(\varepsilon)| < e^{\frac{\rho}{2}} \ (1 \leqslant j \leqslant t). \qquad (6)$$

D'après le lemme 1, le nombre d'unités de $\mathfrak{D}$ qui satisfont à cette condition est fini et on peut trouver explicitement ces unités (pour reconnaître les unités parmi les nombres de $\mathfrak{D}$, on utilise le théorème 4 du § 2). Constituons, avec les unités trouvées, tous les systèmes possibles

$$\varepsilon_1, \ldots, \varepsilon_r \qquad (r = s + t - 1)$$

d'unités tels que les vecteurs $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ soient linéairement indépendants. D'après le théorème 2, un au moins de ces systèmes est un système fondamental d'unités de l'ordre $\mathfrak{D}$. Pour le trouver, calculons le volume du parallélépipède construit sur les vecteurs $l(\varepsilon_1), \ldots, l(\varepsilon_r)$. Le système pour lequel ce volume est le plus petit sera, c'est clair, un système d'unités fondamentales.

La démonstration du théorème 2 résulte de manière évidente des deux lemmes ci-dessous relatifs au lattice $\mathfrak{G}$. D'après le lemme 1, on sait trouver « effectivement » toutes les unités ε telles que I(E) appartienne à un ensemble borné donné. Plus précisément, nous considérerons qu'un lattice $\mathfrak{G}$ est donné « effectivement » si on connaît un algorithme permettant de trouver tous les points de ce lattice qui appartiennent à un ensemble borné donné.

LEMME 2. — *Si un lattice complet $\mathcal{M}$ de l'espace m-dimensionne1 $\mathcal{R}^m$ est donné « effectivement », et si on connaît le volume* A *d'un parallélépipède fondamental,* alors *on peut trouver un nombre* ρ *tel qu'il existe une base du lattice $\mathcal{M}$ dans la boule de rayon p.*

DÉMONSTRATION. — Si $m = 1$, on peut poser $\rho = 2$ A. Dans le cas général, nous procéderons par récurrence sur m. Choisissons dans $\mathcal{R}^m$ un ensemble borné, symétrique par rapport à l'origine et convexe dont le volume est supérieur à $2^m\Delta$. D'après le lemme de Minkowski (§ 4, 2)) cet ensemble contient au moins un vecteur non nul du lattice $\mathcal{M}$; soit u un tel vecteur qui ne soit pas de la forme nx, pour n entier > 1 et $x \in \mathcal{M}$. Soit $\mathfrak{L}'$ le sous-espace orthogonal au vecteur u et soit $\mathcal{M}'$ la projection du lattice $\mathcal{M}$ sur C'. Si $x' \in \mathcal{M}'$, alors pour un certain $x \in \mathcal{M}$, nous avons $x = Eu + x'$, ξ réel. Pour tout entier k, le vecteur $x - ku$ appartient aussi à $\mathcal{M}$; par suite, on peut choisir le vecteur $x \in \mathcal{M}$ (dont la projection x' est donné) tel que $|\xi| < \frac{1}{2}$. Pour un tel x, on aura

$$\| x \|^2 = \xi^2 \| u \|^2 + \| x' \|^2 \leqslant \frac{1}{4} \| u \|^2 + \| x' \|^2.$$

Cette inégalité montre que tous les vecteurs $x' \in \mathcal{M}'$ appartenant à un ensemble borné sont les projections des vecteurs $x \in \mathcal{M}$ qui appartiennent également à un ensemble borné. Ainsi, avec le lattice $\mathcal{M}$, le lattice $\mathcal{M}'$ est donné « effectivement ». Si $u_2, \ldots, u_m$ sont des vecteurs de $\mathcal{M}$ dont les projections $u_2', \ldots, u_m'$ forment une base de $\mathcal{M}'$, alors le système $u_1, u_2, \ldots, u_m$ est une base de $\mathcal{M}$. Il en résulte que le volume d'un parallélépipède fondamental du lattice $\mathcal{M}'$ est égal à $\frac{\Delta}{\| u \|}$ et donc est connu. Par hypothèse de récurrence, on peut trouver un nombre p' tel qu'il existe une base $u_2', \ldots, u_n'$ de $\mathcal{M}'$ telle que $\| u_i' \| < \rho'$ $(i = 1, \ldots, m)$. D'après ce qui a été vu, on peut trouver des vecteurs $u_2, \ldots, u_m$ de $\mathcal{M}$ tels que

$$\| u_i \| < \left(\frac{1}{4} \| u \|^2 + \rho'^2 \right)^{1/2}.$$

Prenant

$$\rho = \max \left(\| u \| + 1, \left(\frac{1}{4} \| u \|^2 + \rho'^2 \right)^{1/2} \right),$$

il est clair que u, $u_2, \ldots, u_m$ est une base du lattice $\mathcal{M}$ contenue dans la boule de rayon p. Ceci démontre le lemme 2.

Pour démontrer le théorème 2, il suffit maintenant de majorer le volume d'un parallélépipède fondamental du lattice $\mathfrak{G}$.

LEMME 3. — ***Le volume v d'un parallélépipède fondamental du lattice*** $\mathfrak{G}$ ***satisfait à l'inégalité***

$$v \leqslant C\,(\operatorname{Log} Q)^{s+t-1} N \leqslant C\,(\operatorname{Log} Q)^{s+t-1} \sum_{a=1}^{[Q]} a^n, \quad \text{où} \quad Q = \left(\frac{2}{\pi}\right)^t \sqrt{|D|} + 1,$$

(D ***est le discriminant de l'ordre*** $\mathfrak{D}$), ***N le nombre d'éléments*** α ***de*** $\mathfrak{D}$, ***non associés deux v deux tels que*** $|N(a)| \leqslant Q$ ***et C une certaine constante qui dépend seulement de*** $s+t$).

DÉMONSTRATION. — Nous utiliserons ici les notations de la démonstration du théorème 5 du § 4. Nous imposerons aux nombres réels $c_1, \ldots, c_{s+t}$ la condition

$$c_1 \ldots c_{s+t} = \left(\frac{4}{\pi}\right)^t \Delta + 1 = \left(\frac{2}{\pi}\right)^t \sqrt{|D|} + 1 = Q.$$

Puisque tous les translatés de l'ensemble $l(X_0)$ par les vecteurs du lattice $\mathfrak{G}$ remplissent $\mathfrak{L}$, alors, d'après le lemme 1 du § 4, nous avons

$$v \leqslant v(l(X_0)).$$

Désignons par U_i ($i = 1, \ldots, N$) l'intersection de l'ensemble $Z(X) - l(\alpha_i)$ avec le sous-espace C. D'après (5) § 4, les ensembles U_i recouvrent $l(X_0)$, d'où

$$v \leqslant \sum_{i=1}^{N} v(U_i). \tag{7}$$

Revenons sur le calcul du volume $v(U_i)$. L'intersection de l'ensemble $I(X) - I(a)$ avec le sous-espace $\mathfrak{L}$ est formée des points $(\lambda_1, \ldots, \lambda_{s+t}) \in \mathfrak{R}^{s+t}$ tels que

$$\begin{gathered} \lambda_1 + \ldots + \lambda_{s+t} = 0, \\ \lambda_k < \operatorname{Log} C_k - l_k(\alpha) \qquad (1 \leqslant k \leqslant s+t). \end{gathered} \tag{8}$$

Posons $|N(a)| = a$ (d'où $\Sigma l_k(\alpha) = \operatorname{Log} a$) et translatons l'ensemble U par le vecteur $(\lambda_1^*, \ldots, \lambda_{s+t}^*) \in \mathfrak{L}$ de composantes

$$\lambda_k^* = -\operatorname{Log} c_k + l_k(\alpha) + \frac{1}{s+t} \operatorname{Log} \frac{Q}{a}.$$

Soit U* ce translaté; d'après (8), U* est défini par les conditions

$$\lambda_k < \frac{1}{s+t} \operatorname{Log} \frac{Q}{a} \qquad (1 \leqslant k \leqslant s+t).$$

Désignons par U_0 l'ensemble de $\mathfrak{L}$ défini par les inégalités

$$\lambda_k < 1 \qquad (1 \leqslant k \leqslant s+t),$$

et par C_0 le volume de cet ensemble. Il est clair que la constante C_0 dépend seulement de $s+t$. Puisque U* est obtenue à partir de U_0 par une homothétie de rapport $\frac{1}{s+t}\operatorname{Log}\frac{Q}{a}$, alors

$$v(U^*) = \frac{1}{s+t}\left(\operatorname{Log}\frac{Q}{a}\right)^{s+r-1} v(U_0),$$

d'où

$$v(U) = C_0\left(\frac{1}{1+t}\operatorname{Log}\frac{Q}{a}\right)^{s+t-1}. \tag{9}$$

Revenons à l'inégalité (7). Pour tout $i = 1, \ldots, N$ la norme $N(\alpha_i)$ satisfait à l'inégalité $1 \leqslant N(\alpha_i) \leqslant |Q|$. De plus, d'après la démonstration du théorème 5 du § 2, nous savons qu'il existe dans l'anneau $\mathfrak{D}$ au plus a^n nombres deux à deux non associés de normes Cgales à a en valeur absolue. Rapprochant ces résultats de l'inégalité (7) et de la formule (9), nous obtenons pour v l'estimation du lemme.

4) Nombres de norme donnés dans un module

Revenons maintenant à la question de la construction effective dans un module d'un système complet de nombres de norme donnée non associés deux à deux.

Dans l'anneau $\mathfrak{D}$ des stabilisateurs du module complet M, fixons un certain système d'unités fondamentales $\varepsilon_1, \ldots, \varepsilon_r$. Les vecteurs $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ et le vecteur $l_0=(1, \ldots, 1)$ forment une base de l'espace logarithmique $\mathfrak{R}^{s+t}$. Ainsi, pour tout $\mu \in M$, le vecteur $l(\mu)$ peut s'écrire

$$l(\mu) = \xi l_0 + \sum_{i=1}^{r} \xi_i l(\varepsilon_i), \tag{10}$$

pour des coefficients réels $\xi, \xi_1, \ldots, \xi_r$. D'après les formules (17) et (18) du § 3, le coefficient ξ est donné par

$$\xi = \frac{1}{s+t}\operatorname{Log}|N(\mu)|.$$

Tous les nombres réels ξ_i peuvent s'écrire sous la forme $\xi_i = k_i + \gamma_i$, où k_i est un entier et $|\gamma_i| \leqslant \frac{1}{2}$. Si $\mu' = \mu\varepsilon_r^{-k_r} \ldots \varepsilon_2^{-k_2}$ est un nombre associé à μ, la décomposition (10) s'écrit

$$l(\mu') = \frac{\operatorname{Log} a}{s+t} l_0 + \gamma_1 l(\varepsilon_1) + \ldots + \gamma_r l(\varepsilon_r),$$

avec a = $|\,N(\mu)\,| = |\,N(\mu')\,|$. Nous avons donc établi l'existence dans $\mathcal{R}^{s+t}$ d'un ensemble borné tel que pour tout $\mu \in M$ de norme $|\,N(\mu)\,| = a$, il existe un nombre μ' associé à μ qui appartient à cet ensemble. Nous avons ainsi des estimations du type (2) pour ces nombres μ'. D'après le lemme 1, il est clair qu'on peut déterminer explicitement tous les nombres de M qui satisfont à ces inégalités. Choisissant parmi ceux-ci les nombres dont la norme $N(\mu')$ a la valeur demandée et prenant un seul représentant pour les nombres associés entre eux, nous avons bien obtenu un système de nombres $\mu_1, \ldots, \mu_k \in M$ de norme donnée, non associés deux à deux tels que tout $\mu \in M$ de même norme soit associé à l'un d'entre eux.

Les résultats de ce paragraphe donnent une méthode permettant de trouver, au bout d'un nombre fini d'opérations, tous les nombres de norme donnée d'un module complet (ou de démontrer qu'il n'en existe pas). Nous avons entièrement résolu le problème de la représentation des nombres rationnels par des formes décomposables complètes à coefficients entiers.

EXERCICES

1. Soit d un nombre entier rationnel sans carrés et divisible par au moins un nombre premier de la forme $4k + 3$. Démontrer qu'alors la norme de toute unité de l'ordre $\{1, \sqrt{d}\}$ du corps $\mathbf{Q}(\sqrt{d})$ est égale à $+1$.

2. Montrer que $5 + 2\sqrt{6}$ est une unité fondamentale de l'ordre maximum du corps $\mathbf{Q}(\sqrt{6})$.

3. Trouver toutes les solutions en nombres entiers de l'équation

$$3x^2 - 4y^2 = 11.$$

4. Montrer que dans le corps cubique Q(0), $\theta^3 = 6$, le nombre $\varepsilon = 1 - 6\theta + 3\theta^2$ est une unité fondamentale.

§ 6. — CLASSES DE MODULES

Dans le § 1, 3), on a défini la notion de modules semblables pour des modules d'un même corps K. On a vu que des modules semblables ont le même anneau de stabilisateurs (lemme 1, § 2) et que les problèmes de la recherche des nombres de norme donnée sont équivalents dans des modules semblables (§ 1, 3)). Il est donc naturel de grouper tous les modules semblables en classes et de considérer l'ensemble des classes de modules semblables. Dans ce paragraphe, nous démontrerons que dans un corps K de nombres algébriques, il existe seulement un nombre fini de classes de modules sem-

blables associés (*) à un ordre donné $\mathfrak{D}$. Ce résultat, de même que le théorème de Dirichlet sur les unités, est essentiel dans la théorie des nombres algébriques. Sa démonstration, de même que celle du théorème sur les unités, repose sur le lemme de Minkowski. Une notion essentielle ici sera la norme d'un module.

1) Norme d'un module

Soit M un module complet d'un corps K de nombres algébriques de degré n; désignons par $\mathfrak{D}$ son anneau de stabilisateurs. Choisissons dans $\mathfrak{D}$ une base $\omega_1, \ldots, \omega_n$ et dans le module M une base $\mu_1, \ldots, \mu_n$. La matrice de passage $A = (a_{ij})$ de la première base à la seconde, i. e. la matrice définie par les égalités

$$\mu = \sum_{i=1}^{n} a_{ij}\omega_j \qquad (1 \leqslant j \leqslant n,\ a_{ij} \in \mathbf{Q}), \tag{1}$$

dépend, bien entendu, non seulement du module M mais aussi du choix des bases ω_i et μ_i. Soient $\omega_1', \ldots, \omega_n'$ et $\mu_j', \ldots, \mu_n'$ des autres bases des modules $\mathfrak{D}$ et M respectivement, et soit

$$\mu_j' = \sum_{i=1}^{n} a_{ij}'\omega_j' \qquad (a_{ij}' \in \mathbf{Q}).$$

La matrice $A' = (a_{ij}')$ est liée à la matrice A par la relation

$$A' = CAD \tag{2}$$

où $C = (c_{ij})$ et $D = (d_{ij})$ sont des matrices unimodulaires à coefficients entiers définies par les égalités :

$$\omega_j = \sum_{i=1}^{n} c_{ij}\omega_j', \qquad \mu_j' = \sum_{i=1}^{n} d_{ij}\mu_i \qquad (c_{ij}d_{ij} \in \mathbf{Q})$$

(comme nous le savons, la matrice de passage d'une base d'un module à une autre est toujours unimodulaire). Ainsi la valeur absolue du déterminant de la matrice A, qui est indépendant du choix des bases ω et μ_j, est un invariant qui dépend seulement du module M; en effet

$$|\det A_1| = |\det C| \cdot |\det A| \cdot |\det D| = |\det A|.$$

(*) Rappelons qu'un module est dit associé à un ordre $\mathfrak{D}$ s'il admet cet ordre pour anneau de stabilisateurs (N. d. T.).

DÉFINITION. — ***Soient*** M ***un module complet dans*** K ***et*** $\mathfrak{D}$ ***son anneau de stabilisateurs. La valeur absolue du déterminant de la matrice de passage d'une base de l'anneau*** $\mathfrak{D}$ ***à une base du module*** M ***s'appelle la norme du module et se désigne par*** N(M).

D'après la formule (12) du § 2 de l'appendice, les discriminants

$$D = D(\mu_1, \ldots, \mu_n) \qquad \text{et} \qquad D_0 = D(\omega_1, \ldots, \omega_n)$$

des bases μ_i et ω_i (i. e. les discriminants des modules M et $\mathfrak{D}$, cf. § 2-5)) sont liés entre eux par la relation $D = D_0 (\det A)^2$. La notion de norme permet d'écrire cette formule :

$$D = D_0 N(M)^2. \tag{3}$$

Pour des modules contenus dans leur anneau de stabilisateurs, la matrice (a_{ij}) définie par les formules (1) est à coefficients entiers et par suite la norme de ces modules est un nombre entier. La signification de la norme dans ce cas est précisée par le théorème suivant.

THÉORÈME 1. — ***Si un module complet*** M ***est contenu dans son anneau de stabilisateurs*** $\mathfrak{D}$, ***alors sa norme*** N(M) ***est égale à l'indice*** $(\mathfrak{D} : M)$.

Ce théorème est un cas particulier du lemme suivant.

LEMME 1. — ***Si*** M_0 ***est un groupe abélien de rang n dont aucun élément n'est d'ordre fini, et si*** M ***est un sous-groupe de même rang n, alors l'indice*** $(M_0 : M)$ ***est fini et égal à la valeur absolue du déterminant de la matrice de passage*** A ***d'une base de*** M_0 à ***une base de*** M.

DÉMONSTRATION. — Soit $\omega_1, \ldots, \omega_n$ une base de M,. D'après le théorème 2 du § 2, il existe dans le sous-groupe M une base $\eta_1, \ldots, \eta_n$ de la forme

$$\left.\begin{aligned} \eta_1 &= c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1n}\omega_n \\ \eta_2 &= \qquad c_{22}\omega_2 + \ldots + c_{2n}\omega_n \\ &\cdots\cdots\cdots\cdots\cdots \\ \eta_n &= \qquad\qquad\qquad c_{nn}\omega_n \end{aligned}\right\}$$

où les c_{ij} sont des entiers rationnels et $c_{ij} > 0$ $(1 \leqslant i \leqslant n)$. Il est clair que det A ne dépend pas du choix des bases dans M_0 et dans M et par suite

$$|\det A| = c_{11}c_{22} \ldots c_{,,}.$$

Considérons les éléments

$$x_1\omega_1 + \ldots + x_n\omega_n, \qquad 0 \leqslant \mathrm{Xi} < c_{ii} \qquad (1 \leqslant i \leqslant n) \tag{4}$$

et montrons qu'ils forment un système complet de représentants des 'classes du quotient du groupe M_0 par le sous-groupe M. Soit

$$a = a_1\omega_1 + \ldots + a_n\omega_n$$

un élément quelconque de M,. Divisons a_1 par c_{11} :

$$a_1 = c_{11}q_1 + x_1, \qquad 0 \leqslant x_1 < c_1.$$

Alors,

$$\alpha - q_1\eta_1 - x_1\omega_1 = a_2'\omega_2 + \ldots + a_n'\omega_n.$$

Si maintenant nous divisons a_2' par c_{22}, $a_2' = c_{22}q_2 + x_2$, nous obtenons

$$\alpha - q_1\eta_1 - q_2\eta_2 - x_1\omega_1 = a_3''\omega_3 + \ldots + a_n''\omega_n.$$

Répétant ce processus n-fois, nous obtenons finalement

$$\alpha - q_1\eta_1 - \ldots - q_n\eta_n - x_1\omega_1 - \ldots - x_n\omega_n = 0,$$

où q_i et x_i sont des entiers rationnels tels que $0 \leqslant x_i < c_{ii}$. Puisque

$$q_1\eta_1 + \ldots + q_n\eta_n$$

appartient à M, cette égalité indique que α et l'élément $x_1\omega_1 + \ldots + x_n\omega_n$ appartiennent à la même classe résiduelle selon le sous-groupe M. Ainsi, dans toute classe résiduelle de $\mathbf{M_0}$ selon M, il existe un représentant de la forme (4). Il reste à vérifier que des éléments distincts de la forme (4) définissent des classes résiduelles distinctes. Raisonnant par l'absurde, supposons que la différence de deux éléments distincts $x_1\omega_1 + \ldots + x_n\omega_n$ et $x_1'\omega_1 + \ldots + x_n'\omega_n$ (de la forme (4)) appartient à M. Soit s le plus petit indice ($1 \leqslant s \leqslant n$) pour lequel $x_s \neq x_s'$. Alors

$$(x_s - x_s')\omega_s + \ldots + (x_n - x_n')\omega_n = b_1\eta_1 + \ldots + b_n\eta_n$$

pour des entiers b_i. Remplaçant $\eta_1, \ldots, \eta_n$ par leurs expressions en fonction des ω_i et comparant les coefficients de ω_i dans les deux nombres de cette égalité, on obtient facilement que $b_1 = 0, \ldots, b_{s-1} = 0$ et $c_{ss}b_s = x_s - x_s'$. Cette dernière égalité est impossible pour un entier b_s puisque $0 < x_s - x_s' < c_{ss}$. Ainsi les éléments de la forme (4) forment bien un système complet de représentants des classes résiduelles de $\mathbf{M_0}$ selon M. Puisque leur nombre est fini et égal à $c_{11}c_{22} \ldots c_{nn} = |\det A|$, le lemme 1 et par suite le théorème 1 sont démontrés.

THÉORÈME 2. — *Les normes des deux modules complets semblables* M *et* αM *sont liés entre eux pur la relation*

$$N(aM) = |N(a)|\,N(M).$$

En particulier, pour les modules semblables à un ordre $\mathfrak{D}$, *on a*

$$N(\alpha\mathfrak{D}) = |N(a)|.$$

DÉMONSTRATION. — Si $\mu_1, \ldots, \mu_n$ est une base de M, on peut prendre les nombres $\alpha\mu_1, \ldots, \alpha\mu_n$ comme base de $\alpha\mathbf{M}$. La norme du nombre $N(a)$ est le déterminant de la matrice de passage C de la base μ_i à la base $\alpha\mu_i$ (cf. appendice § 2-2)). D'après le lemme 1 du § 2, les modules M et $\alpha\mathbf{M}$ ont le même anneau de facteurs $\mathfrak{D}$. Désignons par A et A, les matrices de passage de la base de l'anneau $\mathfrak{D}$ aux bases μ_i et $\alpha\mu_i$ respectivement. On a A, = AC, d'où

$$\mathbf{N}(\alpha\mathbf{M}) = |\det \mathbf{A}_1| = |\det \mathbf{A}|\ |\det \mathbf{C}| = \mathbf{N}(\mathbf{M})\,|\,\mathbf{N}(\alpha)\,|.$$

La deuxième partie du théorème résulte du fait que N(9) = 1.

2) Finitude du nombre des classes

Démontrons le théorème fondamental de ce paragraphe. Il repose sur deux lemmes.

LEMME 2. — *Pour tout module complet* $\mathbf{M}_1$ *du corps* K *et pour tout sous-module complet* $\mathbf{M}_2$ *de* $\mathbf{M}_1$, *il existe seulement un nombre fini de modules* M *intermédiaires* (i. e. des modules M tels que $\mathbf{M}_2 \subset \mathrm{M} \subset \mathbf{M}_1$).

DÉMONSTRATION. — Choisissons un système $\xi_1, \ldots, \xi_s$ ($s = (\mathrm{M}, : \mathbf{M}_2)$) de représentants des classes résiduelles de $\mathbf{M}_1$ selon le sous-groupe M,. Si $\alpha_1, \ldots,$ a,, est une base de M,, tout élément $\theta \in \mathbf{M}_1$ s'écrit de manière unique sous la forme $\theta = \xi_k + c_1\alpha_1 + \ldots + c_n\alpha_n$, où ξ_k est l'un des représentants ci-dessus et $c_1, \ldots, c_n$ des entiers rationnels. Soit $\theta_1, \ldots, \theta_n$ une base d'un module intermédiaire M. Pour tout θ_j, on a une représentation

$$\theta_j = \xi_{k_j} + c_{1j}\alpha_1 + \ldots + c_{nj}\alpha_n,$$

à coefficients c_{ij} entiers. Par suite

$$\mathrm{M} = \{\theta_1, \ldots, \theta_n\} = \{\theta_1, \ldots, \theta_n, \mathrm{a},, \ldots, a,,\}$$
$$= \{\xi_{k_1}, \ldots, \xi_{k_n}, \alpha_1, \ldots, \alpha_n\}$$

Puisqu'il y a seulement un nombre fini de possibilité dans le choix des représentants $\xi_{k_1}, \ldots, \xi_{k_n}$, le nombre des modules intermédiaires M est fini.

COROLLAIRE. — *Pour tout module* $\mathbf{M}_0 \subset \mathrm{K}$ *et pour tout entier naturel r, il existe seulement dans* K *un nombre fini de modules* $\mathbf{M} \supset \mathbf{M}_0$ *tels que*

$$(\mathbf{M} : \mathbf{M}_0) = r.$$

En effet, puisque le groupe quotient $\mathbf{M}/\mathbf{M}_0$ est fini, nous avons $r\mathbf{M} \subset \mathbf{M}_0$, d'où $\frac{1}{r}\mathbf{M}_0 \supset \mathrm{M} \supset \mathbf{M},$.

LEMME 3. — *Dans tout module complet* M *de discriminant* D *d'un corps* K *de nombres algébriques de degré* $n = s + 2t$, *il existe un nombre* $\alpha \neq 0$ *dont la norme satisfait à l'inégalité*

$$| N(\alpha) | \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{| D |}. \tag{5}$$

DÉMONSTRATION. — Choisissons des nombres réels positifs $c_1, \ldots, c_{s+t}$ tels que

$$c_1 \ldots c_{s+t} = \left(\frac{2}{\pi}\right)^t \sqrt{| D |} + \varepsilon, \tag{6}$$

où ε est un nombre réel positif quelconque. Il résulte des théorèmes 2 et 4 du § 4 qu'il existe dans le module M au moins un nombre $a \neq 0$ tel que

$$| \sigma_k(\alpha) | < c_k (1 \leqslant k \leqslant s), | \sigma_{s+j}(\alpha) |^2 < c_{s+j} (1 \leqslant j \leqslant t).$$

La norme

$$N(\alpha) = \sigma_1(\alpha) \ldots \sigma_s(\alpha) | \sigma_{s+1}(\alpha) |^2 \ldots | \sigma_{s+t}(\alpha) |^2$$

de ce nombre ne dépasse pas en valeur absolue le produit (6). Puisque ce résultat est vrai pour ε aussi petit que l'on veut, il existe nécessairement dans M_0 au moins un nombre α satisfaisant à l'inégalité (5).

THÉORÈME 3. — ***Pour tout ordre*** $\mathfrak{D}$ ***d'un corps*** K ***de nombres algébriques il existe seulement un nombre fini de classes de modules semblables associés à*** $\mathfrak{D}$.

DÉMONSTRATION. — Soit M un module associé à l'ordre $\mathfrak{D}$; désignons par D le discriminant du module M et par D_0 le discriminant de l'ordre $\mathfrak{D}$. Choisissons dans le module M un nombre $\alpha \neq 0$ vérifiant la condition (5). D'après la formule (3), on peut écrire la condition (5) sous la forme

$$| N(\alpha) | \leqslant \left(\frac{2}{\pi}\right)^t N(M) \sqrt{| D_0 |}.$$

Puisque $\alpha\mathfrak{D} \subset M$, alors $\mathfrak{D} \subset \frac{1}{\alpha} M$. En outre, d'après le lemme 1 et la définition de la norme d'un module, nous avons

$$\left(\frac{1}{\alpha} M : \mathfrak{D}\right) = N\left(\frac{1}{\alpha} M\right)^{-1} = \frac{| N(\alpha) |}{N(M)} \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{| D_0 |}.$$

Cela démontre que dans toute classe de modules semblables associés à $\mathfrak{D}$ il existe un module M' tel que

$$M' \supset \mathfrak{D}, \quad (M' : a) < \left(\frac{2}{\pi}\right)^t \sqrt{| D_0 |}. \tag{7}$$

D'après le corollaire du lemme 2, il existe dans le corps K seulement un nombre fini de modules M' vérifiant la condition (7). Il en résulte que le nombre des classes de modules semblables associés à $\mathfrak{D}$ est aussi fini, ce qui termine la démonstration du théorème.

Remarque. — Pour deux modules complets $\mathbf{M}_1$ et $\mathbf{M}_2$ d'un corps K de nombres algébriques, nous avons un procédé « effectif » pour savoir s'ils sont semblables ou non. Pour cela, trouvons tout d'abord leurs anneaux de stabilisateurs. Si ces anneaux sont distincts, alors $\mathbf{M}_1$ et $\mathbf{M}_2$ ne sont pas semblables. Supposons que $\mathbf{M}_1$ et $\mathbf{M}_2$ aient le même anneau de stabilisateurs $\mathfrak{D}$. Remplaçant peut-être un de nos modules par un module semblable nous pouvons supposer $\mathbf{M}_1 \supset \mathrm{M},$. Calculons l'indice $(\mathrm{M}, : \mathrm{M},) = a$. Si $\alpha\mathbf{M}_1 = \mathbf{M}_2$, alors $a \in \mathfrak{D}$ et $| N(a) | = a$. C'est pourquoi, nous choisirons dans l'anneau $\mathfrak{D}$ un système complet de nombres $\alpha_1, \ldots, \alpha_k$ non associés deux à deux de norme égale à a en valeur absolue (cf. § 5-4)) où on a trouvé « effectivement » un tel système. Si a est un nombre quelconque de l'anneau $\mathfrak{D}$ tel que $| N(a) | = a$, il est associé à un certain α_i, d'où $\alpha\mathbf{M}_1 = \alpha_i\mathbf{M}_1$. Pour savoir si les modules $\mathbf{M}_1$ et $\mathbf{M}_2$ sont semblables, il suffit maintenant de comparer le module $\mathbf{M}_2$ aux modules $\alpha_i\mathbf{M}_1$ $(1 \leqslant i \leqslant k)$. Les modules $\mathbf{M}_1$ et $\mathbf{M}_2$ seront semblables si et seulement si $\mathbf{M}_2$ coïncide avec un des modules $\alpha_i\mathbf{M}_1$.

EXERCICES

1. Montrer que tout corps de nombres algébriques, différent du corps des nombres rationnels, contient une infinité d'ordres (par suite, le nombre de toutes les classes de modules semblables, associés aux différents ordres possibles, est infini).

2. Utilisant l'exercice 2 du § 4, démontrer que tout module complet M de discriminant D contient un nombre $a \neq 0$ tel que

$$| \mathrm{N}(\alpha) | \leqslant \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{| \mathrm{D} |}.$$

($n = s + 2t$ est le degré du corps de nombre algébriques).

3. Appliquant l'exercice 2 à l'ordre maximum à un corps K de nombres algébriques de degré $n = s + 2t$ et utilisant la formule de Stirling

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{\theta}{12n}}, \qquad 0 < \theta < 1,$$

montrer que le discriminant $\mathbf{D}_0$ du corps K satisfait à l'inégalité

$$| \mathbf{D}_0 | > \left(\frac{\pi}{4}\right)^{2t} \frac{1}{2\pi n} e^{2n - \frac{1}{6n}}.$$

Ainsi, quand le degré n croît, le discriminant d'un corps de nombres algébriques tend en valeur absolue vers l'infini.

4. Démontrer que le discriminant d'un corps K de nombres algébriques de degré $n > 1$ est différent de ± 1 (théorème de Minkowski).

5. Démontrer qu'il existe seulement un nombre fini de corps dont le discriminant a une valeur donnée (théoréme d'Hermite).

INDICATION. — D'après l'exercice 3, il suffit de montrer qu'il existe seulement un nombre fini de corps K de degré fixé $n = s + 2t$ et de discriminant donné D_0. Considérer dans l'espace $\mathcal{R}^n$ (formé des points $(x_1, \ldots, x_s, y_1, z_1, \ldots, y_t, z_t)$) l'ensemble X défini, dans le cas $s > 0$ par les conditions

$$|x_1| < \sqrt{|D_0| + 1}, \quad |x_k| < 1 \ (2 \leqslant k \leqslant s), \quad y_j^2 + z_j^2 < 1 \ (1 \leqslant j \leqslant t),$$

et, dans le cas $s = 0$, par les conditions

$$|y_1| < \frac{1}{2}, \quad |z_1| < \sqrt{|D_0| + 1}, \quad y_j^2 + z_j^2 < 1 \quad (2 \leqslant j \leqslant t).$$

Appliquant alors le lemme de Minkowski à l'ensemble X et au lattice représentant les nombres de l'ordre maximum $\tilde{\mathfrak{D}}$ du corps K, montrer qu'il existe un élément primitif $\theta \in \tilde{\mathfrak{D}}$ du corps K, dont le polynôme caractéristique a des coefficients bornés.

§ 7. — REPRÉSENTATION DES NOMBRES PAR DES FORMES QUADRATIQUES BINAIRES

Dans ce paragraphe, nous ferons une étude beaucoup plus détaillée des questions de ce chapitre dans le cas de formes quadratiques binaires. Puisque toute forme rationnelle irréductible $ax^2 + bxy + cy^2$ se décompose en facteurs linéaires dans un certain corps quadratique, notre étude est liée à l'étude des modules complets et de leurs anneaux de stabilisateurs dans les corps quadratiques.

1) Corps quadratiques

On appelle ***corps quadratique*** toute extension de degré 2 du corps Q des nombres rationnels. Commençons par décrire ces corps qui forment les exemples les plus simples de corps algébriques.

Soit $d \neq 1$ un nombre entier rationnel non divisible par un carré (positif ou négatif). Puisque le polynôme $t^2 - d$ est irréductible dans le corps des nombres rationnels, le corps $\mathbf{Q}(\theta)$ obtenu à partir de Q par adjonction d'une racine θ de ce polynôme est de degré 2 sur $\mathbf{Q}$, i. e. est un corps quadratique. Nous le désignerons dans la suite par $Q(\sqrt{d})$. Il est facile de voir que, réciproquement, tout corps quadratique K est de cette forme; démontrons-le. Si $\alpha \in K$ et n'est pas rationnel, alors $K = Q(a)$. Le polynôme minimal de α

sur $\mathbf{Q}$ est de degré 2 et par suite il existe des rationnels p et q tels que

$$\alpha^2 + p\alpha + q = 0.$$

Posons $\beta = a + \frac{p}{2}$; alors $\beta^2 = \frac{p^2}{4} - q$. Le nombre rationnel $\frac{p^2}{4} - q$ peut s'écrire sous la forme c^2d, d étant un entier sans carrés. Il est clair que $d \neq 1$ puisque sinon β et par suite a seraient des nombres rationnels. Si $\theta = \frac{\beta}{c}$, alors $\theta^2 = d$ et K = Q(0), i. e. K = $\mathbf{Q}(\sqrt{d})$.

Montrons que pour des entiers d distincts ($\neq 1$ et sans carrés) les corps Q($\sqrt{d}$) correspondants sont distincts. En effet, si $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{d'})$, alors

$$\sqrt{d'} = x + y\sqrt{d}$$

pour des rationnels x et y; d'où

$$d' = x^2 + dy^2 + 2xy\sqrt{d}$$

et par suite

$$d' = x^2 + dy^2, \qquad 2xy = 0.$$

Si y = 0, alors $d' = x^2$ ce qui est impossible par hypothèse. Si maintenant $x = 0$, $d' = dy^2$ et cela signifie $d' = d$. On a donc démontré que les corps quadratiques sont en correspondance biunivoque avec l'ensemble des entiers rationnels $\neq 1$ et sans carrés.

2) Ordres dans un corps quadratique

Les nombres du corps $\mathbf{Q}(\sqrt{d})$ s'écrivent

$$\alpha = x + y\sqrt{d}$$

x, y rationnels. Puisque le polynôme caractéristique de a est égal à

$$t^2 - 2xt + x^2 - dy^2,$$

a appartient à l'ordre maximum $\tilde{\mathfrak{D}}$ du corps $\mathbf{Q}(\sqrt{d})$ si et seulement si les nombres 2x = Tr (a) et $x^2 - dy^2 = N(a)$ sont des entiers rationnels. Posons 2x = m. Puisque $\frac{m^2}{4} - dy^2$ doit être entier et que d est sans carrés, le dénominateur du nombre rationnel y (écrit sous forme irréductible) peut au plus être égal à 2, i. e. y = $\frac{n}{2}$, n entier. Il est clair que $N(a) = \frac{m^2}{4} - \frac{dn^2}{4}$ est entier si et seulement si

$$m^2 - dn^2 \equiv 0 \pmod 4. \qquad (1)$$

La résolution de cette congruence dépend bien entendu de d et plus précisément de la valeur de d module 4. Puisque d est sans carrés, alors $d \not\equiv 0 \pmod 4$, d'où trois possibilités :

$$d \equiv 1 \pmod 4; \qquad d \equiv 2 \pmod 4; \qquad d \equiv 3 \pmod 4.$$

Si $d \equiv 1 \pmod 4$, la congruence (1) s'écrit $m^2 \equiv n^2 \pmod 4$ ce qui est équivalent à $m \equiv n \pmod 2$, i. e. $m = n + 21$; nous obtenons

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} = l + n\frac{1+\sqrt{d}}{2}$$

pour des entiers l et n. Ainsi, dans ce cas, on peut prendre comme base de l'ordre maximum $\mathfrak{D}$, i. e. comme base fondamentale du corps $\mathbf{Q}(\sqrt{d})$ (cf. fin du § 2), les nombres 1 et $\omega = \frac{1+\sqrt{d}}{2}$.

Supposons maintenant $d \equiv 2$ ou 3 (mod 4). Si la congruence (1) avait une solution telle que n soit impair, de $d \equiv m^2 \pmod 4$ résulterait que $d \equiv 0 \pmod 4$ pour m pair et $d \equiv 1 \pmod 4$ pour m impair, ce qui contredit notre hypothèse. n étant pair, il résulte de la congruence $m^2 \equiv 0 \pmod 4$ que m est pair. Nous avons donc démontré dans ce cas que le nombre $x + y\sqrt{d}$ appartient à l'ordre maximum $\tilde{\mathfrak{D}}$ du corps $\mathbf{Q}(\sqrt{d})$ si et seulement si $x = \frac{m}{2}$ et $y = \frac{n}{2}$, m et n entiers pairs. Dans ce cas, on peut donc prendre pour base de $\tilde{\mathfrak{D}}$ les nombres 1 et $\omega = \sqrt{d}$.

Dans la suite, quand nous parlerons d'une base de l'ordre maximum du corps $\mathbf{Q}(\sqrt{d})$ nous prendrons toujours la base 1, ω où $\omega = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1 \pmod 4$ et $\omega = \sqrt{d}$ pour $d \equiv 2$ ou 3 (mod 4).

Considérons maintenant un ordre quelconque $\mathfrak{D}$ du corps $\mathbf{Q}(\sqrt{d})$. Puisque $\mathfrak{D}$ est contenu dans l'ordre maximum $\tilde{\mathfrak{D}}$ (cf. § 2-4)), tous les nombres de $\mathfrak{D}$ sont de la forme $x + y\omega$, x, y entiers rationnels. Choisissons parmi eux un nombre pour lequel le coefficient y est > 0 et a la plus petite valeur possible; soit $a + f\omega$ ce nombre. Puisque a est un nombre entier rationnel contenu dans $\mathfrak{D}$, alors $f\omega \in \mathfrak{D}$. Il est maintenant clair que pour tout

$$x + y\omega \in \mathfrak{D}$$

le coefficient y est divisible parf et cela signifie $\mathfrak{D} = \{1, f\omega\}$. Réciproquement, d'après le lemme 3 du § 2, pour tout entier naturel f, le module $\{1, f\omega\}$

est un anneau et par suite un ordre du corps $\mathbf{Q}(\sqrt{d})$. Puisque pour des entiers naturelsfdistincts les ordres $\{1, f\omega\}$ sont aussi distincts, nous obtenons : tous les ordres d'un corps quadratique sont en correspondance biunivoque avec l'ensemble des entiers naturels.

Par la suite, nous désignerons par $\mathfrak{D}_f$ l'ordre $\{1, f\omega\}$. Il est facile de voir que le nombre f est égal à l'indice de l'ordre $\mathfrak{D}_f$ dans l'ordre maximum

$$\tilde{\mathfrak{D}} = \mathfrak{D}_1 = \{1, \omega\}.$$

Ainsi tout ordre d'un corps quadratique est complètement défini par son indice dans l'ordre maximum du corps.

Calculons maintenant le discriminant de l'ordre $\mathfrak{D}_f$. Supposons tout d'abord $d \equiv 1 \pmod 4$. Puisque $\mathrm{Tr}\,(\sqrt{d}) = 0$, alors

$$\mathrm{Tr}\,\omega = \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) = 1$$

$$\mathrm{Tr}\,\omega^2 = \mathrm{Tr}\left(\frac{d+1}{4} + \frac{\sqrt{d}}{2}\right) = \frac{d+1}{2}$$

et par suite

$$\mathrm{D}_f = \begin{vmatrix} \mathrm{Tr}\,1 & \mathrm{Tr}\,\omega \\ \mathrm{Tr}\,f\omega & \mathrm{Tr}\,f^2\omega^2 \end{vmatrix} = \begin{vmatrix} 2 & f \\ f & f^2\left(\frac{d+1}{2}\right) \end{vmatrix} = f^2 d.$$

Si maintenant $d \equiv 2$ ou $3 \pmod 4$, alors

$$\mathrm{D}_f = \begin{vmatrix} \mathrm{Tr}\,1 & \mathrm{Tr}\,f\sqrt{d} \\ \mathrm{Tr}\,f\sqrt{d} & \mathrm{Tr}\,f^2 d \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2f^2 d \end{vmatrix} = f^2 . 4d.$$

Les formules obtenues pour D_f nous montrent que tout ordre d'un corps quadratique est défini de manière unique par son discriminant.

Nous rassemblerons sous forme d'un théorème les résultats obtenus ci-dessus.

THÉORÈME 1. — ***Soit d un nombre entier rationnel*** $\neq 1$ ***et sans carrés. Comme base de l'ordre maximum*** $\tilde{\mathfrak{D}}$ ***du corps quadratique*** $\mathbf{Q}(\sqrt{d})$, ***on peut prendre les nombres 1 et*** ω, ***avec*** $\omega = \dfrac{1+\sqrt{d}}{2}$ ***si*** $d \equiv 1 \pmod 4$ ***et*** $\omega = \sqrt{d}$ ***si*** $d \equiv 2$ ***ou*** $3 \pmod 4$. ***Le discriminant*** D_1 ***de l'ordre*** $\mathfrak{D}$ (i. ***e. le discriminant du corps*** $\mathbf{Q}(\sqrt{d})$) ***est égal à d dans le premier cas et à 4d dans le second. Un ordre quelconque*** $\mathfrak{D}$ ***du corps*** $Q(\sqrt{d})$ ***s'écrit alors*** $\mathfrak{D}_j = \{1, f\omega\}$ ***(où*** f ***est l'indice*** $(\tilde{\mathfrak{D}} : \mathfrak{D})$); ***le discriminant de l'ordre*** $\mathfrak{D}_f$ ***est égal à*** $\mathrm{D}_f = \mathrm{D},. f^2$

3) Unités

Puisque tout nombre de l'ordre $\mathfrak{D}_f$ est représentable sous la forme $x+yf\omega$, x et y entiers rationnels, alors, d'après le théorème 4 du § 2, nous trouverons toutes les unités de l'ordre $\mathfrak{D}$ en résolvant l'équation

$$N(x + yf\omega) = +1, \tag{2}$$

i. e. l'équation

$$x^2 + fxy + f^2\left(\frac{1-d}{4}\right)y^2 = \pm 1, \tag{3}$$

pour $d \equiv 1 \pmod 4$, et l'équation

$$x^2 - df^2y^2 = +1 \tag{4}$$

pour $d \equiv 2$ ou $3 \pmod 4$.

Pour un corps quadratique imaginaire, $s = 0$, $t = 1$, $r = s + t - 1 = 0$; ainsi le groupe des unités dans tout ordre de ce corps est fini et formé de racines de 1. Ce résultat est en relation avec le fait que, pour $d < 0$, les équations (3) et (4) ont au plus un nombre fini de solutions en nombres entiers. En fait, pour $d = -1$, $f = 1$, l'équation (4) a quatre solutions :

$$x = \pm 1, \quad y = 0; \quad x = 0, \quad y = \pm 1,$$

qui correspondent à ± 1 et $\pm i$ qui sont les racines quatrièmes de 1. Pour $d = -3$, $f = 1$, l'équation (3) à 6 solutions :

$$x = 1,\ y = 0;\ x = 0,\ y = \pm 1;\ x = 1,\ y = -1;\ x = -1,\ y = 1,$$

qui correspondent à toutes les racines sixièmes de 1. Pour tous les ordres restants des corps quadratiques imaginaires les équations (3) ou (4) ont au moins deux solutions : x = $\pm$ 1, y = 0, i. e. $\pm$ 1 sont toujours des unités.

Le cas d'un corps quadratique réel $\mathbf{Q}(\sqrt{d})$, $d > 0$ est plus compliqué. Puisque alors $s = 2$, $t = 0$, toutes les unités d'un ordre $\mathfrak{D}_f$ du corps Q($\sqrt{d}$) sont de la forme $\pm \varepsilon^n$, où ε est une unité fondamentale de l'ordre $\mathfrak{D}_f$. Le problème ici est donc de déterminer une unité fondamentale E. De même que ε, les nombres $\frac{1}{\varepsilon}$, $-$ E, $-\frac{1}{2}$ sont aussi des unités fondamentales; par suite, on peut supposer que $\varepsilon > 1$. Il est clair que la condition $\varepsilon > 1$ définit de manière unique l'unité fondamentale ε.

Soit η une unité de $\mathfrak{D}_f$ et soit η = x + y f ω sa décomposition sur la base 1, ω ; montrons que si $\eta > 1$, alors les coefficients x et y sont positifs (pour $d = 5$, $f = 1$ il se peut que x = 0). Pour tout $\alpha \in \mathbf{Q}(\sqrt{d})$, soit α' son

conjugué, i. e. l'image de α par l'automorphisme $\sqrt{d} \to -\sqrt{d}$ du corps $\mathbf{Q}(\sqrt{d})$. Il est facile de voir que $\omega - \omega' > 0$. Puisque $\mathbf{N}(\eta) = \eta\eta' = \pm 1$, l'unité η' est égale, ou bien à $\frac{1}{\eta}$, ou bien à $-\frac{1}{\eta}$; dans ces deux cas, $\eta - \eta' > 0$, i. e. $yf(\omega - \omega') > 0$ et par suite $y > 0$. Puis?que $|\eta'| = |x + yf\omega'| < 1$ et $f\omega' < -1$, sauf dans le cas $d = 5, f = 1$, alors $x > 0$ (si $d = 5, f = 1$, alors $-1 < f\omega' = \frac{1-\sqrt{5}}{2} < 0$ et nous obtenons $x \geqslant 0$).

Soit $\varepsilon > 1$ une unité fondamentale de l'ordre $\mathfrak{D}_f$. Pour l'unité

$$\varepsilon^n = x_1 + y_1 f\omega \quad (n \text{ entier naturel}),$$

ou $ax_1 > x$ et $y_1 > y$. Par suite, pour trouver une unité fondamentale $\varepsilon > 1$, il suffit de trouver une solution > 0 de l'équation (2) qui soit la plus petite possible. Utilisant les résultats du § 5-3), nous pouvons borner supérieurement ces nombres x et y par une constante C puis considérer successivement les unités (en nombre fini) qui satisfont à ces inégalités.

Montrons tout de suite par une remarque que l'on peut réduire le nombre de vérifications à effectuer pour déterminer une unité fondamentale. On s'appuie sur le théorème qui affirme que si pour un nombre réel ξ il existe des nombres entiers naturels premiers x et y tels que

$$\left|\frac{x}{y} - \xi\right| < \frac{1}{2y^2},$$

alors $\frac{x}{y}$ est nécessairement une des fractions qui interviennent dans la décomposition du nombre ξ en fraction continue.

D'après (2),

$$\left|\frac{x}{y} + f\omega'\right| = \frac{1}{y(x + yf\omega)}.$$

Si $d \equiv 1 \pmod 4$ alors, en laissant de côté le cas $d = 5$, $f = 1$, nous obtenons

$$\left|\frac{x}{y} - f\frac{\sqrt{d}-1}{2}\right| = \frac{1}{y^2\left(\frac{x}{y} + f\frac{\sqrt{d}+1}{2}\right)} < \frac{1}{2y^2}$$

(puisque $\frac{x}{y} > 0$ et $\frac{f\sqrt{d}+1}{2} > 2$). Si maintenant $d \equiv 2 \text{ ou } 3 \pmod 4$, alors on a $x^2 = fdy^2 \pm 1 \geqslant dy^2 - 1 \geqslant y^2(d-1)$ et $d \geqslant 2$, d'oh

$$\left|\frac{x}{y} - f\sqrt{d}\right| = \frac{1}{y(x + yf\sqrt{d})} \leqslant \frac{1}{y^2\sqrt{d-1} + \sqrt{d}} < \frac{1}{2y^2}.$$

D'après le théorème rappelé ci-dessus de la théorie des fractions continues, $\frac{x}{y}$ est une des fractions de la décomposition du nombre irrationnel $-f\omega'$

en fraction continue. Pour trouver la plus petite solution > 0 de l'équation (2), il suffit donc de considérer seulement les couples de nombres qui interviennent dans la décomposition de $-f\omega'$ en fraction continue (et qui ne dépassent pas la constante C calculée plus haut). Dans la pratique, on conduit les calculs de la manière suivante. Pour le nombre $-f\omega'$, on détermine des dénominateurs partiels q_k ($k \geqslant 0$) et les numérateurs P_k et dénominateurs Q_k des fractions correspondantes. Nous continuerons les calculs jusqu'à ce que l'expression $N(P_k + \omega f Q_k)$ ne soit pas égale à ± 1. Cela a lieu forcément pour un $P_k < C$ et l'unité fondamentale correspondante $\varepsilon = P_k + \omega f Q_k$ est ainsi déterminée (pour le cas exclu $d = 5$, $f = 1$, on peut prendre pour unité fondamentale $\omega = \frac{1+\sqrt{5}}{2}$). Illustrons cette méthode par deux exemples.

Exemple 1. — Pour trouver une unité fondamentale de l'ordre $\{1, 3\sqrt{6}\}$ du corps $Q(\sqrt{6})$, décomposons le nombre $-3\omega' = 3\sqrt{6}$ en fraction continue :

$$\sqrt{54} = 7 + (\sqrt{54} - 7),$$

$$\frac{1}{\sqrt{54}-7} = 2 + \frac{\sqrt{54}-3}{5},$$

$$\frac{5}{\sqrt{54}-3} = 1 + \frac{\sqrt{54}-6}{9},$$

$$\frac{9}{\sqrt{54}-6} = 6 + \frac{\sqrt{54}-6}{2},$$

$$\frac{2}{\sqrt{54}-6} = 1 + \frac{\sqrt{54}-3}{9},$$

Constituons le tableau :

k	0	1	2	3	4	5
q_k	7	2	1	6	1	2
P_k	7	15	22	147	169	485
Q_k	1	2	3	20	23	66
$P_k^2 - 54\,Q_k^2$	- 5	9	- 2	9	- 5	1

L'unité fondamentale de l'ordre $\{1, 3\sqrt{6}\}$ est par suite égale à

$$485 + 66 \cdot 3\sqrt{6} = 485 + 198\sqrt{6}.$$

Exemple 2. — Calculons une unité fondamentale du corps $\mathbf{Q}(\sqrt{41})$. Nous avons

$$\frac{\sqrt{41}-1}{2} = 2 + \frac{\sqrt{41}-5}{2}$$

$$\frac{2}{\sqrt{41}-5} = 1 + \frac{\sqrt{41}-3}{8}$$

$$\frac{8}{\sqrt{41}-3} = 2 + \frac{\sqrt{41}-5}{4}$$

$$\frac{4}{\sqrt{41}-5} = 2 + \frac{\sqrt{41}-3}{4}$$

$$\frac{4}{\sqrt{41}-3} = 1 + \frac{\sqrt{41}-5}{8}$$

k	0	1	2	3	4
q_k	2	1	2	2	1
P_k	2	3	8	19	27
Q_k	1	1	3	7	10
$P_k^2 - P_k Q_k - 10Q_k^2$	— 4	2	- 2	4	- 1

L'unité fondamentale de l'ordre maximum du corps $\mathbf{Q}(\sqrt{41})$ est ainsi égale à

$$27 + 10\,\frac{\sqrt{41}+1}{2} = 32 + 5\sqrt{41}.$$

4) Modules

Étudions maintenant les modules complets des corps quadratiques. Puisque tout module $\{\alpha, \beta\}$ est semblable au module $\left\{1, \frac{\beta}{\alpha}\right\}$, il suffit d'étudier les modules de la forme $\{1, y\}$.

Tout nombre non rationnel y de $Q(\sqrt{d})$ est racine d'un certain polynôme $at^2 + bt + c$ à coefficients entiers rationnels. Si nous imposons à a, *b, c* les conditions (a, *b, c)* = 1 et $a > 0$, alors pour tout y le polynôme $at^2 + bt + c$ est défini de manière unique; nous le désignerons dans la suite par $\varphi_\gamma(t)$. Il est clair que pour son conjugué y', nous avons $\varphi_{\gamma'}(t) = \varphi_\gamma(t)$; de plus, l'égalité $\varphi_{\gamma_1}(t) = \varphi_\gamma(t)$ a lieu si et seulement si γ_1 est égal soit à y soit à y',

LEMME 1. — *Si le polynôme $\varphi_\gamma(t)$ d'un nombre y non rationnel de* $Q(\sqrt{d})$ *est égal à $at^2 + bt + c$, alors l'anneau $\mathfrak{D}$ des stabilisateurs du module*

$$M = \{1, \gamma\}$$

est l'ordre $\{1, a\gamma\}$ *de discriminant* $D = b^2 - 4ac$.

DÉMONSTRATION. — Considérons le nombre $a = x + y\gamma$, x, y rationnels. Puisque l'inclusion $\alpha M \subset M$ équivaut au fait que $a.1 = x + y\gamma \in M$ et

$$a.\gamma = -\frac{cy}{a} + \left(x - \frac{by}{a}\right)\gamma \in M,$$

alors, a appartient à l'anneau de stabilisateurs $\mathfrak{D}$ si et seulement si les nombres rationnels

$$x, \quad y, \quad \frac{cy}{a}, \quad \frac{by}{a}$$

sont des entiers, i. e. si x et y sont entiers et y divisible par a (puisque (a, *b,* c) = 1). Cela démontre que $\mathfrak{D} = \{1, a\gamma\}$. Pour terminer la démonstration du lemme 1, il suffit de calculer le discriminant de l'ordre $\mathfrak{D}$:

$$D = \begin{vmatrix} \mathrm{Tr}\ 1 & \mathrm{Tr}\ a\gamma \\ \mathrm{Tr}\ a\gamma & \mathrm{Tr}\ a^2\gamma^2 \end{vmatrix} = \begin{vmatrix} 2 & -b \\ -b & b^2 - 2ac \end{vmatrix} = b^2 - 4ac.$$

COROLLAIRE. — *Avec les notations du lemme 1, la norme du module* $\{1, y\}$ *est égale à* $\frac{1}{a}$.

En effet, la matrice de passage de la base 1, $a\gamma$ à la base 1, y est égale à

$$\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$$

LEMME 2. — *Pour que les modules* $\{1, y\}$ *et* $\{1, \gamma_1\}$ *soient semblables, il faut et il suffit que les nombres y et γ_1 soient liés par la relation*

$$\gamma_1 = \frac{k\gamma + l}{m\gamma + n}, \tag{5}$$

où les entiers rationnels k, 1, m, n sont tels que

$$\begin{vmatrix} k & l \\ m & n \end{vmatrix} = \pm 1. \qquad (6)$$

DÉMONSTRATION. — Puisque deux bases distinctes d'un même module sont liées par une transformation unimodulaire (cf. § 2-1)), l'égalité

$$\{\alpha, \alpha\gamma_1\} = \{1, \gamma\}$$

entraîne

$$\alpha\gamma_1 = k\gamma + l$$
$$\alpha = m\gamma + n$$

pour des entiers k, l, m, n vérifiant la condition (6). Divisant la première de ces égalités par la seconde, nous obtenons (5). Réciproquement, soient γ_1 et y liés par la relation (5). Alors

$$\{1, \gamma_1\} = \frac{1}{m\gamma + n}\{m\gamma + n, k\gamma + l\} = \frac{1}{m\gamma + n}\{1, \gamma\}$$

(l'égalité $\{my + n, ky + l\} = \frac{1}{m\gamma + n}\{1, y\}$ a lieu d'après (6)). Ceci termine la démonstration du lemme 2.

Considérons dans le corps $\mathbf{Q}(\sqrt{d})$ les modules associés à un certain ordre fixé $\mathfrak{D}$ (i. e. dont $\mathfrak{D}$ est l'anneau de stabilisateurs). D'après le théorème § 6, il existe seulement un nombre fini de classes de tels modules semblables. Introduisant une opération de multiplication des classes, nous allons montrer que, pour cette opération, toutes les classes de modules semblables associés à un ordre donné $\mathfrak{D}$ forment un groupe.

Si $M = \{a, \beta\}$ et $M_1 = \{\alpha_1, \beta_1\}$ sont deux modules, alors, par définition, le module produit sera le module MM, $= \{\alpha\alpha_1, \alpha\beta_1, \beta\alpha_1, \beta\beta_1\}$ (cf. exercice 7, § 2). 11 est évident que pour $A \neq 0$, $\mu \neq 0$, on a la formule

$$(\lambda M)(\mu M_1) = \lambda\mu(MM_1). \qquad (7)$$

Pour tout module M, nous désignons par [M] la classe de modules semblables dont M est un représentant. De l'égalité (7) résulte que la classe [MM,] dépend seulement des classes [M] et [M,]. La classe [MM,] sera appelée le produit des classes [M] et $[M_1]$. Pour multiplier deux classes, il faut donc choisir arbitrairement un représentant dans chacune de ces classes et les multiplier; la classe de modules semblables contenant le produit obtenu sera le produit des classes considérées.

Pour tout module M, nous désignerons par M' le module formé des conjugués a' de tous les nombres $a \in M$. Puisque $a + a' = \mathrm{Tr}\, a$ est rationnel, alors $a' \in \mathbf{Q}(\sqrt{d})$ et par suite M' est simultanément avec M un module

complet du corps $\mathbf{Q}(\sqrt{d})$. Il est facile de voir que pour tout ordre $\mathfrak{D}$ son conjugué $\mathfrak{D}'$ coïncide avec $\mathfrak{D}$. Il en résulte que deux modules conjugués ont le même anneau de stabilisateurs.

Démontrons la formule

$$MM' = N(M)\mathfrak{D}, \tag{8}$$

dans laquelle $\mathfrak{D}$ est l'anneau de stabilisateurs et N(M) la norme du module M.

Supposons tout d'abord que le module $\mathfrak{D}$ est de la forme $\{ 1, y \}$. Dans ce cas, on obtient, en utilisant les notations du lemme 1 :

$$\begin{aligned} MM' &= \{ 1, \gamma \} \{ 1, \gamma' \} = \{ 1, \gamma, \gamma', \gamma\gamma' \} \\ &= \left\{ 1, \gamma, -\gamma - \frac{b}{a}, -\frac{c}{a} \right\} \\ &= \left\{ 1, \gamma, -\frac{b}{a}, -\frac{c}{a} \right\} = \frac{1}{a} \{ a, b, c, a\gamma \}. \end{aligned}$$

Puisque a, b et c sont premiers entre eux, l'ensemble de leurs combinaisons linéaires à coefficients entiers coïncide avec l'anneau Z tout entier; par suite

$$MM' = \frac{1}{a} \{ 1, \gamma \} = \frac{1}{a} \mathfrak{D} = N(M)\mathfrak{D}$$

(corollaire du lemme 1). Si maintenant M est un module quelconque, on peut toujours l'écrire sous la forme $M = \alpha M_1$ où M_1 est de la forme $\{ 1, y \}$. D'après le théorème 2 du § 6, nous obtenons

$$MM' = \alpha\alpha' M_1 M_1' = N(\alpha)N(M_1)\mathfrak{D} = |N(a)|\, N(M_1)\mathfrak{D} = N(M)\mathfrak{D},$$

ce qui démontre la formule (8) dans le cas général.

Soient maintenant M et M_1 deux modules associés au même ordre $\mathfrak{D}$. Si $\overline{\mathfrak{D}}$ est l'anneau des stabilisateurs du produit MM_1, alors, d'après la formule (8),

$$MM_1(MM_1)' = N(MM_1)\mathfrak{D}.$$

D'autre part, puisque la multiplication des modules est commutative et associative, en multipliant entre elles les formules $MM' = N(M)\mathfrak{D}$ et $M_1M_1' = N(M_1'')\mathfrak{D}$, on obtient

$$(MM_1)(MM_1)' = N(M)N(\mu_1)\mathfrak{D}.$$

Comparant cette égalité à la précédente et remarquant que des ordres distincts ne sont jamais semblables, nous obtenons l'égalité $\mathfrak{D} = \overline{\mathfrak{D}}$. Remarquant de plus que si a et b sont des rationnels positifs, l'égalité $a\mathfrak{D} = b\mathfrak{D}$ entraîne $a = b$, nous obtenons aussi

$$N(MM_1) = N(M).\ N(M_1).$$

Ainsi si deux modules M et $\mathbf{M_1}$ sont associés à l'ordre $\mathfrak{D}$, leur produit MM, est encore associé à $\mathfrak{D}$. Puisque de plus pour tout module M d'anneau de facteurs $\mathfrak{D}$, on a simultanément $\mathbf{M}\mathfrak{D}$ = M et $\mathbf{M}\left(\frac{1}{\mathbf{N}(\mathbf{M})}\,\mathbf{M}'\right) = \mathfrak{D}$, nous obtenons le théorème suivant.

THÉORÈME *2.* — ***Tous les modules d'un corps quadratique qui sont associés à un ordre donné forment un groupe commutatif pour l'opération de multiplication des modules.***

De ce théorème et du théorème 3 du § 6 résulte de manière évidente le résultat suivant :

THÉORÈME *3.* — ***Toutes les classes de modules semblables d'un corps quadratique d'anneau de stabilisateurs $\mathfrak{D}$ donnéforment un groupe fini commutatif.***

Remarquons que les théorèmes 2 et 3 sont spécifiques des corps quadratiques et ne seraient vrais dans le cas général d'un corps algébrique que pour les modules qui admettent pour anneau de stabilisateurs l'ordre maximum (cf. exercice 18, § 2).

5) Correspondance entre modules et formes

D'après le § 1-3), à toute base α, β d'un module complet M $\subset \mathbf{Q}(\sqrt{d})$ correspond de manière unique une forme quadratique binaire $\mathbf{N}(\alpha x + \beta y)$ à coefficients rationnels. Puisque à des bases distinctes de M correspondent des formes équivalentes, au module M correspond une classe de formes équivalentes. Si maintenant on remplace M par un module $\gamma\mathbf{M}$ qui lui est semblable, toutes les formes précédentes sont multipliées par le facteur constant N(y). Ainsi, considérant les formes à un facteur constant près on peut dire qu'à toute classe de modules semblables correspond une classe de formes équivalentes. Cependant, cette correspondance n'est pas biunivoque. En effet, des modules conjugués M = { *a,* β} et M' = { a', β' } ne sont pas semblables et pourtant les formes correspondantes coïncident. Nous allons définir de nouvelles notions d'équivalence des formes et de similitude des modules pour rendre biunivoque la correspondance entre les classes.

DÉFINITION. — ***Une forme quadratique binairef (x, y) = $Ax^2 + Bxy + Cy^2$ à coefficients entiers rationnels est dite primitive si le plus grand diviseur commun de ses coefficients est égal à 1. Le nombre entier $B^2 - 4AC$ est appelé le discriminant de la forme primitive f.***

Ainsi, le discriminant d'une forme primitive diffère de son déterminant $AC - \frac{B^2}{4}$ par le facteur constant — 4.

Il est facile de voir que toute forme équivalente à une forme primitive est primitive. Par une transformation linéaire de la variable de matrice C, le déterminant d'une forme quadratique est multiplié par le facteur (det C)² et par suite il ne change pas si et seulement si det C = ± 1. Il en résulte que des formes primitives équivalentes ont le même discriminant.

DÉFINITION. — *Deux formes primitives sont dites strictement équivalentes si l'une se transforme en l'autre pour une transformation linéaire des variables à coefficients entiers et de déterminant* + 1.

Toutes les formes quadratiques binaires primitives se décomposent en classes de formes strictement équivalentes. Dans la suite, le mot classe de formes s'appliquera à l'équivalence stricte.

Donnons maintenant une nouvelle définition de la similitude des modules.

DÉFINITION. — *Deux modules complets* M *et* M_1 *d'un corps quadratique seront dits strictement semblables si* $M_1 = \alpha M$ *pour un certain* α *de norme positive.*

Puisque pour un corps quadratique imaginaire la norme de tout élément $a \neq 0$ est positive alors dans un tel corps la similitude au sens strict coïncide avec la similitude prise au sens habituel. Il en sera de même pour un corps quadratique réel si dans l'anneau $\mathfrak{D}$ des stabilisateurs des modules considérés il existe une unité ε telle que $N(\varepsilon) = -1$. En effet, si $M_1 = \alpha M$ et $N(a) < 0$, alors puisque $\varepsilon M = M$, nous avons $M_1 = (\alpha\varepsilon)M$ avec $N(\alpha\varepsilon) > 0$. Réciproquement, si ces deux notions de similitude coïncident, i. e. si $M_1 = \alpha M$, $N(a) < 0$ entraîne qu'il existe β tel que $N(\beta) > 0$ et $M_1 = \beta M$, posons $\varepsilon = \alpha\beta^{-1}$; on a $\varepsilon M = M$ et cela entraîne (§ 2-3)) que ε est une unité de l'anneau de stabilisateurs $\mathfrak{D}$ telle que $N(\varepsilon) = -1$.

Ainsi la notion de similitude au sens strict diffère de la notion habituelle seulement pour les modules d'un corps quadratique réel dont toutes les unités de l'anneau de stabilisateurs sont de norme + 1. Il est clair qu'alors toute classe de modules semblables au sens habituel se décompose en deux classes de modules strictement semblables.

Précisons la correspondance entre les classes de modules et les classes de formes.

Pour tout module M du corps $\mathbf{Q}(\sqrt{d})$, nous considérons seulement les bases $\{ a, \beta \}$ pour lesquelles le déterminant

$$\Delta = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix} \qquad (9)$$

satisfait à la condition :

$$\left.\begin{array}{ll} \Delta > 0 & \text{pour} \quad d > O \\ \frac{1}{i}\Delta > 0 & \text{pour} \quad d < 0 \end{array}\right\} \tag{10}$$

(Comme ci-dessus α' et β' désignent les conjugués de α et β dans le corps $\mathbf{Q}(\sqrt{d})$. Il existe toujours des bases de M possédant la propriété (10) : si pour une base α_1, α_2 cette propriété n'est pas satisfaite, alors il suffit de permuter α_1 et α_2).

A toute base a, β du module M satisfaisant à la condition (10) nous associerons la forme

$$f(x, y) = Ax^2 + Bxy + Cy^2 = \frac{N(\alpha x + \beta y)}{N(M)} = \frac{(\alpha x + \beta y)(\alpha' x + \beta' y)}{N(M)} \tag{11}$$

(N(M) est la norme du module M). Si nous introduisons le polynôme minimal $\varphi_\gamma(t) = at^2 + bt + c$ du nombre $\gamma = -\frac{\beta}{\alpha}$ (cf. début de 4)), alors nous aurons

$$N(\alpha x + \beta y) = \frac{N(\alpha)}{a}(ax^2 + bxy + cy^2).$$

D'autre part, d'après le corollaire du lemme 1 et le théorème 2 du § 6, la norme du module $M = a\{1, \gamma\}$ est égale à $\frac{|N(\alpha)|}{a}$; il en résulte que les coefficients A, B, C sont égaux à a, b, c au signe près. Ceci démontre que la forme (11) est primitive et que son discriminant $B^2 - 4AC$ coïncide avec le discriminant $b^2 - 4ac$ de l'anneau de stabilisateurs du module M (lemme 1). Ainsi nous avons défini une application

$$\{\alpha, \beta\} \to f(x, y) \tag{12}$$

qui à toute base $\{a, \beta\}$ vérifiant (10) du corps $\mathbf{Q}(\sqrt{d})$ associe une forme primitive $f(x, y)$ (dans le cas d'un corps réel, le coefficient A peut être négatif). Il est clair que dans le cas d'un corps quadratique imaginaire la forme (11) est toujours définie positive puisque les formes définies négatives ne sont pas obtenues par la correspondance (12).

THÉORÈME *4.* — ***Soient $\mathcal{M}$ l'ensemble de toutes les classes de modules strictement semblables du corps quadratique $\mathbf{Q}(\sqrt{d})$ et $\mathcal{F}$ l'ensemble de toutes les classes de formes pour $d > 0$ et des classes de formes définies positives pour $d < 0$, primitives, strictement équivalentes, décomposables en facteurs linéaires dans $\mathbf{Q}(\sqrt{d})$. L'application*** (12) ***établit une correspondance***

biunivoque entre $\mathcal{M}$ *et* $\mathcal{F}$; *de plus, si le discriminant de l'anneau de stabilisateurs d'un module* M *est égal à* D, *la forme correspondante a aussi pour discriminant* D.

Soient α, β et α_1, β_1 deux bases du corps $\mathbf{Q}(\sqrt{d})$ pour lesquelles les déterminants du type (9) satisfont à la condition (10) et soient f et f_1 les formes correspondantes. Pour établir le théorème 4, nous devons montrer que les formes f et f_1 sont strictement équivalentes si et seulement si $\{ a, \beta \}$ et $\{ \alpha_1, \beta_1 \}$ sont strictement semblables; de plus, nous devrons montrer que pour toute forme $g(x, y)$ irréductible primitive (décomposable en facteurs linéaires dans $\mathbf{Q}(\sqrt{d})$ et de plus définie positive si $d < 0$), il existe une base $\{ a, \beta \}$, vérifiant la condition (10) telle que $g(x, y)$ coïncide avec la forme (11). Nous nous limiterons à ces indications et laisserons au lecteur le soin de faire une démonstration détaillée.

On a défini dans 3) le produit des classes de modules semblables; nous pouvons de la même manière définir le produit des classes de modules strictement semblables. D'après la correspondance biunivoque $\mathcal{M} \to \mathcal{F}$, la multiplication des classes de modules peut se transporter aux classes de formes; l'opération ainsi définie sur $\mathcal{F}$ s'appelle la composition des classes de formes (cette terminologie est due à Gauss qui a considéré cette opération pour la première fois). Puisque toutes les classes de modules admettant un anneau de stabilisateurs donné forment un groupe (comme il est facile de le voir), toutes les classes de formes primitives de discriminant D donné (définies positives pour $d < 0$) forment aussi un groupe.

6) Représentation des nombres par des formes binaires et similitude des modules

Nous montrerons ici que le problème de la recherche des représentations des nombres entiers par des formes quadratiques binaires se réduit au problème de la similitude des modules d'un corps quadratique.

Soit $f(x, y)$ une forme quadratique binaire primitive de discriminant $D \neq 0$ décomposable en facteurs linéaires dans le corps $Q(\sqrt{d})$ et soit m un entier naturel. Dans le cas $d < 0$, nous supposerons de plus que la forme f est définie positive. Le problème posé est la recherche de toutes les solutions en nombres entiers de l'équation

$$f(x, y) = m \tag{13}$$

(nous nous limiterons aux valeurs > 0 de m puisque si $m > 0$, $D < 0$, à la place de la forme f on peut considérer la forme $-f$). D'après le théorème 4, la forme f s'écrit

$$f(x, y) = \frac{N(\alpha x + \beta y)}{N(M)}, \tag{14}$$

la base α, β du module M satisfaisant à la condition (10). L'application

$$(x, y) \to \xi = \alpha x + \beta y$$

établit une correspondance biunivoque entre les solutions de l'équation (13) et les nombres $\xi \in M$ de norme N(S) = m.N(M). Deux solutions de (13) seront dites associées si les nombres de M correspondants sont associés. Il est facile de vérifier que la notion de solutions associées ne dépend pas du choix de la représentation (14). Désignons par $\mathfrak{D}$ l'anneau des stabilisateurs du module M et par C la classe des modules strictement semblables à M. D'après le théorème 4, la classe C est définie de manière unique par la forme *f*.

Soit ξ un nombre de M de norme ***mN(M).*** Considérons le module $A = \xi M^{-1}$. Puisque $AM = \xi M^{-1}M = \xi\mathfrak{D} \subset M$, alors le module A est contenu dans $\mathfrak{D}$. Sa norme est égale à $N(\xi)N(M^{-1}) = m$. Il est clair que A appartient à la classe inverse C^{-1}.

Réciproquement supposons qu'il existe dans la classe C^{-1} un module A contenu dans $\mathfrak{D}$ et de norme ***m.*** Alors, pour un certain ξ de norme > 0 nous avons $A = \xi M^{-1}$ et par suite $\xi \in MA \subset M$ et N(E,) = ***m.*** Si A, est un autre module de la classe C^{-1} contenu dans $\mathfrak{D}$ et de norme ***m*** et si A, $= \xi_1 M^{-1}$, $N(\xi_1) > 0$, alors A, $= \xi_1\xi^{-1}A$ et cela signifie que A, coïncide avec A, ξ et ξ_1 sont associés.

Nous avons donc démontré le théorème suivant.

THÉORÈME *5.* — ***Supposons que la forme f (x, y) correspond à la classe C de modules*** (au sens strict) ***d'anneau de stabilisateurs*** $\mathfrak{D}$. ***Les classes de solutions associées de l'équation*** (13) ***sont en correspondance biunivoque avec l'ensemble des modules*** A ***qui appartiennent à la classe inverse*** C^{-1}, ***sont contenus dans l'anneau de stabilisateurs*** $\mathfrak{D}$ ***et sont de norme m. Les solutions (x, y) qui correspond au module*** A ***sont définies par les nombres*** ξ ***tels que***

$$A = \xi M^{-1}, \qquad N(\xi) > 0,$$

où M ***est un module de la classe C.***

Pour tout entier naturel ***m,*** il est facile d'écrire les modules A d'anneau de facteurs $\mathfrak{D}$ qui sont contenus dans $\mathfrak{D}$ et sont de norme ***m.*** Soit A un tel module; désignons par ***k*** le plus petit entier naturel contenu dans A. Le module A s'écrit sous la forme

$$A = \{k, k y\} = k\{l, y\}.$$

Le générateur y est défini au signe près et à l'addition près d'un nombre entier. Nous pouvons donc choisir y tel que

$$\left.\begin{array}{lll} \operatorname{Im}\gamma > 0 & \text{si} & d < 0, \\ \operatorname{Irr} y > 0 & \text{si} & d > 0 \end{array}\right\} \qquad (15)$$

(Irr y désigne la partie irrationnelle du nombre y) et tel que la partie rationnelle de y appartienne au segment $\left]-\frac{1}{2}, +\frac{1}{2}\right]$ Si nous utilisons les notations du lemme 1, le nombre y peut s'écrire

$$\gamma = \frac{-b + \sqrt{D}}{2a} \tag{16}$$

avec la condition

$$-a \leqslant b < a. \tag{17}$$

D'après l'égalité $\mathfrak{D} = \{1, a\gamma\}$ (cf. démonstration du lemme 1) et la condition $A \subset \mathfrak{D}$, nous obtenons facilement que k est divisible par a, i. e. $k = as$ pour un certain entier s. Puisque $m = N(A) = \frac{k^2}{a}$ (corollaire du lemme 1), alors

$$m = as^2. \tag{18}$$

Montrons que la représentation ainsi trouvée du module A s'écrit de manière unique

$$A = as\{1, \gamma\} \tag{19}$$

où les nombres a, s et y satisfont aux conditions (18), (15) et (15). En effet, si $as\{1, y\} = a_1 s_1\{1, y\}$, a, s_1, γ_1 satisfaisant aux mêmes exigences, alors $as = a_1 s_1$ d'où $\{1, y\} = \{1, \gamma_1\}$. D'après le corollaire du lemme 1, nous obtenons alors $a = a_1$, d'où $s = s_1$. En outre, puisque le générateur y dans le module $\{1, y\}$ satisfaisant aux conditions (15) et (17) est défini de manière unique, alors $y = \gamma_1$.

Supposons maintenant que, pour m donné, on choisit des entiers naturels a et s satisfaisant à l'égalité (18). Si b et c satisfont aux conditions

$$b^2 - 4ac = D, \qquad (a, b, c) = 1, \qquad -a \leqslant b < a, \tag{20}$$

alors pour tout nombre y de la forme (16), le module $A = as\{1, y\}$ est contenu dans son anneau de stabilisateurs $\mathfrak{D} = \{1, a\gamma\}$ et sa norme est égale à $a^2 s^2 \cdot \frac{1}{a} = m$.

Ainsi nous obtiendrons tous ces modules A en déterminant tous les systèmes de quatre nombres entiers $s > 0$, $a > 0$, b, c satisfaisant aux conditions (18) et (20).

Si nous possédons un algorithme permettant de préciser si deux modules complets du corps $\mathbf{Q}(\sqrt{d})$ sont strictement semblables, alors nous pourrons trouver parmi tous les modules $A \subset \mathfrak{D}$ de norme m ceux qui sont semblables au module M^{-1}. D'après le théorème 5, cela nous donne toutes les solutions de l'équation (13).

Du théorème 5 découle facilement le théorème suivant.

THÉORÈME *6.* — ***Pour que le nombre naturel n soit représentable par une forme quadratique binaire primitive de discriminant*** D, ***il faut et il suffit que l'ordre*** $\mathfrak{D}$ ***de discriminant*** D ***contienne un module*** A ***de norme m admettant l'ordre*** $\mathfrak{D}$ ***pour anneau de stabilisateurs.***

Cette condition équivaut à l'existence d'entiers $s > 0$, $a > 0$, b, c satisfaisant aux conditions $m = as^2$, $b^2 - 4ac = D$, $(a, b, c) = 1$, $-a \leqslant b < a$.

Dans le cas où D est le discriminant de l'ordre maximum $\tilde{\mathfrak{D}}$, le théorème 6 se simplifie. On a

THÉOREME *7.* — ***Soit*** D ***le discriminant d'un corps quadratique*** (i. e. le ***discriminant de l'ordre maximum). Pour qu'un entier naturel*** $m = as^2$ ***où a est sans carré soit représentable par une forme primitive binaire de discriminant*** D, ***il faut et il suffit que la congruence***

$$x^2 \equiv D \pmod{4a} \tag{21}$$

admette une solution.

Nous laissons au lecteur la démonstration du théorème 7.

7) Similitude des modules dans un corps quadratique imaginaire

Dans le cas d'un corps quadratique imaginaire $\mathbf{Q}(\sqrt{d})$, $d < 0$ le problème de la similitude des modules admet une solution simple.

La représentation des nombres $a \in \mathbf{Q}(\sqrt{d})$ par des points de l'espace $\mathcal{R}^2$ (cf. § 3, 1)) coïncide avec la représentation habituelle des nombres complexes dans le plan de la variable complexe. Les nombres d'un module complet $M \subset \mathbf{Q}(\sqrt{d})$ sont représentés dans $\mathcal{R}^2$ par les points (ou les vecteurs) d'un certain lattice complet. Nous ne distinguerons pas dans la suite les nombres complexes de leur représentation dans le plan $\mathcal{R}^2$; ainsi nous désignerons par M le lattice correspondant de $\mathcal{R}^2$. Puisque la multiplication des points du lattice M par un nombre complexe $\xi \neq 0$ correspond à une rotation d'angle arg ξ (autour de l'origine) du lattice M suivie d'une homothétie de rapport $|\xi|$, les lattices de deux modules semblables M et ξM sont semblables au sens géométrique. Cette remarque évidente est la base de ce qui suit.

Le problème de la similitude des lattices du plan sera résolu au moyen d'une base particulière dite base réduite. Une ***base réduite*** a, β est formée d'un vecteur $a \neq 0$ le plus court possible et d'un vecteur $\beta \neq 0$ le plus court possible parmi les vecteurs non colinéaires à a (assujettis à certaines conditions supplémentaires). Montrons qu'une telle paire de vecteurs a, β for-

ment toujours une base. En effet, dans le cas contraire, il existerait dans M un vecteur $\xi = u\alpha + v\beta$ pour lequel les nombres réels u et v ne sont pas tous les deux entiers. Ajoutant éventuellement à ce vecteur une combinaison linéaire de a et β à coefficients entiers, il est clair que nous pouvons supposer $|u| \leqslant \frac{1}{2}$ et $|v| \leqslant \frac{1}{2}$. Si $v \neq 0$, alors, d'après le choix de β, on aurait $|\xi| \geqslant |\beta|$ ce qui contredit l'inégalité

$$|\xi| < |u\alpha| + |v\beta| \leqslant \frac{1}{2}|\alpha| + \frac{1}{2}|\beta| \leqslant |\beta|.$$

Si maintenant $v = 0$, alors $|\xi| = |u\alpha| \leqslant \frac{1}{2}|a| < a$ en contradiction avec le choix de a. Ceci démontre que a, β est une base.

Si a est un des vecteurs les plus courts et β un des vecteurs les plus courts non colinéaires à a, alors la longueur de la projection du vecteur β sur le vecteur a ne dépasse pas $\frac{1}{2}|a|$. En effet, parmi les vecteurs $\beta + na$ (n entier), il existe un vecteur dont la projection est inférieure ou égale à $\frac{1}{2}|a|$. D'autre part, celui des vecteurs $\beta + na$ qui a la plus petite longueur est le vecteur qui a la plus petite projection.

Pour un lattice donné M, considérons maintenant tous les vecteurs $\neq 0$ de longueur minimum; soit w le nombre de ces vecteurs. Puisque $-a$ est de même longueur que a, le nombre w est pair. De plus, l'angle de deux vecteurs a et a' de longueur minimum ne peut pas être inférieur à $\frac{\pi}{3}$; en effet, sinon le vecteur $a - a'$ du lattice serait de longueur plus petite. Par suite, $w \leqslant 6$ et cela signifie que les seules valeurs possibles sont $w = 2$, $w = 4$, $w = 6$.

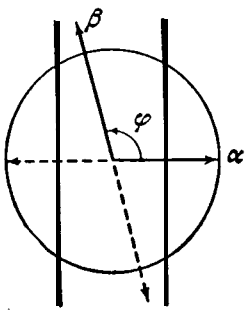


FIG. 1.

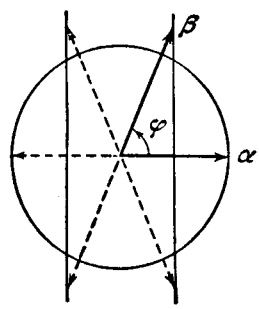


FIG. 2.

Construisons une ***buse réduite*** du lattice M. Si $w = 2$, nous choisirons pour a un des deux vecteurs de longueur minimum. Parmi les vecteurs non colinéaires à α, il existe deux ou quatre vecteurs de longueur minimum (cf. fig. 1 et 2); nous choisirons pour β celui pour lequel l'angle φ compté de a vers β dans le sens inverse des aiguilles d'une montre est le plus petit.

Si maintenant w = 4 ou w = 6, nous prendrons pour base réduite un couple de vecteurs a et β de longueur minimum pour lequel l'angle φ compté de α vers β dans le sens positif soit minimum.

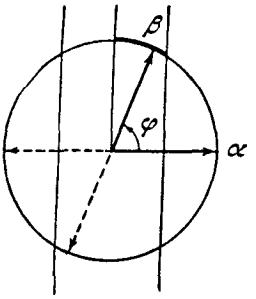


FIG. 3.

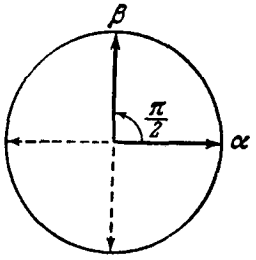


FIG. 4.

Il est facile de voir que la base réduite est définie par le lattice de manière unique, à une rotation près laissant le lattice invariant. Dans les cas w = 2, $w = 4, \frac{\pi}{3} < \varphi < \frac{\pi}{2}$ (cf. fig. 3) on a deux bases réduites qui sont superposables par rotation d'angle un multiple de π. Pour w = 4, $\varphi = \frac{\pi}{2}$ (fig. 4) nous avons un lattice qui a quatre bases réduites déduites l'une de l'autre par des rotations d'angles multiples de $\frac{\pi}{2}$. Enfin, pour w = 6 nous avons six bases réduites déduites l'une de l'autre par des rotations d'angle multiples de $\frac{\pi}{3}$ (fig. 5); la circonférence est divisée en six parties égales puisque les

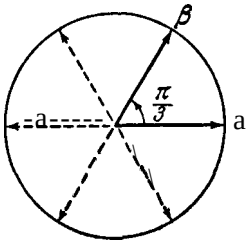


FIG. 5.

angles entre les vecteurs de longueur minimum ne peuvent pas être inférieurs à $\frac{\pi}{3}$,

En utilisant la notion de base réduite, on peut maintenant résoudre facilement le problème de la similitude des lattices du plan.

THÉORÈME 8. — *Deux lattices* M *et* M_1 *de* $\mathcal{R}^2$ *sont semblables si et seulement si leurs bases réduites sont semblables* (i. e. passent l'une dans l'autre par une rotation suivie d'une homothétie).

DÉMONSTRATION. — Soient α, β et α_1, β_1 des bases réduites des lattices M et M,. Si $\xi M = M_1$, alors $\xi\alpha$ et $\xi\beta$ est une base réduite de M,. Comme nous l'avons vu, cette base est déduite par rotation de la base α_1, β_1; ainsi, il existe un nombre η (racine d'ordre 1, 2, 4 ou 6 de l'unité) tel que $\eta\xi\alpha = \alpha_1$ et $\eta\xi\beta = \beta_1$. La base α_1, β_1 est bien obtenue à partir de a, β par rotation d'angle arg $(\eta\xi)$ suivie d'une homothétie de rapport $|\xi|$. La réciproque est triviale.

Passons à la description des classes de modules semblables d'un corps quadratique imaginaire. Soit M un module de $\mathbf{Q}(\sqrt{d})$, $d < 0$ et soit a, β une base réduite de M ; considérons un module semblable $\frac{1}{\alpha} M = \{1, y\}$ avec $y = \frac{\beta}{a}$. La base 1, y est ici réduite; il résulte facilement de la définition d'une base réduite que le nombre y satisfait aux conditions

$$\operatorname{Im} \gamma > 0 \tag{22}$$

$$-\frac{1}{2} < \operatorname{Re}\gamma \leqslant \frac{1}{2}, \tag{23}$$

$$\left.\begin{array}{ll} |\gamma| > 1 \text{ si } & -\frac{1}{2} < \operatorname{Re}\gamma < 0 \\ |\gamma| \geqslant 1 \text{ si } & 0 \leqslant \operatorname{Re}\gamma \leqslant \frac{1}{2} \end{array}\right\} \tag{24}$$

DÉFINITION. — *Un nombre y d'un corps quadratique imaginaire est dit réduit s'il satisfait aux conditions* (22), *(23) et (24). Simultanément avec y, le module* $\{1, y\}$ *est dit réduit.*

La signification géométrique du fait que y soit réduit est que sa représentation dans le plan complexe appartient à la région Γ indiquée par la figure 6 (la frontière est divisée en deux parties, l'une qui inclut le point *i* appartient à Γ et l'autre pas).

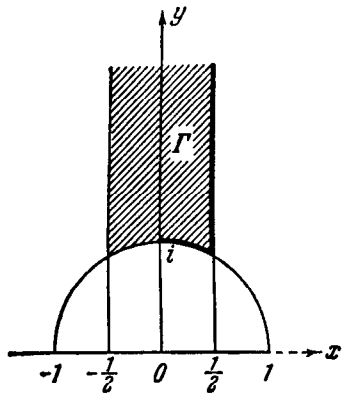


FIG. 6.

THÉORÈME 9. — *Toute classe de modules semblables du corps quadratique imaginaire* $\mathbf{Q}(\sqrt{d})$, $d > 0$, *contient un module réduit et un seul.*

DÉMONSTRATION. — On a déjà dtmontré que tout module est semblable à un module réduit. Il reste à vérifier que deux modules réduits distincts ne sont pas semblables. Pour cela, démontrons tout d'abord que pour tout nombre $y = x + yi$ réduit, les nombres 1, y forment une base réduite du lattice $\{ 1, y \}$. Il faut vérifier que y est le plus petit vecteur du lattice $\{ 1; y \}$ non situé sur la droite réelle, i. e. que $| k + l\gamma | \geqslant | y |$ pour tous les entiers k et $l \neq 0$. Puisque $| x | \leqslant \frac{1}{2}$, alors

$$| k \pm y |^2 = (k \pm x)^2 + y^* \geqslant x^2 + y^2 = | y |^2.$$

Si maintenant $| l | \geqslant 2$, alors

$$| k + l\gamma |^2 \geqslant l^2 y^2 > 2y^2 > x^2 + y^2 = | \gamma |^2,$$

ce qui démontre notre affirmation. Soient maintenant y et γ_1 deux nombres réduits. Si les modules $\{ 1, y \}$ et $\{ 1, \gamma_1 \}$ sont semblables alors, d'après le théorème 8, les bases 1, y et 1, γ_1 sont semblables. Mais cela n'est possible, comme il est facile de le voir, que pour $y = \gamma_1$. Le théoréme 9 est complètement démontré.

Pour résoudre complètement le problème de la similitude des modules, il faut donner un algorithme permettant de trouver le module réduit semblable à un module donné. Un tel algorithme est construit dans l'exercice 24. Les modules $\mathbf{M}_1$ et $\mathbf{M}_2$ sont semblables si et seulement si les modules réduits qui leur sont semblables coïncident.

Remarque. — Dans la démonstration du théorème 9 nous n'avons nulle part utilisé le fait que les modules considérés sont contenus dans un corps quadratique imaginaire. L'argument de ce théorème est donc vrai pour des lattices plans quelconques : ***tout lattice du plan complexe est semblable à*** un lattice et un seul de la forme $\{1, y\}$ y étant un nombre de la région Γ hachurée sur la figure 6. D'après le lemme 2, deux lattices de la forme $\{1, A\}$ et $\{1, y\}$ sont semblables si et seulement si A et y sont liés par la relation

$$\lambda = \frac{k\gamma + l}{m\gamma + n}, \qquad k n - m l = \pm 1,$$

à coefficients entiers $k, l, m,$ n. Deux tels nombres complexes non réels sont dits ***modulairement équivalents.*** Le résultat ci-dessus signifie donc que tout nombre complexe non réel est modulairement équivalent à un nombre de la région Γ et un seul. Cet ensemble Γ est souvent appelé ***domaine modulaire.*** D'après ce qui a été vu ci-dessus les points de Γ correspondent biunivoquement aux classes de lattices plans semblables. Le problème de la similitude des lattices plans est lié à de très nombreuses questions, en particulier à la théorie des fonctions elliptiques. Tout corps de fonctions elliptiques est caractérisé par son lattice de périodes et deux corps de fonctions elliptiques sont isomorphes si et seulement si les lattices de périodes correspondants sont semblables (cf. par exemple C. Chevalley, ***Introduction to the theory of algebraic jiinctions of one variable,*** New York, A. M. S., 1951). Ainsi les points du domaine modulaire Γ correspondent biunivoquement aux types de corps de fonctions elliptiques non isomorphes.

Considérons maintenant les classes de modules semblables admettant pour anneau de stabilisateurs un certain ordre $\mathfrak{D}$ de discriminant $D < 0$. Considérons un module $\{1, y\}$, $y \in \Gamma$, associé à l'ordre $\mathfrak{D}$. Si nous utilisons les notations du lemme 1, le nombre y s'écrit

$$\gamma = \frac{-b + i\sqrt{|D|}}{2a},$$

et les conditions (23) et (24) donnent :

$$\left.\begin{array}{lll} -a \leqslant b < a & & \\ c \geqslant a & \text{si} & b \leqslant 0 \\ c > a & \text{si} & b > 0 \end{array}\right\} \qquad (25)$$

Ainsi, pour obtenir un système complet de modules réduits d'anneau de stabilisateurs de discriminant D, il faut trouver tous les systèmes de trois nombres entiers $a > 0$, $b,$ c satisfaisant aux inégalités (25) et aux conditions

$$D = b^2 - 4ac, \qquad (a, b, c) = 1. \qquad (26)$$

D'après le théorème 3 du § 6, le nombre de tels systèmes de trois nombres est fini, ce qui est d'ailleurs clair d'après les inégalités

$$|D| = 4ac - b^2 \geqslant 4a^2 - a^2 = 3a^2, \qquad |b| \leqslant a < \sqrt{\frac{|D|}{3}}.$$

Exemple 1. — Déterminons le nombre de classes de modules admettant pour anneau de stabilisateurs l'ordre maximum du corps $\mathbf{Q}(\sqrt{-47})$. Puisque ici $D = -47$, alors $|b| \leqslant a < \sqrt{\frac{47}{3}}$. Remarquant que puisque D est impair, le nombre b est aussi impair, nous avons les possibilités suivantes :

$$b = \pm 1, \qquad b = \pm 3.$$

Dans ce dernier cas nous aurions $b^2 - D = 56 = 4ac$, $ac = 14$, $3 \leqslant a \leqslant c$, ce qui est impossible. Si maintenant $b = \pm 1$, alors $b^2 - D = 48 = 4ac$, d'où $a = 1$, $c = 12$; $a = 2$, $c = 6$; $a = 3$, $c = 4$. Puisque le cas $b = 1 = a$ doit être exclu, nous obtenons qu'il existe cinq classes de modules semblables associés à l'ordre maximum du corps $\mathbf{Q}(\sqrt{-47})$. Les modules réduits $\{1, y\}$ de ces classes sont obtenus pour les valeurs de y ci-dessous

$$\frac{1 + i\sqrt{47}}{2}, \qquad \frac{\pm 1 + i\sqrt{47}}{4}, \qquad \frac{\pm 1 + i\sqrt{47}}{6}.$$

Exemple 2. — Cherchons dans le module $M = \{13, 1 + 5i\}$ tous les nombres de norme 650. L'anneau de stabilisateurs est ici l'ordre $\mathfrak{D} = \{1, 5i\}$ de discriminant $D = -100$. Puisque $N(M) = 13$, il nous faut trouver les modules $A \subset \mathfrak{D}$, associés à $\mathfrak{D}$ et de norme $m = \frac{650}{13} = 50$. Les conditions (18) et (20) donnent les possibilités suivantes :

1°	$s = 5$,	$a = 2$,	$b = -2$,	$c = 13$;
2°	$s = 1$,	$a = 50$,	$b = 10$,	$c = 1$;
3°	$s = 1$,	$a = 50$,	$b = -10$,	$c = 1$;
4°	$s = 1$,	$a = 50$,	$b = -50$,	$c = 13$.

Pour chacun de ces quatre cas, considérons le module A de type (19) correspondant et déterminons le module réduit qui lui est semblable :

$$10\left\{1, \frac{1 + 5i}{2}\right\},$$

$$50\left\{1, \frac{-1 + i}{10}\right\} = (-55 + 5i)\{1, 5i\}$$

$$50\left\{1, \frac{1 + i}{10}\right\} = (5 + 5i)\{1, 5i\}$$

$$50\left\{1, \frac{5 + i}{10}\right\} = 10i\left\{1, \frac{1 + 5i}{2}\right\}.$$

Trouvons de même le module réduit semblable à M^{-1} :

$$M^{-1} = \left\{1, \frac{1-5i}{13}\right\} = \frac{1-5i}{13}\left\{1, \frac{1+5i}{2}\right\}$$

Les modules A qui correspondent aux cas 2° et 3° sont à rejeter car ils ne sont pas semblables au module M^{-1}. Dans les deux autres cas 1° et 4° l'égalité $A = \xi M^{-1}$ est satisfaite pour $\xi = 5 + 2i$ et $\xi = -25 + 5i$. Puisque les deux seules unités de $\mathfrak{D}$ sont ± 1, nous avons démontré qu'il existe dans le module M quatre nombres $\pm(5 + 25i), \pm(-25 + 5i)$ de norme 650.

Nous avons ainsi établi que l'équation $13x^2 + 2xy + 2y^2 = 50$ a quatre solutions en nombres entiers :

$$x = 0,\ y = 5\ ; \qquad x = 0,\ y = -5$$
$$x = 2,\ y = -1\ ; \qquad x = -2,\ y = 1\ .$$

Exemple 3. — Quels sont les entiers naturels qui sont représentables par la forme $x^2 + y^2$?

Le discriminant de la forme est égal à $D = -4$. Pour l'ordre $\mathfrak{D} = \{1, i\}$ du corps $\mathbf{Q}(\sqrt{-1})$ (de discriminant -4), il existe seulement un module réduit puisque les conditions (25) et (26) ne sont satisfaites que pour $a = c = 1$, $b = 0$. Cela signifie que tous les modules admettant $\mathfrak{D}$ pour anneau de stabilisateurs sont semblables entre eux et par suite toutes les formes binaires de discriminant -4 sont équivalentes à la forme $x^2 + y^2$. Mais des formes équivalentes représentent les mêmes nombres et par suite, d'après le théorème 6, la forme $x^2 + y^2$ reprbente le nombre m si et seulement s'il existe un module $A \subset \mathfrak{D}$, d'anneau de stabilisateurs $\mathfrak{D}$ et de norme m. Si un tel module existe, il existe des entiers s, a, b, c tels que

$$m = as^2, \qquad D = -4 = b^2 - 4ac, \qquad (a, b, c) = 1.$$

Ici le nombre b est nécessairement pair : $b = 2z$, et z satisfait à la congruence

$$z^2 \equiv -1 \pmod{a}. \tag{27}$$

Réciproquement si cette congruence est résoluble pour un certain $a = \frac{m}{s^2}$, i. e. $z^2 = -1 + ac$, alors il est facile de voir que (a, 2z, c) = 1 et cela signifie qu'il existe un module $A \subset \mathfrak{D}$, d'anneau de stabilisateurs $\mathfrak{D}$ de norme m, i. e. m est représentable par la forme $x^2 + y^2$.

Comme on le sait, la congruence (27) est résoluble si et seulement si a n'est pas divisible ni par 4 ni par un nombre premier de la forme $4k + 3$. Puisque a contient tous les facteurs premiers qui figurent dans m avec un exposant impair, nous obtenons finalement que m est représenté par la forme $x^2 + y^2$ si et seulement si les nombres premiers de la forme $4k + 3$ qui interviennent dans sa décomposition sont affectés d'un exposant pair.

EXERCICES

1. Trouver des unités fondamentales des corps $\mathbf{Q}(\sqrt{19})$ et $\mathbf{Q}(\sqrt{37})$.

2. Démontrer que si $d \equiv 1 \pmod 8$ (et d sans carrés), alors toute unité fondamentale de l'ordre $\{1, \sqrt{d}\}$ est aussi une unité fondamentale de l'ordre maximum du corps $\mathbf{Q}(\sqrt{d})$, $d > 0$.

3. Démontrer que si le discriminant d'un ordre $\mathfrak{D}$ d'un corps de nombres algébriques est divisible par au moins un nombre premier de la forme $4n + 3$, alors la norme de toute unité de $\mathfrak{D}$ est égale à $+1$.

4. Soit $m > 1$ un entier qui n'est pas un carré parfait. Montrer que dans la décomposition de $\sqrt{m}$ en fraction continue, la suite des quotients partiels s'écrit

$$q_0, q_1, \ldots, q_s, 2q_0, q_1, \ldots, q_s, 2q_0, q_1, \ldots$$

(ici $q_{i+1} = q_{s-i}$, $i = 0, 1, \ldots, s-1$).

5. Utilisant les mêmes notations, montrer que si $\frac{P_s}{Q_s}$ est la fraction qui correspond à l'avant-dernier terme de la plus petite période,' alors $P_s + Q_s\sqrt{m}$ est une unité fondamentale de l'ordre $\{1, \sqrt{m}\}$ (dans le corps $\mathbf{Q}(\sqrt{d})$).

6. Supposons que les anneaux de stabilisateurs de deux modules $\mathbf{M}_1$ et $\mathbf{M}_2$ d'un corps quadratique sont respectivement $\mathfrak{D}_{f_1}$ et $\mathfrak{D}_{f_2}$ (pour les notations, voir fin du point 2)). Montrer que l'anneau des stabilisateurs du produit $\mathbf{M}_1\mathbf{M}_2$ est l'ordre $\mathfrak{D}_f$ où f est le plus grand diviseur commun de f_1 et f_2.

7. Pour tout entier naturel f, désignons par $\mathfrak{C}_f$ le groupe des modules d'un corps quadratique donné qui sont associés à l'ordre $\mathfrak{D}_f$ (cf. fin du point 4)). Montrer que si d est un diviseur de f, alors l'application $M \to M\mathfrak{D}_d$ (Me $\mathfrak{C}_f$) est un homomorphisme du groupe $\mathfrak{C}_f$ sur le groupe $\mathfrak{C}_d$.

8. Soit ξ un nombre de l'ordre maximum $\tilde{\mathfrak{D}} = \{1, \omega\}$ d'un corps quadratique, premier avec l'entier naturel f. Montrer que l'anneau des stabilisateurs du module $\mathbf{M} = \{f, f\omega, \xi\}$ est $\mathfrak{D}_f$ et que $\mathbf{M}\tilde{\mathfrak{D}} = \tilde{\mathfrak{D}}$. Montrer réciproquement que tout module M associé à l'ordre $\mathfrak{D}_f$ et tel que $\mathbf{M}\tilde{\mathfrak{D}} = \tilde{\mathfrak{D}}$ est de la forme $\mathrm{M} = \{f, f\omega, \xi\}$ pour un certain $\xi \in \tilde{\mathfrak{D}}$ premier avec f.

9. Soient ξ_1 et ξ_2 deux nombres de $\tilde{\mathfrak{D}}$ premiers avec f. Démontrer que les modules $\{f, f\omega, \xi_1\}$ et $\{f, f\omega, \xi_2\}$ sont égaux si et seulement si $s\xi_1 = \xi_2$ pour un certain entier rationnel s.

10. Soient $\mathbf{M}_1$ et $\mathbf{M}_2$ des modules complets quelconques (non associés nécessairement au même ordre) d'un corps quadratique. Démontrer la formule

$$\mathrm{N}(\mathbf{M}_1\mathbf{M}_2) = \mathrm{N}(\mathbf{M}_1)\,\mathrm{N}(\mathbf{M}_2).$$

11. Démontrer que le nombre h de classes de modules semblables associés à l'ordre maximum $\tilde{\mathfrak{D}}$ d'un corps quadratique et le nombre h_f de classes de modules semblables associés à l'ordre $\mathfrak{D}_f$ (d'indice f) sont liés entre eux par la relation

$$h_f = h\,\frac{\Phi(f)}{e_f\varphi(f)},$$

où@(f) est le nombre de classes résiduelles de $\tilde{\mathfrak{D}}$ modulo f formées de nombres premiers avec f (l'analogue de la fonction d'Euler $\varphi(f)$) et e_f l'indice du groupe des unités de l'ordre $\mathfrak{D}_f$ dans le groupe des unités de l'ordre maximum $\tilde{\mathfrak{D}}$.

12. Un nombre y d'un corps quadratique réel est dit ***réduit*** s'il vérifie la condition $0 < y < 1$ et si son conjugué y' vérifie l'inégalité $y' < -1$. Simultanément avec y, le module $\{1, y\}$ est aussi dit ***réduit.*** Avec les notations du lemme 1, démontrer que y est réduit si et seulement si

$$0 < b < \sqrt{D}, \quad -b + \sqrt{D} < 2a < b + \sqrt{D}.$$

En déduire que le nombre de modules réduits associés à un ordre fixé d'un corps quadratique est fini.

13. Soit y un nombre irrationnel d'un corps quadratique réel tel que $0 < y < 1$. Posons

$$\gamma_1 = -(\text{signe de } y') \frac{1}{\gamma} - n,$$

où l'entier rationnel n est choisi de telle sorte que $0 < \gamma_1 < 1$. Démontrer qu'au bout d'un nombre fini de transformations du type $\{1, y\} \to \{1, \gamma_1\}$, le module $\{1, y\}$ a pour image un module semblable qui est réduit. Ainsi, toute classe de modules semblables (au sens usuel) d'un corps quadratique réel contient un module réduit.

14. Soit y un nombre réduit d'un corps quadratique réel. Puisque le signe de y' est égal à -1, la transformation $y \to \gamma_1$ de l'exercice précédent s'écrit, dans le cas où y est réduit,

$$\gamma_1 = \frac{1}{\gamma} - n, \qquad n = \left[\frac{1}{\gamma}\right],$$

Démontrer que le nombre γ_1 est aussi réduit; on dit que γ_1 est adjacent à droite au nombre y et que le nombre initial y est adjacent à gauche à γ_1. Vérifier que pour tout γ_1 réduit il existe un nombre réduit y adjacent à gauche et un seul.

15. Partant d'un nombre réduit γ_0 d'un corps quadratique réel, construisons la suite de nombres réduits $\gamma_0, \gamma_1, \gamma_2, \ldots$ dans laquelle tout nombre est adjacent à droite au nombre qui le précède. Pour un certain entier naturel m, on a l'égalité $\gamma_m = \gamma_0$, i. e. la suite est périodique. Si on choisit m minimum, les nombres $y_{,,,}$ $\gamma_1, \ldots, \gamma_{m-1}$ sont distincts; une telle suite finie de nombres réduits est appelée une période. Démontrons que deux modules réduits $\{1, y\}$ et $\{1, y^*\}$ sont semblables (au sens usuel) si et seulement si les nombres y et y* appartiennent à une même période.

16. Trouver le nombre de classes de modules semblables associés à l'ordre maximum du corps $\mathbf{Q}(\sqrt{10})$.

17. Montrer que toutes les solutions en nombres entiers de l'équation

$$17x2 + 32xy + 14y^2 = 9$$

sont données par les formules

$$\pm (15 + 6\sqrt{2})(3 + 2\sqrt{2})^n = \pm [17x_n + (16 + 3\sqrt{2})y_n]$$

(pour tout entier n).

18. Parmi les modules

$$\{1, \sqrt{15}\}, \{2, 1 + \sqrt{15}\}, \{3, \sqrt{15}\}, \{35, 20 + \sqrt{15}\}$$

du corps $\mathbf{Q}(\sqrt{15})$, quels sont ceux qui sont semblables entre eux ?

19. Trouver un systéme complet de représentants des classes de formes primitives strictement équivalentes de discriminant 252.

20. Combien existe-t-il de classes de formes primitives strictement équivalentes de discriminant 360 ?

21. Quels sont les nombres premiers représentables par les formes $x^2 + 5y^2$ et $2x^2 + 2xy + 3y^2$?

22. Résoudre en nombres entiers les équations suivantes :

1) $5x^2 + 2xy + 2y^2 = 26;$

2) $5x^2 - 2y^2 = 3;$

3) $80x^2 - y^2 = 16.$

23. Montrer que les équations

1) $13x^2 + 34xy + 22y^2 = 23;$

2) $5x^2 + 16xy + 13y^2 = 23,$

n'ont pas de solutions en nombres entiers.

24. Soit y un nombre d'un corps quadratique imaginaire qui satisfait aux conditions Im $\gamma > 0$, $-\frac{1}{2} <$ Re y $\leqslant \frac{1}{2}$ mais n'est pas réduit. Posons $\gamma_1 = -\frac{1}{\gamma} + n$, ou l'entier rationnel n est choisi tel que $-\frac{1}{2} <$ Re y $\leqslant \frac{1}{2}$. Si γ_1 n'est pas réduit, nous poserons de même $\gamma_2 = -\frac{1}{\gamma_1} + n_1$, etc. Démontrer qu'au bout d'un nombre fini de telles opérations le module $\{ 1, y \}$ a pour image un module semblable réduit $\{ 1, \gamma_s \}$.

25. Déterminer le nombre de classes de modules semblables associés à l'ordre maximum du corps $\mathbf{Q}(\sqrt{-47})$.

26. Trouver, dans le module $\{ 13,1 + 5i \}$, tous les nombres de norme 650.

27. Déterminer les anneaux des stabilisateurs des modules

$$\{11,\ 6 + 2i\sqrt{2}\},\ (2,\ 1 + i\sqrt{2}\},\ (4,\ i\sqrt{2}\},\ \{2, i\sqrt{2}\}.$$

Quels sont ceux de ces modules qui sont semblables entre eux ?

28. Montrer que dans le corps $\mathbf{Q}(\sqrt{-43})$ tous les modules associés à l'ordre maximum sont semblables entre eux.

CHAPITRE III

THÉORIE DE LA DIVISIBILITÉ

Dans le chapitre précédent, nous avons vu un exemple de résolution d'un problème pratique à l'aide de la théorie des nombres algébriques : la recherche des représentations des nombres rationnels par des formes décomposables complètes à coefficients entiers est étroitement liée à la théorie des unités dans les ordres des corps de nombres algébriques.

De nombreux problèmes de la théorie des nombres dépendent d'une importante question de l'arithmétique des corps de nombres algébriques, la décomposition des nombres algébriques en facteurs premiers.

Dans ce chapitre, nous exposerons la théorie générale de la décomposition des nombres algébriques en facteurs et donnerons ses applications à certains problèmes de la théorie des nombres. Nous utiliserons ici les résultats de la théorie des anneaux qui sont exposés dans le § 5 de l'appendice. Ces propriétés et les propriétés des extensions finies des corps déjà utilisées dans le deuxième chapitre constituent l'appareil algébrique de ce chapitre.

Le théorème de Fermat est étroitement lié à cette décomposition des nombres algébriques en facteurs. Historiquement, c'est ce théorème qui a conduit Kummer à ses travaux sur l'arithmétique des nombres algébriques qui contiennent les idées essentielles de cette théorie.

Nous commencerons donc par l'étude du premier résultat de Kummer relatif au théorème de Fermat, comme introduction à la théorie de la décomposition des nombres algébriques en facteurs.

§ 1. — QUELQUES CAS PARTICULIERS DU THÉORÈME DE FERMAT

1) Lien entre le théorème de Fermat et la décomposition en facteurs

L'hypothèse de Fermat est la suivante : pour $n > 2$, l'équation

$$x^n + y^n = z^n$$

n'a pas de solution x, y, z en nombres entiers rationnels non nuls.

Il est clair que si on a démontré le théorème de Fermat pour un certain exposant n, ce théorème est aussi démontré pour tous les exposants multiples de n. Puisque tout entier $n > 2$ est divisible soit par 4 soit par un nombre premier impair, on peut se limiter aux cas où l'exposant est égal à 4 ou à un nombre premier impair. Pour $n = 4$, Euler a donné une démonstration élémentaire. Nous nous limiterons donc dans ce qui suit à l'étude de l'équation

$$x^l + y^l = z^l \tag{1}$$

dans laquelle l'exposant l est un nombre premier impair. Il est évident que l'on peut supposer les nombres x, y, z dans l'équation (1) premiers entre eux deux à deux.

Pour les valeurs de l pour lesquelles le théorème de Fermat a été dtmontré, la démonstration se décompose en deux étapes : on montre tout d'abord que l'équation (1) n'a pas de solutions parmi les entiers non divisibles par l; on montre ensuite qu'elle n'a pas non plus de solution x, y, z telle que l'un de ces nombres (et seulement un) soit divisible par l. Ces deux étapes s'appellent respectivement ***premier*** et ***deuxième cas*** du théorème de Fermat. On peut conjecturer actuellement d'après les cas particuliers déjà démontrés que les démonstrations de ces deux cas sont de même difficulté, bien que le premier cas semble un peu plus simple techniquement. Nous nous occuperons pour commencer du premier cas du théorème de Fermat.

Le rôle des nombres algébriques dans le théorème de Fermat s'explique par les considérations simples suivantes. Si on désigne par ζ une racine primitive d'ordre l de 1, l'équation (1) peut s'écrire

$$\prod_{k=0}^{l-1} (x + \zeta^k y) = z^l. \tag{2}$$

Dans le cas des entiers rationnels, si un produit de facteurs premiers entre eux deux à deux est une puissance $l^{\text{ième}}$ d'un nombre, alors chacun des facteurs est déjà une puissance $l^{\text{ième}}$ (d'après l'unicité de la décomposition en facteurs premiers). Ici les facteurs de la partie gauche de (1) appartiennent au corps $\mathbf{Q}(\zeta)$ de nombres algébriques, de degré $l - 1$ sur Q (il est facile de montrer que le polynôme $t^{l-1} + t^{l-2} + \ldots + t + 1$, pour l premier, est irréductible sur le corps des nombres rationnels; cf. par exemple exercice 6 ou théorème 1 du § 2 du chapitre 5). Considérons dans le corps $\mathbf{Q}(\zeta)$ l'ordre $\mathfrak{D} = \{1, \zeta, \ldots, \zeta^{l-2}\}$ (d'après le théorème 1, § 5 du chapitre V, $\mathfrak{D}$ est l'ordre maximum du corps $\mathbf{Q}(\zeta)$). Supposons que dans l'anneau $\mathfrak{D}$, la décomposition d'un nombre en facteurs premiers soit définie de manière unique. Alors, pour tout $\alpha \in \mathfrak{D}$, $a \neq 0$,

$$a = \varepsilon \pi_1^{a_1} \ldots \pi_r^{a_r}$$

où ε est unité de l'anneau $\mathfrak{D}$, où les nombres premiers $\pi_1, \ldots, \pi_2$ ne sont pas associés et où les exposants a, . . . , a, sont définis de manière unique. Il est clair que tout nombre premier π intervenant dans la décomposition du nombre z^l intervient dans la décomposition avec un exposant multiple de l. D'autre part, on montrera ci-dessous que, dans le premier cas du théorème de Fermat, les nombres $x + \zeta^k y$ $(k = 0, 1, \ldots, l - 1)$ sont premiers deux à deux. Par suite, si nous représentons $x + \zeta^k y$ comme produit de puissances de facteurs premiers, tout nombre premier de cette décomposition interviendra avec un exposant multiple de l. Cela signifie que tout $x + \zeta^k y$, à un facteur qui est une unité près, est une puissance $l^{\text{ième}}$. En particulier,

$$x + \zeta y = \varepsilon\alpha^l, \tag{3}$$

où ε est une unité de l'anneau $\mathfrak{D}$ et $a \in \mathfrak{D}$.

Puisque l'égalité $x^l + y^l = z^l$, d'après l'imparité de l, peut s'écrire sous la forme

$$x^l + (-z)^l = (-y)^l,$$

nous obtenons de manière analogue

$$x - \zeta z = \varepsilon_1\alpha_1^l. \tag{3'}$$

Il faut montrer que les égalités (3) et (3') conduisent à une contradiction. Dans ce cas, on aura démontré l'impossibilité de résoudre l'équation (1) en nombres entiers x, y, z non divisibles par l.

Établissons quelques propriétés de l'anneau $\mathfrak{D}$.

2) L'anneau Z [ζ]

LEMME 1. — *Dans l'anneau* $\mathfrak{D} = \mathbf{Z}[\zeta]$ *le nombre* $1 - \zeta$ *est premier et* l *admet la décomposition*

$$l = \varepsilon^*(1 - \zeta)^{l-1} \tag{4}$$

où ε^* *est une unité de* $\mathfrak{D}$.

DÉMONSTRATION. — Faisant $t = 1$ dans la décomposition

$$t^{l-1} + t^{l-2} + \ldots + t + 1 = (t - \zeta)(t - \zeta^2) \ldots (t - \zeta^{l-1}),$$

nous obtenons

$$l = (1 - \zeta)(1 - \zeta^2) \ldots (1 - \zeta^{l-1}). \tag{5}$$

Si $a = r(\zeta)$ est un nombre du corps $\mathbf{Q}(\zeta)$ (ici $r(t)$ est *un* polynôme à coefficients rationnels), alors les nombres

$$\sigma_k(\alpha) = r(\zeta^k) \qquad (1 \leqslant k \leqslant l - 1) \tag{6}$$

peuvent être considérés comme les images de α par tous les isomorphismes de $\mathbf{Q}(\zeta)$ dans le corps des nombres complexes. Autrement dit, d'après la terminologie du § 2-3) de l'appendice, ce sont les conjugués de α et par suite $N(a) = \prod_{k=1}^{l-1} r(\zeta^k)$. En particulier, pour $s \not\equiv 0 \pmod{l}$, nous avons

$$N(1-\zeta^s) = \prod_{k=1}^{l-1}(1-\zeta^{ks}) = \prod_{k=1}^{l-1}(1-\zeta^k) = 1.$$

Il en résulte que $1-\zeta, 1-\zeta^2, \ldots, 1-\zeta^{l-1}$ sont des nombres premiers de l'anneau $\mathfrak{D}$. En effet, si $1-\zeta^s = \alpha\beta$, alors $N(\alpha)N(\beta) = l$, d'où $N(a) = 1$ ou $N(\beta) = 1$, i. e. un des facteurs est une unité (théorème 4, § 2 du chapitre II). Passant aux normes dans l'égalité

$$1-\zeta^s = (1-\zeta)(1+\zeta+\ldots+\zeta^{s-1}) = (1-\zeta)\varepsilon_s, \qquad (7)$$

nous obtenons $N(\varepsilon_s) = 1$ et cela signifie que ε_s est une unité de l'ordre $\mathfrak{D}$. Ainsi tous les nombres $1-\zeta^s$ pour $s \not\equiv 0 \pmod{l}$ sont associés à $1-\zeta$. La décomposition (4) résulte maintenant de (5) et (7).

LEMME 2. — *Si un nombre entier rationnel a est divisible par* $1-\zeta$ (dans l'anneau $\mathfrak{D}$), *alors il est aussi divisible par 1.*

DÉMONSTRATION. — Soit $a = (1-\zeta)\alpha$ où $\alpha \in \mathfrak{D}$. Passant aux normes dans cette égalité, nous obtenons $a^{l-1} = lN(\alpha)$, où $N(\alpha)$ est un entier rationnel.

LEMME 3. — *Les seules racines de* 1 *dans le corps* $\mathbf{Q}(\zeta)$ *sont les racines* $(2l)^{\text{ième}}$ *de* 1.

DÉMONSTRATION. — Il est clair que les racines de 1 contenues dans $\mathbf{Q}(\zeta)$ appartiennent à l'ordre maximum. D'après le théorème 2, § 3 du chapitre II, elles forment un groupe cyclique fini; désignons par m l'ordre de ce groupe et par η une racine primitive de degré m de 1. Puisque $-\zeta$ appartient à $\mathbf{Q}(\zeta)$ et est aussi une racine de degré 21 de 1, alors m est divisible par 21. Nous démontrerons dans le § 2 du chapitre V (corollaire du théorème 1) que le degré du corps $\mathbf{Q}(\eta)$ sur Q est égal à $\varphi(m)$ où $\varphi(m)$ est la fonction arithmétique d'Euler. Posons

$$m = l^r m_0, \qquad (m_0, l) = 1 \qquad (r \geqslant 1, m_0 \geqslant 2).$$

Puisque $\mathbf{Q}(\eta)$ est contenu dans $\mathbf{Q}(\zeta)$ et que le degré de ce dernier corps est égal à $l-1$, alors

$$\varphi(m) = l^{r-1}(l-1)\varphi(m_0) \leqslant l-1.$$

Cette inégalité entraîne $r = 1$ et $\varphi(m_0) = 1$. Puisque les conditions $\varphi(m_0) = 1$ et $m_0 \geqslant 2$ entraînent $m_0 = 2$, alors $m = 21$, ce qui démontre le lemme 3.

LEMME 4 (lemme de Kummer). — ***Toute unité de l'anneau $\mathfrak{D}$ est le produit d'une puissance de ζ par une unité réelle.***

DÉMONSTRATION. — Soit

$$\varepsilon = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2} = r(\zeta) \qquad (a_i \in \mathbf{Z})$$

une unité quelconque de l'anneau $\mathfrak{D}$. Il est évident que le nombre complexe conjugué $\bar{\varepsilon} = r(\zeta^{-1}) = r(\zeta^{l-1})$ est aussi une unité de l'anneau $\mathfrak{D}$. Considérons l'unité $\mu = \frac{\varepsilon}{\bar{\varepsilon}} \in \mathfrak{D}$. D'après (6), les conjugués de μ s'écrivent

$$\sigma_k(\mu) = \frac{r(\zeta^k)}{r(\zeta^{(l-1)k})}\,\frac{r(\zeta^k)}{r(\zeta^{-k})}.$$

Puisque $r(\zeta^k)$ et $r(\zeta^{-k})$ sont complexes conjugués, alors $|\sigma_k(\mu)| = 1$ (pour tout $k = 1, \ldots, l-1$). D'après le théorème 2, § 3 du chapitre II, μ est une racine de 1 et par suite, d'après le lemme 3,

$$\mu = \pm \zeta^a.$$

Montrons qu'on a le signe + dans la partie droite de cette égalité; en effet, dans le cas contraire, nous aurions l'égalité

$$\varepsilon = -\zeta^a\bar{\varepsilon}.$$

Considérons dans l'anneau $\mathfrak{D}$ des congruences modulo $\lambda = 1 - \zeta$. Puisque $\zeta \equiv 1 \pmod{\lambda}$, toutes les puissances de λ sont congrues à 1 modulo λ et nous obtenons

$$\varepsilon \equiv \bar{\varepsilon} \equiv a_0 + a_1 + \ldots + a_{l-2} = M \pmod{\lambda};$$

cela signifie que $M \equiv -M \pmod{\lambda}$ ou $2M \equiv 0 \pmod{\lambda}$. D'après le lemme 2, il en résulte que

$$2M \equiv 0 \pmod{l}, \qquad M \equiv 0 \pmod{l}, \qquad M \equiv 0 \pmod{A},$$

d'où

$$\varepsilon \equiv 0 \pmod{A},$$

et cela contredit le fait que ε est une unité de l'anneau $\mathfrak{D}$. Ainsi

$$\varepsilon = \zeta^a\bar{\varepsilon}.$$

Choisissons maintenant un nombre entier s tel que $2s \equiv a \pmod{l}$. Alors $\zeta^a = \zeta^{2s}$ et l'égalité $\varepsilon = \zeta^{2s}\bar{\varepsilon}$ peut s'écrire sous la forme

$$\frac{\varepsilon}{\zeta^s} = \zeta^s\bar{\varepsilon} = \frac{\bar{\varepsilon}}{\zeta^{-s}} = \overline{\left(\frac{\varepsilon}{\zeta^s}\right)}.$$

L'égalité obtenue montre que l'unité $\eta = \frac{\varepsilon}{\zeta^s}$ est réelle. Ainsi ε est le produit de ζ^s par l'unité réelle η. C. Q. F. D.

LEMME 5. — *Soient x et y des nombres entiers rationnels. Pour que* $x + \zeta^m y$ *et* $x + \zeta^n y$ *soient premiers entre eux pout* $m \not\equiv n \pmod{l}$ (i. *e. que les unités soient leurs seuls diviseurs communs), il faut et il suffit que x et y soient premiers entre eux et que* $x + y$ *ne soit pas divisible par 1.*

DÉMONSTRATION. — Si x et y ont un diviseur commun $d > 1$, alors $x + \zeta^m y$ et $x + \zeta^n y$ sont divisibles par d. Si maintenant x + y est divisible par l, $x + \zeta^m y$ et $x + \zeta^n y$ ont pour diviseur commun $1 - \zeta$ (qui n'est pas une unité) ; en effet

$$x + \zeta^m y = x + y + (\zeta^m - 1)y = (x + y) - (1 - \zeta)\varepsilon_m y \equiv 0 \pmod{1 - \zeta}.$$

Ainsi, nous avons démontré la nécessité des deux conditions du lemme. Pour la suffisance, nous montrerons qu'il existe dans l'anneau $\mathfrak{D}$ des nombres ξ_0 et η_0 tels que

$$(x + \zeta^m y)\xi_0 + (x + \zeta^n y)\eta_0 = 1.$$

Considérons l'ensemble A de tous les nombres de la forme

$$(x + \zeta^m y)\xi + (x + \zeta^n y)\eta,$$

où ξ et η parcourent $\mathfrak{D}$ indépendamment l'un de l'autre. Il est évident que si α et β appartiennent à A, alors toute combinaison linéaire $\alpha\xi' + \beta\eta'$ à coefficients ξ' et η' dans $\mathfrak{D}$ appartient aussi à A. Nous voulons montrer que le nombre 1 appartient à A.

Des égalités

$$(x + \zeta^m y) - (x + \zeta^n y) = \zeta^m(1 - \zeta^{n-m})y = \zeta^m\varepsilon_{n-m}(1 - \zeta)y,$$

$$(x + \zeta^m y)\zeta^n - (x + \zeta^n y)\zeta^m = -\zeta^m(1 - \zeta^{n-m})x = -\zeta^m\varepsilon_{n-m}(1 - \zeta)x,$$

il résulte que $(1 - \zeta)y \in$ A et $(1 - \zeta)x \in$ A (puisque $\zeta^m\varepsilon_{n-m}$ est une unité de l'anneau $\mathfrak{D}$). Puisque x et y sont premiers entre eux, il existe des entiers rationnels a et b tels que $ax + by = 1$. Ainsi,

$$(1 - \zeta)xa + (1 - \zeta)yb = 1 - \zeta \in \mathrm{A}.$$

De plus,

$$x + y = (x + \zeta^m y) + (1 - \zeta^m)y = (x + \zeta^m y) + (1 - \zeta)\varepsilon_m y$$

et par suite x + y ∈ A. Puisque l est divisible par $1 - \zeta$, alors $l \in$ A. D'après la seconde hypothèse du lemme, les nombres x + y et l sont premiers entre eux et par suite il existe des entiers rationnels u et v tels que $(x+y)u+lv = 1$, d'où $1 \in$ A. Ceci termine la démonstration du lemme 5.

3) Le théorème de Fermat dans le cas d'unicité de la décomposition en facteurs premiers

THÉORÈME 1. — *Soient l un nombre premier impair et ζ une racine primitive d'ordre l de* 1. *Si dans l'ordre $\mathfrak{D} = \mathbf{Z}[\zeta] = \{1, \zeta, \ldots, \zeta^{l-2}\}$ du corps $\mathbf{Q}(\zeta)$, la décomposition en facteurs premiers est unique, alors le premier cas du théorème de Fermat est résolu,* i. *e. l'équation*

$$x^l + y^l = z^l$$

n'a pas de solution en nombres entiers rationnels x, y, z non divisibles par 1.

DÉMONSTRATION. — Le nombre premier 3 jouera un rôle particulier dans la démonstration, c'est pourquoi nous considérerons séparément le cas $l = 3$. Montrons que non seulement l'équation $x^3 + y^3 = z^3$ mais même la congruence $x^3 + y^3 \equiv z^3 \pmod 9$ n'a pas de solutions parmi les nombres non divisibles par 3. En effet, supposons que cette dernière congruence soit possible. De la congruence $x^3 + y^3 \equiv z^3 \pmod 3$ il résulte (d'après le petit thtorème de Fermat) que $x + y \equiv z \pmod 3$, i. e. $z = x + y + 3u$, d'où

$$x^3 + y^3 \equiv (x + y + 3u)^3 \equiv x^3 + y^3 + 3x^2y + 3xy^2 \pmod 9;$$

par suite

$$0 \equiv x^2y + xy^2 = xy(x + y) \equiv xyz \pmod 3.$$

Ainsi, un des nombres x, y, z est divisible par 3, ce qui démontre notre affirmation.

Soit maintenant $l \geqslant 5$. Raisonnant par l'absurde, supposons que pour certains entiers rationnels x, y, z premiers deux à deux et non divisibles par l on ait l'égalité $x^l + y^l = z^l$, que nous avons aussi écrite sous la forme (2). Puisque $x + y \equiv x^l + y^l \equiv z \not\equiv 0 \pmod l$ et x et y premiers entre eux, alors, d'après le lemme 5, les nombres $x + \zeta^k y$ ($k = 0, 1, \ldots, l-1$) sont premiers entre eux deux à deux. Comme on l'a déjà vu dans 1), l'unicité de la décomposition en facteurs premiers entraîne

$$x + \zeta y = \mathrm{E}\mathfrak{d}^l \tag{3}$$

$$x - \zeta z = \varepsilon_1 \alpha_1^{l'}, \tag{3'}$$

où ε et ε_1 sont des unités de l'anneau $\mathfrak{D}$. Nous avons déjà indiqué que la réunion des égalités (3) et (3') conduit à une contradiction. Montrons que les congruences correspondantes modulo l dans l'anneau $\mathfrak{D}$ sont contradictoires.

Soit a = a, + $a_1\xi$ + . . . + $a_{l-2}\zeta^{l-2}$ (a_0, a_1, . . . , a_{l-2} entiers rationnels). Alors

$$a' \equiv a_0^l + a_1^l\zeta^l + \ldots + a_{l-2}^l\zeta^{l(l-2)} \equiv \mathrm{M} \pmod{l},$$

avec M = a_0 + a_1 + . . . + a_{l-2}. D'après le lemme de Kummer, l'unité ε peut s'écrire $\varepsilon = \zeta^s\eta$ où η est une unité réelle. Par suite, d'après l'égalité **(3),** on a la congruence

$$x + \zeta y = \zeta^s\eta\mathrm{M} = \zeta^s\xi \pmod{l},$$

où ξ est un nombre réel appartenant à $\mathfrak{D}$. Nous pouvons écrire cette congruence sous la forme

$$\zeta^{-s}(x + \zeta y) = \xi \pmod{l}. \tag{8}$$

Remarquons maintenant que pour tout $a \in \mathfrak{D}$, le nombre complexe conjugué $\bar{\alpha}$ appartient aussi à $\mathfrak{D}$. Si nous avons la congruence $\alpha \equiv \beta \pmod{l}$, alors $\alpha - \beta = l\gamma$ d'où $\bar{\alpha} - \bar{\beta} = l\bar{\gamma}$ et par suite $\bar{\alpha} \equiv \bar{\beta} \pmod 1$. Passant aux nombres complexes conjugués dans la congruence (8), nous obtenons

$$\zeta^s(x + \zeta^{-1}y) \equiv \bar{\xi} \pmod 1. \tag{9}$$

Mais $\bar{\xi} = \xi$ et il résulte de (8) et (9) que

$$\zeta^{-s}(x + \zeta y) \equiv \zeta^s(x + \zeta^{-1}y) \pmod{l}$$

ou encore

$$x\zeta^s + y\zeta^{s-1} - x\zeta^{-s} - y\zeta^{1-s} \equiv 0 \pmod{l}. \tag{10}$$

Il est clair qu'un nombre de $\mathfrak{D}$ représenté sous la forme canonique

$$a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$$

est divisible par l si et seulement si tous les coefficients a,, . . ., a_{l-2} sont divisibles par l. Si les exposants

$$s,\ s-1,\ -s,\ 1 - s \tag{11}$$

ne sont pas congrus deux à deux ni congrus avec $l - 1$ modulo l, alors le nombre qui figure dans la partie gauche de la congruence (10) est écrit sous forme canonique et par suite tous les coefficients sont divisibles par 1. Ainsi, dans ce cas, x $\equiv$ 0 (mod l) et y $\equiv$ 0 (mod l) ce qui est impossible puisque x et y sont premiers entre eux (et non divisibles par l).

Considérons maintenant les cas où la partie gauche de (10) n'est pas sous

forme canonique, i. e. si l'un des nombres (11) est congru à $l-1$ ou si deux d'entre eux sont congrus modulo 1. Un des exposants (11) sera congru à $l-1$ modulo l seulement pour les valeurs suivantes de ces exposants.

s	s - l	$-s$	l - s
$l-1$	1 - 2	1	2
0	$l-1$	0	1
1	0	$l-1$	0
2	1	1 - 2	$l-1$

Nous voyons que, dans chacun de ces cas, il existe seulement un exposant congru à $l-1$ (puisque $l \geqslant 5$). Pour écrire la partie gauche de (10) sous forme canonique, il faut utiliser l'égalité

$$\zeta^{l-1} = -1 - \zeta - \cdots - \zeta^{l-2}$$

Substituant cette expression dans le terme de la partie gauche de (10) dont l'exposant est congru à $l-1$ modulo l, nous obtenons pour ce terme une somme de monômes affectes des coefficients $\pm$ x ou $\pm$ y. Puisque le nombre de ces monômes est égal à $l-1 \geqslant 4$ (puisque $l \geqslant 5$), alors, par réduction des termes semblables, au moins un d'entre eux ne se réduit pas avec les termes restants de la congruence (10). Mais alors la congruence (10) dont nous venons d'écrire la partie gauche sous forme canonique entraîne

$$\pm x \equiv 0 \pmod{l} \qquad \text{ou} \qquad \pm y \equiv 0 \pmod{l}.$$

Nous avons obtenu une contradiction puisque par hypothèse x et y ne sont pas divisibles par 1.

Il reste à considérer le cas où certains des exposants (11) sont congrus modulo 1. Les congruences $s \equiv s-1 \pmod{l}$ et $-s \equiv 1-s \pmod{l}$ sont impossibles. Si $s \equiv -s \pmod{l}$ ou $s-1 \equiv 1-s \pmod{l}$, alors nous aurons respectivement $s \equiv 0 \pmod{l}$ et $s \equiv 1 \pmod{l}$, ce qui correspond aux cas $s-1 \equiv 1-1 \pmod{1}$ et $-s \equiv l-1 \pmod{l}$. Les deux cas restants $s \equiv 1-s \pmod{l}$ et $s-1 \equiv -s \pmod{l}$ entraînent $s \equiv \frac{l+1}{2} \pmod{l}$. Dans ce cas, la congruence (10) s'écrit

$$(x-y)\zeta^{\frac{l+1}{2}} + (y-x)\zeta^{\frac{l-1}{2}} \equiv 0 \pmod{l}$$

Puisque la partie gauche de cette congruence est écrite sous forme canonique (les exposants $\frac{l+1}{2}$ et $\frac{l-1}{2}$ ne sont pas congrus entre eux ni congrus à $l-1$), alors

$$x \equiv y \pmod{l}.$$

De manière analogue, il résulte de (3') que

$$x \equiv -z \pmod{l}$$

De la congruence

$$x + y \equiv x^l + y^l \equiv z^l \equiv z \pmod{l}$$

il résulte maintenant que $2x \equiv -x \pmod{l}$ ou $3x \equiv 0 \pmod{l}$. Puisque $l \neq 3$, alors $x \equiv 0 \pmod{l}$ et nous avons obtenu de nouveau une contradiction. Ceci termine la **démonstration** du théorème 1.

En utilisant des propriétés plus fines des nombres entiers du corps $\mathbf{Q}(\zeta)$, Kummer a démontré que si le nombre premier l satisfait aux hypothèses du théorème 1, alors le second cas du théorème de **Fermat** est vrai pour l'exposant 1.

La généralisation du théorème 1 à une classe plus large d'exposants l sera étudiée dans le § 7-3) de ce chapitre. Nous démontrerons le second cas du théorème de **Fermat** pour ces exposants au § 7-l) du chapitre V.

Ajoutons quelques remarques.

Remarque 1. — La partie fondamentale de la démonstration du théorème 1 est la démonstration de l'impossibilité de certaines congruences modulo l. Bien sûr, cela ne démontre pas que l'équation $x^l + y^l \equiv z^l \pmod{l}$ n'a pas de solution. Puisque cette congruence équivaut à $x + y \equiv z \pmod{l}$, elle a toujours une solution en nombres non divisibles par 1. On peut montrer de plus, pour $l = 7$ par exemple, que l'équation $x^7 + y^7 = z^7$ considérée comme congruencc modulo un nombre quelconque a toujours une solution en nombres entiers non divisibles par 7.

Ainsi la démonstration de l'impossibilité de l'équation (1) repose sur sa réduction aux équations (3) et (3') qui utilise l'unicité de la décomposition en facteurs dans l'anneau $\mathbf{Z}[\zeta]$, puis ensuite sur l'application de la théorie des congruences aux équations obtenues.

Remarque 2. — La méthode employée dans ce paragraphe pour étudier le théorème de **Fermat** s'applique aussi à d'autres problèmes analogues (cf. exercice 2).

Remarque 3. — Si nous voulons appliquer le théorème ci-dessus à des cas concrets, il faut savoir dans quels cas il y a unicité de la décomposition en facteurs dans l'anneau $\mathbf{Q}(\zeta)$.

En liaison avec ce qui précède, nous sommes donc conduits aux deux problèmes fondamentaux suivants de la théorie des nombres algébriques :

1° Dans quels corps K de nombres algébriques la décomposition des nombres entiers en facteurs premiers est-elle unique ?

2° Quelle est la structure arithmétique des corps K dans lesquels il n'y a pas unicité de la décomposition des nombres entiers en facteurs premiers ?

EXERCICES

1. Démontrer que la congruence $x^5 + y^5 \equiv z^5 \pmod{5^2}$ n'a pas de solution en nombres entiers rationnels x, y, z non divisibles par 5.

2. Soit ω une racine primitive d'ordre 3 de 1. Supposant connu le fait que la décomposition des nombres entiers en facteurs premiers dans le corps $\mathbf{Q}(\omega)$ est unique, démontrer que l'équation $x^3 + y^3 = 5z^3$ n'a pas de solutions en nombres entiers rationnels x, y, z non divisibles par 3.

3. Soient l un nombre premier, ζ une racine primitive $l^{\text{ième}}$ de 1, x et y des nombres entiers rationnels et d le plus grand commun diviseur de x et y. Posons $\delta = d$ si $x + y \not\equiv 0 \pmod{l}$ et $\delta = d(1 - \zeta)$ si $x + y \equiv 0 \pmod{l}$. Démontrer que δ est un diviseur commun des nombres $x + \zeta^m y$ et $x + \zeta^n y$ $(m \not\equiv n \pmod{l})$ et est divisible par tout autre diviseur commun de ces nombres.

4. Démontrer qu'un produit $\alpha\beta$ est divisible par $1 - \zeta$ dans l'ordre $\{1, \zeta, \ldots, \zeta^{l-2}\}$ du corps $\mathbf{Q}(\zeta)$ si et seulement si l'un au moins des facteurs α ou β est divisible par $1 - \zeta$.

5. Utilisant la notion de congruence de polynômes à coefficients entiers (chap. 1, § l-l)), montrer que

$$t^{l-1} + \ldots + t + 1 \equiv (t-1)^{l-1} \pmod{l}.$$

6. Démontrer que le polynôme $t^{l-1} + \ldots + t + 1$ est irréductible sur le corps des nombres rationnels, en considérant des congruences de polynômes (à coefficients entiers) modulo l^2.

§ 2. — DÉCOMPOSITION EN FACTEURS

1) Facteurs premiers

Dans le paragraphe précédent nous avons vu l'importance de la décomposition en facteurs premiers dans les ordres des corps de nombres algébriques; nous donnerons ultérieurement d'autres applications de cette notion. Étudions la décomposition en facteurs premiers dans le cas général.

Pour parler de décomposition en facteurs premiers, il faut préciser l'anneau $\mathfrak{D}$ dont nous étudierons les éléments. Nous commencerons par poser le problème sous forme générale dans un anneau commutatif unitaire sans diviseurs de zéro. Ces conditions seront supposées satisfaites dans la suite, sauf hypothèses complémentaires.

DÉFINITION. — ***Un élément $\pi \neq 0$ d'un anneau $\mathfrak{D}$ qui n'est pas une unité est dit premier s'il n'est pas décomposable en facteurs, $\pi = \alpha\beta$, dont aucun des deux n'est une unité dans $\mathfrak{D}$.***

Ainsi un nombre est premier s'il est divisible seulement par les unités et par les éléments qui lui sont associés.

Il n'existe pas d'élément premier dans tout anneau et les éléments d'un anneau ne sont pas toujours représentables comme produit d'éléments premiers. Considérons par exemple l'anneau $\mathfrak{D}$ de tous les nombres entiers algébriques. Pour tout $\alpha \neq 0$ de $\mathfrak{D}$ qui n'est pas une unité, nous avons la décomposition $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ où $\sqrt{\alpha}$ appartient à $\mathfrak{D}$ et n'est pas une unité. Ainsi aucun élément de $\mathfrak{D}$ n'est premier.

Comme exemple d'anneaux dans lesquels la décomposition est possible, on peut considérer les ordres dans les corps de nombres algébriques. Les éléments premiers d'un ordre seront aussi appelés nombres premiers.

THÉORÈME 1. — ***Dans un ordre quelconque $\mathfrak{D}$ d'un corps K de nombres algébriques, tout nombre non nul qui n'est pas une unité est représentable comme produit de nombres premiers.***

DÉMONSTRATION. — D'après le théorème du § 2, chapitre II, les unités ε de l'anneau $\mathfrak{D}$ sont caractérisées par le fait que leurs normes N(E) sont égales à ± 1. Nous démontrerons ce théorème par récurrence sur le nombre $|\,N(a)\,|$, $a \in \mathfrak{D}$. Si le nombre α est premier, alors c'est terminé. Si $\alpha = \beta\gamma$ où β et y sont des nombres de $\mathfrak{D}$ qui ne sont pas des unités, alors

$$1 < |\,N(\beta)\,| < |\,N(\alpha)\,|, \qquad 1 < |\,N(\gamma)\,| < |\,N(\alpha)\,|.$$

Par hypothèse de récurrence, β et y sont des produits de nombres preOiers de l'anneau $\mathfrak{D}$. Mais alors, d'après l'égalité $a = \beta\gamma$, le nombre a est aussi produit de nombres premiers. Le théorème 1 est démontré.

2) Unicité de la décomposition.

Supposant maintenant que dans l'anneau $\mathfrak{D}$ la décomposition en facteurs premiers est possible, étudions l'unicité éventuelle de cette décomposition (à des éléments associés près).

DÉFINITION. — *Nous dirons que dans l'anneau $\mathfrak{D}$ la décomposition en facteurs premiers est définie de manière unique si pour deux décompositions*

$$a = \pi_1, \ldots, \pi_r, \qquad \alpha = \pi'_1 \ldots \pi'_s$$

le nombre des facteurs est le même ($r = s$) et si, pour une énumération convenable, les éléments π_i et π'_i sont deux à deux associés.

Dans la décomposition $\alpha = \pi_1, \ldots, \pi_s$ on peut regrouper les nombres premiers associés en les multipliant par une unité. Nous obtenons ainsi une décomposition de la forme

$$\alpha = \varepsilon\pi_1^{k_1} \ldots \pi_m^{k_m}$$

où les nombres $\pi_1, \ldots, \pi_m$ sont deux à deux non associés et où ε est une unité de l'anneau $\mathfrak{D}$. Si la décomposition en facteurs premiers est unique, les éléments $\pi_1, \ldots, \pi_m$ sonr définis à une unité près et les exposants $k_1, \ldots, k_m$ sont définis de manière unique.

L'exemple le plus classique d'anneau dans lequel la décomposition en facteurs est définie de manière unique est l'anneau des nombres entiers rationnels. Dans le cas général, il n'y a pas unicité de la décomposition dans tous les anneaux où la décomposition en facteurs premiers est possible. Ainsi, le résultat de l'exercice 1 montre que parmi tous les ordres des corps de nombres algébriques, on peut seulement espérer l'unicité de la décomposition dans les ordres maxima.

L'unicité de la décomposition en facteurs premiers dans l'anneau $\mathbf{Z}$ de tous les entiers rationnels résulte du théorème de la division avec reste qui affirme que pour tous les entiers a et b non nuls de $\mathbf{Z}$, il existe des entiers q et r tels que $a = bq + r$ et $|r| < |b|$. Par suite, si dans un anneau $\mathfrak{D}$ on a un analogue de cette division avec reste, on pourra démontrer dans $\mathfrak{D}$ l'unicité de la décomposition en facteurs premiers.

DÉFINITION. — *On dira qu'il existe dans l'anneau $\mathfrak{D}$ un algorithme de division avec reste si on a défini une fonction $\|\alpha\|$ pour les nombres $a \neq 0$ de $\mathfrak{D}$, à valeurs entières positives, satisfaisant aux conditions suivantes :*

1° *Si $a \neq 0$ est divisible par β, alors $\|a\| \geqslant \|\beta\|$.*

2° *Pour des éléments α et β non nuls de $\mathfrak{D}$, il existe γ et ρ tels que $\alpha = \beta\gamma + \rho$ avec $\rho = 0$ ou bien $\|\rho\| < \|\beta\|$.*

L'anneau $\mathfrak{D}$ et alors appelé un anneau euclidien.

Reprenons la démonstration de l'unicité de la décomposition des nombres entiers rationnels en facteurs premiers et de la décomposition des polynômes en facteurs irréductibles. En dehors des propriétés générales des anneaux, on utilise seulement le théorème de la division avec reste. Transcrivant textuellement ces démonstrations, nous obtenons le résultat suivant.

THÉORÈME 2. — *Dans tout anneau euclidien la décomposition des éléments en facteurs premiers est possible et définie de manière unique.*

Considérons comme exemple l'ordre maximum $\mathfrak{D}$ du corps quadratique $\mathbf{Q}(\sqrt{-1})$ et montrons qu'il existe dans $\mathfrak{D}$ un algorithme de division avec reste pour la fonction $\|a\| = N(\alpha)$. Soient a et $\beta \neq 0$ des nombres quelconques de $\mathfrak{D}$. Pour les nombres rationnels u et v définis par l'égalité

$$\frac{\alpha}{\beta} = u + v\sqrt{-1},$$

Choisissons les nombres entiers rationnels x et y les plus proches :

$$|u-x| \leqslant \frac{1}{2}, \qquad |v-y| \leqslant \frac{1}{2}.$$

Si nous posons maintenant $y = x + y\sqrt{-1}$, $p = a - \beta\gamma$, alors d'après l'inégalité

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = (u-x)^2 + (v-y)^2 \leqslant \frac{1}{4} + \frac{1}{4} < 1,$$

nous aurons

$$N_{(\rho)} = N\left(\frac{\alpha}{\beta} - \gamma\right) N(\beta) < N(\beta)$$

ce qui démontre le résultat.

D'après le théorème 2, nous obtenons donc que dans l'ordre maximum du corps $\mathbf{Q}(\sqrt{-1})$, la décomposition en facteurs premiers est définie de manière unique.

On peut ainsi démontrer l'unicité de la décomposition pour une série d'autres anneaux (cf. exercices 3, 4 et 7). Remarquons aussi qu'il existe des anneaux non euclidiens dans lesquels la décomposition en facteurs premiers est cependant définie de manière unique. L'exemple le plus simple d'un tel anneau est l'ordre maximum du corps $\mathbf{Q}(\sqrt{-19})$. L'absence dans cet anneau d'un algorithme de division avec reste résulte de l'exercice 6. L'unicité de la décomposition en facteurs premiers dans cet anneau résulte de l'exercice 11 du § 7 de ce chapitre.

On peut définir un algorithme de division avec reste pour la norme dans l'ordre maximum des corps $\mathbf{Q}(\sqrt{d})$ pour et seulement pour les valeurs suivantes de *d* :

2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.

3) Exemple de non-unicité de la décomposition

Il est facile de construire des contre-exemples montrant que la décomposition en facteurs premiers n'est pas nécessairement unique. Considérons par exemple le corps $\mathbf{Q}(\sqrt{-5})$. Comme on l'a montré dans le § 7-2) du chapitre II, les nombres de l'ordre maximum de ce corps s'écrivent

$$\alpha = x + y\sqrt{-5}$$

pour des entiers rationnels x et y et par suite N(a) = $x^2 + 5y^2$. Le nombre 21 admet dans l'anneau $\mathfrak{D}$ les deux décompositions

$$21 = 3.7 \tag{1}$$

$$21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}). \tag{2}$$

Montrons que tous les facteurs de droite sont premiers dans l'anneau $\mathfrak{D}$. En effet, si par exemple $3 = \alpha\beta$ où ni a ni β n'est une unité, alors l'égalité

$$9 = N(\alpha\beta) = N(\alpha)N(\beta)$$

entraînerait N(a) = 3. Pourtant, cela est impossible car l'égalité $x^2 + 5y^2 = 3$ est impossible en nombres entiers rationnels x et y. On montre aussi que les nombres $7,1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ sont premiers. Puisque les quotients

$$\frac{1 \pm 2\sqrt{-5}}{3} \qquad \text{et} \qquad \frac{1 \pm 2\sqrt{-5}}{7}$$

n'appartiennent pas à l'anneau $\mathfrak{D}$, alors les nombres 3 et 7 ne sont pas associés à $1 + 2\sqrt{-5}$ et $1 - 2\sqrt{-5}$. Ainsi il existe dans $\mathfrak{D}$ des nombres qui admettent plusieurs décompositions distinctes en facteurs premiers (cf. exercices 10 et 11 pour d'autres exemples).

On pourrait penser que le phénomène de non-unicité de la décomposition en facteurs premiers rend impossible toute théorie arithmétique fructueuse dans un tel anneau mais il n'en est pas ainsi. Au milieu du siècle dernier, Kummer a montré que bien que l'arithmétique d'un tel corps se distingue radicalement de celle du corps des rationnels, elle peut donner d'importants résultats en théorie des nombres.

L'idée fondamentale de Kummer est essentiellement la suivante : si dans l'ordre maximum $\mathfrak{D}$ d'un certain corps de nombres algébriques, la décomposition en facteurs premiers n'est pas définie de manière unique, alors on peut représenter les nombres $\neq 0$ de $\mathfrak{D}$ comme objets d'un nouvel ensemble muni d'une multiplication et dans lequel la décomposition en facteurs premiers est cette fois définie de manière unique.

Pour tout nombre $a \neq 0$ de $\mathfrak{D}$, son image (a) dans cette représentation sera décomposable de manière unique en facteurs premiers, mais ces facteurs premiers n'appartiendront pas à notre anneau mais à un nouvel ensemble. L'unicité de la décomposition au sens de Kummer devra tenir compte du fait que certains nombres premiers de $\mathfrak{D}$ (et peut-être tous) ont pour images des éléments non premiers du nouvel ensemble, i. e. leurs images admettent des décompositions non triviales. Ainsi, dans l'exemple de l'ordre maximum du corps $\mathbf{Q}(\sqrt{-5})$, pour obtenir l'unicité de la décom-

position à partir des décompositions (1) et (2), il doit exister des objets $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_4$ tels que

$$3 = \mathfrak{p}_1\mathfrak{p}_2, \quad 7 = \mathfrak{p}_3\mathfrak{p}_4, \quad 1 + 2\sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3, \quad 1 - 2\sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4$$

(dans ces égalités, nous n'avons pas distingué les nombres de leurs images). Les décompositions (1) et (2) s'écrivent maintenant

$$21 = \mathfrak{p}_1\mathfrak{p}_2 . \mathfrak{p}_3\mathfrak{p}_4 = \mathfrak{p}_1\mathfrak{p}_3 . \mathfrak{p}_2\mathfrak{p}_4$$

qui diffèrent seulement par l'ordre des facteurs.

Kummer a appelé ces nouveaux objets nombres idéaux. Ils sont appelés maintenant diviseurs. Les paragraphes suivants sont consacrés à l'étude systématique de ces diviseurs.

EXERCICES

1. Démontrer que si dans un certain ordre $\mathfrak{D}$ d'un corps K de nombres algébriques la décomposition en facteurs premiers est définie de manière unique, alors cet ordre est l'ordre maximum. Plus généralement, montrer que si dans un anneau $\mathfrak{D}$ la décomposition en facteurs premiers existe et est définie de manière unique, alors l'anneau $\mathfrak{D}$ est intégralement clos.

2. Démontrer que si dans un anneau euclidien un élément $\alpha \neq 0$ est divisible par β et n'est pas associé à β, alors $\| \alpha \| > \| \beta \|$.

3. Soit m un lattice du plan complexe dont les points représentent les nombres de l'ordre maximum $\mathfrak{D}$ d'un corps quadratique imaginaire. Démontrer qu'il existe dans $\mathfrak{D}$ un algorithme de division avec reste pour la norme $N(\alpha)$ si et seulement si les translatés du disque unité (sans sa frontière) par les vecteurs du lattice m recouvrent tout le plan.

4. Montrer qu'il existe un algorithme de division avec reste pour la norme dans l'ordre maximum du corps $\mathbf{Q}(\sqrt{d})$ avec $d < 0$, si et seulement si d est égal à l'un des nombres :

$$-1, -2, -3, -7, -11.$$

5. Démontrer que, dans le corps quadratique imaginaire $\mathbf{Q}(\sqrt{d})$ où $d < 0$ est sans carrés et différent de -1, -2, -3, -7, -11, la norme de tout élément entier est égale à 0, ± 1 ou est plus grande que 3.

6. Démontrer qu'en dehors des cinq corps considérés dans l'exercice 4, pour aucun autre corps quadratique imaginaire l'ordre maximum n'est un anneau euclidien.

Indication. — Raisonner par l'absurde en supposant qu'il existe une fonction $\| a \|$ définie pour $a \in \mathfrak{D}$ qui satisfait aux conditions de la définition du point 2). Parmi les nombres de l'anneau $\mathfrak{D}$ qui ne sont pas des unités, soit y un nombre pour lequel $\| y \|$ soit minimum. Montrer qu'alors tout $\alpha \in \mathfrak{D}$ est congru modulo y à l'un des trois nombres 0, -1 ou 1.

7. Démontrer l'existence d'un algorithme de division avec reste pour l'ordre maximum du corps $\mathbf{Q}(\sqrt{2})$.

8. Démontrer que dans l'ordre maximum du corps $\mathbf{Q}(\sqrt{-1})$ tout nombre premier rationnel impair p est premier s'il est de la forme $4k + 3$ et se décompose en un produit $p = \pi\pi'$ de deux facteurs premiers non associés s'il est de la forme $4k + 1$. Trouver la décomposition du nombre 2 en facteurs premiers dans cet anneau.

9. Soit $\mathfrak{D}$ un anneau dans lequel la décomposition en facteurs premiers est définie de manière unique. Démontrer que pour tout couple a, β d'éléments de $\mathfrak{D}$ (non nuls simultanément) il existe un diviseur commun δ qui est divisible par tout autre diviseur commun de a et β (δ est appelé le plus grand commun diviseur de a et β).

10. Démontrer que dans l'ordre maximum du corps $\mathbf{Q}(\sqrt{-6})$ on a les décompositions distinctes suivantes en facteurs premiers :

$$55 = 5.11 = (7 + \sqrt{-6})(7 - \sqrt{-6}),$$
$$6 = 2.3 = -(\sqrt{-6})^2.$$

11. Vérifier que dans l'ordre maximum du corps $\mathbf{Q}(\sqrt{-23})$ on a les décompositions en facteurs premiers

$$6 = 2.3 = \frac{1 + \sqrt{-23}}{2} \cdot \frac{1 - \sqrt{-23}}{2},$$
$$27 = 3.3.3 = (2 + \sqrt{-23})(2 - \sqrt{-23}).$$

Trouver les différentes décompositions du nombre 8 en facteurs premiers dans cet anneau.

§ 3. — DIVISEURS

1) Définition axiomatique des diviseurs

Soit $\mathfrak{D}$ un anneau commutatif quelconque (avec unité et sans diviseurs de zéro); donnons un sens précis aux considérations de la fin du § 2-2).

Notre théorie comporte deux parties : construire un nouvel ensemble A dans lequel la décomposition en facteurs premiers soit définie de manière unique et comparer les éléments non nuls de l'anneau $\mathfrak{D}$ aux éléments de l'ensemble A. Commençons par la première partie. Pour pouvoir parler de décomposition en facteurs dans A, il faut définir une opération de multiplication faisant correspondre à tout couple d'éléments de A un troisième élément qui soit leur produit. Nous imposerons à cette opération d'être associative et commutative. Un ensemble muni d'une telle opération est appelé un ***monoïde commutatif.*** Nous imposerons également l'existence d'un élément unité dans A, i. e. d'un élément e tel que e. a = a pour tout $a \in A$.

Dans tout monoïde commutatif A avec unité, on peut parler de divisibilité : un élément $a \in A$ est divisible par $b \in A$ s'il existe un élément $c \in A$ tel que a = bc (on dit aussi que b est un diviseur de a ou que a est un multiple de b). Un élément $p \in A$, différent de e, est dit ***premier*** s'il est divisible seu-

lement par lui-même et par l'unité e. On dit de plus qu'on a ***unicité de la décomposition en facteurs premiers dans le monoïde*** A si tout élément $a \in A$ se représente comme un produit d'éléments premiers

$$a = p_1 p_2 \dots p_r \qquad (r \geqslant 0),$$

une telle décomposition étant unique, à l'ordre près des facteurs (pour $r = 0$, le produit est, par définition, égal à l'unité e). L'unicité de la décomposition suppose en particulier que l'unité e est le seul élément inversible (i. e. diviseur de e). Il est clair qu'un monoïde avec unicité de la décomposition en facteurs premiers est complètement défini par l'ensemble de ses éléments premiers (et de leurs puissances). L'exemple le plus simple d'un tel monoïde est l'ensemble des entiers naturels.

Dans un monoïde A où la décomposition en facteurs premiers est définie de manière unique, tout couple d'éléments admet un plus grand commun diviseur (i. e. un diviseur commun divisible par tout autre diviseur commun) et un plus petit commun multiple. Deux éléments de A sont dits premiers entre eux si leur plus grand commun diviseur est égal à e. Remarquons les propriétés élémentaires suivantes de la divisibilité dans A : si un produit ab est divisible par c et a et c premiers entre eux, alors b est divisible par c; si c est divisible par des éléments a et b premiers entre eux, alors c est divisible par le produit ab; si un produit ab est divisible par un Clément premier p, alors au moins un des facteurs est divisible par p.

Précisons maintenant la seconde partie de notre théorie.

Désignons par $\mathfrak{D}^*$ l'ensemble de tous les éléments non nuls de l'anneau $\mathfrak{D}$. Puisque, par hypothèse, l'anneau $\mathfrak{D}$ est sans diviseurs de zéro, alors l'ensemble $\mathfrak{D}^*$ est un monoïde pour l'opération de multiplication.

Supposons définie une application du monoïde $\mathfrak{D}^*$ dans un monoïde A dans lequel la décomposition en facteurs premiers est définie de manière unique; nous désignerons par (a) l'image de l'élément $a \in \mathfrak{D}^*$ par cette application. Il est clair que l'étude de la structure multiplicative de l'anneau $\mathfrak{D}$ à l'aide du monoïde A n'est possible que si l'application $\alpha \to (\alpha)$ est multiplicative, i. e. $(\alpha\beta) = (\alpha)(\beta)$ pour tous $\alpha, \beta \in A$. Nous imposerons donc à l'application $a \to (a)$ d'être un homomorphisme du monoïde $\mathfrak{D}^*$ dans le monoïde A. La divisibilité de a par β dans l'anneau $\mathfrak{D}$ entraîne alors que (a) est divisible par (β) dans le monoïde A. Pour que la relation de divisibilité dans $\mathfrak{D}$ corresponde exactement à la divisibilité dans A, il est nécessaire d'exiger que, réciproquement, la divisibilité de (a) par (β) dans le monoïde A entraîne que a est divisible par β dans $\mathfrak{D}$.

Nous dirons dans la suite qu'un élément $a \neq 0$ de $\mathfrak{D}$ est divisible par un élément $\alpha \in A$ et nous écrirons $a|\alpha$ si (a) est divisible par α dans le monoïde A. On considérera que 0 est divisible par tous les éléments de A.

L'ensemble de tous les éléments de l'anneau $\mathfrak{D}$ qui sont divisibles par un élément $\alpha \in \mathfrak{D}^*$ est fermé pour les opérations d'addition et de soustraction. Nous devrons exiger, bien entendu, que cette propriété soit conservée pour les diviseurs a du monoïde A.

Enfin, nous imposerons à A de ne pas contenir d'éléments « superflus », en signifiant par là que deux éléments distincts de A doivent différer l'un de l'autre par leurs propriétés de divisibilité par rapport aux éléments de $\mathfrak{D}$.

Tout ce qui précède nous conduit à la définition suivante.

DÉFINITION. — ***Par theorie*** des ***diviseurs d'un anneau*** $\mathfrak{D}$ ***on entend la construction d'un certain monoïde*** A, ***dans lequel la décomposition en facteurs premiers est définie de manière unique et d'un homomorphisme*** $a \to (a)$ ***du monoïde*** $\mathfrak{D}^*$ ***dans le monoïde*** A, ***tels que***

1° ***dans l'anneau*** $\mathfrak{D}$, ***un élément*** $a \in \mathfrak{D}^*$ ***est divisible par*** $\beta \in \mathfrak{D}^*$ ***si et seulement si*** (a) ***est divisible par*** (β) ***dans le monoïde*** A;

2° ***si*** $a, \beta \in \mathfrak{D}$ ***sont divisibles par un élément*** $a \in$ A, ***alors*** $a \pm \beta$ ***sont aussi divisibles par*** a;

3° ***soient*** a ***et*** $\mathfrak{b}$ ***deux éléments de*** A; ***si les ensembles de tous les éléments de*** $\mathfrak{D}$ ***qui sont divisibles respectivement par*** a ***et*** $\mathfrak{b}$ ***coïncident, alors*** $a = \mathfrak{b}$.

Les éléments du monoïde A sont appelés des ***diviseurs*** de l'anneau $\mathfrak{D}$ et les diviseurs de la forme (a), $a \in \mathfrak{D}^*$, sont appelés des ***diviseurs principaux.*** L'élément unité e du monoïde A est appelé le ***diviseur unité.***

La première condition de la définition ci-dessus entraîne le résultat suivant:

L'égalité $(a) = (\beta)$ ***a lieu si et seulement si*** a ***et*** β ***sont associés dans l'anneau*** $\mathfrak{D}$. ***En particulier, les unités*** ε ***de l'anneau*** $\mathfrak{D}$ ***sont caractérisées par l'égalité*** $(\varepsilon) = e$.

Dans la suite, nous désignerons par $\mathfrak{D}^* \to$ A une théorie des diviseurs pour l'anneau $\mathfrak{D}$. Dans le point suivant, nous examinerons la question de l'unicité d'une théorie des diviseurs et, dans le point 3), nous donnerons une importante condition nécessaire (mais non suffisante) d'existence.

Dans le § 5, nous démontrerons l'existence d'une théorie des diviseurs pour tout ordre maximum d'un corps de nombres algébriques (pour les ordres non maxima, alors, d'après le théorème 3, il n'existe pas de théorie des diviseurs).

2) Unicité

THÉORÈME 1. — ***Si un anneau*** $\mathfrak{D}$ ***admet une théorie des diviseurs, alors elle est unique. Plus précisément, cela signifie que pour deux homomorphismes***

$$\mathfrak{D}^* \to \text{A} \qquad \textit{et} \qquad \mathfrak{D}^* \to \text{A}'$$

satisfaisant à la déjinition ci-dessus, il existe un isomorphisme $\Delta \simeq$ A' ***faisant se correspondre les diviseurs principaux de*** A ***et*** A' ***respectivement, qui correspondent aux mêmes éléments*** $\alpha \in \mathfrak{D}^*$.

DÉMONSTRATION. — Soient $\mathfrak{D}^* \to$ A et $\mathfrak{D}^* \to$ A' deux théories des diviseurs de l'anneau $\mathfrak{D}$. Pour des diviseurs premiers $\mathfrak{p} \in$ A et $\mathfrak{p}' \in$ A' nous désignerons par $\bar{\mathfrak{p}}$ et $\mathfrak{p}'$ les ensembles des éléments de l'anneau $\mathfrak{D}$ divisibles, respectivement par $\mathfrak{p}$ et $\mathfrak{p}'$ (la divisibilité par $\mathfrak{p}$ est considérée pour la théorie $\mathfrak{D}^* \to$ A et la divisibilité par $\mathfrak{p}'$ pour la théorie $\mathfrak{D}^* \to$ A'). Démontrons que pour tout diviseur premier $\mathfrak{p}' \in$ A', il existe un diviseur premier $\mathfrak{p} \in$ A tel que $\bar{\mathfrak{p}} \subset \bar{\mathfrak{p}'}$. Supposons qu'il n'en soit pas ainsi, i. e. que $\bar{\mathfrak{p}} \not\subset \bar{\mathfrak{p}'}$ pour tout diviseur premier $\mathfrak{p} \in$ A. Il résulte facilement de la condition 3° que, pour tout diviseur, l'ensemble de tous les éléments de $\mathfrak{D}$ qu'il divise ne peut être réduit à 0. Choisissons dans $\mathfrak{D}$ un élément $\beta \neq 0$ divisible par $\mathfrak{p}'$ et décomposons le diviseur principal $(\beta) \in$ A en facteurs premiers

$$(\beta) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}$$

($\mathfrak{p}_1, \dots, \mathfrak{p}_r$ sont des diviseurs premiers du monoïde A). Puisque nous avons supposé que $\bar{\mathfrak{p}}_i \not\subset \bar{\mathfrak{p}'}$, alors, pour tout $i = 1, \dots, r$, on peut trouver un élément $\gamma_i \in \mathfrak{D}$ divisible par $\mathfrak{p}_i$ mais non divisible par p'. Le produit

$$\gamma = \gamma_1^{k_1} \dots \gamma_r^{k_r}$$

est divisible par $\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}$ ce qui entraîne, d'après la condition 1°, que y est divisible par β dans l'anneau $\mathfrak{D}$. Mais alors y est aussi divisible par p' ; nous avons obtenu une contradiction puisque le produit $\gamma_1^{k_1} \dots \gamma_r^{k_r}$ ne peut pas être divisible par p' puisque $\mathfrak{p}'$ est premier et ne divise aucun des nombres γ_i.

Ainsi, pour tout diviseur premier $\mathfrak{p}' \in$ A' on peut trouver un diviseur premier $\mathfrak{p} \in$ A tel que $\bar{\mathfrak{p}} \subset \bar{\mathfrak{p}'}$. Par symétrie, il existe un diviseur premier q' $\in$ A' tel que $\bar{\mathfrak{q}'} \subset \bar{\mathfrak{p}}$. Montrons que q' = $\mathfrak{p}'$ et par suite $\bar{\mathfrak{q}'} = \bar{\mathfrak{p}} = \bar{\mathfrak{p}'}$. En effet, d'après la condition 3° il existe dans l'anneau $\mathfrak{D}$ un élément ξ divisible par q' et non divisible par q'p'. Si on suppose q' $\neq$ p', alors cet élément ξ n'est pas divisible par $\mathfrak{p}'$ et nous obtenons une contraction avec l'inclusion $\bar{\mathfrak{q}'} \subset \bar{\mathfrak{p}'}$.

Puisque le diviseur p $\in$ A tel que $\bar{\mathfrak{p}} = \bar{\mathfrak{p}'}$ (pour $\mathfrak{p}' \in$ A' donné) est défini de manière unique (condition 39, nous avons défini une correspondance biunivoque $\mathfrak{p} \leftrightarrow \mathfrak{p}'$ entre les diviseurs premiers de A et de A'. On peut prolonger cette correspondance (et de manière unique, c'est évident) en un isomorphisme A $\sim$ A' de la manière suivante : si $\mathfrak{p}_1 \leftrightarrow \mathfrak{p}_1', \dots, \mathfrak{p}_r \leftrightarrow \mathfrak{p}_r'$, alors

$$\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \leftrightarrow \mathfrak{p}_1'^{k_1} \dots \mathfrak{p}_r'^{k_r}.$$

Il nous reste à vérifier que cet isomorphisme fait se correspondre les diviseurs principaux $(a) \in A$ et $(a)' \in A'$ définis par le même élément $a \in \mathfrak{D}$. Supposons que des diviseurs $\mathfrak{p} \in A$ et $\mathfrak{p}' \in A'$ qui se correspondent l'un à l'autre interviennent respectivement avec les exposants k et l dans les décompositions de (a) et (a)'. D'après la condition 3°, il existe dans l'anneau $\mathfrak{D}$ un élément π divisible par $\mathfrak{p}$ et non divisible par $\mathfrak{p}^2$. D'après l'égalité $\overline{\mathfrak{p}} = \overline{\mathfrak{p}'}$, l'élément π est aussi divisible par p'. Ainsi, le diviseur principal (π) s'écrit $(\pi) = \mathfrak{p}\mathfrak{b}$ où b n'est pas divisible par p. Choisissons dans $\mathfrak{D}$ un élément ω divisible par $\mathfrak{b}^k$ et non divisible par $\mathfrak{b}^k\mathfrak{p}$. Puisque $\mathfrak{p}$ ne divise pas $\mathfrak{b}^k$, alors ω n'est pas divisible par $\mathfrak{p}$ et par suite par p'. Considérons le produit $\alpha\omega$. Puisque a est divisible par $\mathfrak{p}^k$ et ω par $\mathfrak{b}^k$ alors $\alpha\omega$ est divisible par $\mathfrak{p}^k\mathfrak{b}^k = (\pi^k)$, d'oh, d'après la condition (1), $\alpha\omega = \pi^k\eta$, $\eta \in \mathfrak{D}$. Mais $\mathfrak{p}' | \pi$ et par suite $\alpha\omega$ est divisible par $\mathfrak{p}'^k$ et puisque $\mathfrak{p}' \nmid \omega$, alors $\mathfrak{p}'^k | \alpha$. Cela montre que dans le diviseur $(a)' \in A'$, le diviseur premier $\mathfrak{p}'$ intervient avec un exposant supérieur à k, i. e. que $l \geqslant k$. Par symétrie, on a aussi $k \geqslant l$ d'où $l = k$.

Nous avons démontré ainsi que si

$$(a) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \text{ et } \mathfrak{p}_1 \leftrightarrow \mathfrak{p}_1', \dots, \mathfrak{p}_r \leftrightarrow \mathfrak{p}_r' \text{ alors } (a)' = \mathfrak{p}_1'^{k_1} \dots \mathfrak{p}_r'^{k_r}$$

ce qui montre que, par l'isomorphisme $A \sim A'$, les diviseurs principaux (a) et $(a)'$ correspondent l'un à l'autre. Le théorème 1 est ainsi complètement démontré.

S'il y a unicité de la décomposition en facteurs premiers dans l'anneau $\mathfrak{D}$, alors il est facile de construire une théorie des diviseurs $\mathfrak{D}^* \to A$ de cet anneau; pour cette théorie, tous les diviseurs seront principaux. En effet, décomposons $\mathfrak{D}^*$ en classes d'éléments associés entre eux et soit A l'ensemble de ces classes. Pour tout $a \in \mathfrak{D}^*$, désignons par (a) la classe des éléments associés à a. Il est facile de voir que pour la multiplication $(\alpha)(\beta) = (\alpha\beta)$, l'ensemble A est un monoïde dans lequel la décomposition en facteurs premiers est unique et que l'application $a \to (a)$, $a \in a)^*$, satisfait aux conditions 1°, 2° et 3°. Les diviseurs premiers sont ici les classes (π), où π est un élément premier de $\mathfrak{D}$. D'après le théorème 1, toute thtorie des diviseurs pour l'anneau $\mathfrak{D}$ coïncide avec celle que nous venons de construire.

Supposons maintenant qu'un certain anneau $\mathfrak{D}$ admet une théorie des diviseurs $\mathfrak{D}^* \to A$ pour laquelle tous les diviseurs de A sont principaux et démontrons qu'alors un élément $\pi \neq 0$ de l'anneau $\mathfrak{D}$ est premier si et seulement si le diviseur (π) est premier. En effet, si $(\pi) = \mathfrak{p}$ est un diviseur premier et si y divise π dans l'anneau $\mathfrak{D}$, alors le diviseur (y) divise $\mathfrak{p}$ (dans le monoïde A) et par suite coïncide soit avec $\mathfrak{p}$, soit avec le diviseur unité $\mathfrak{e}$. Dans le premier cas, y est associé avec π et dans le second cas c'est une unité de l'anneau $\mathfrak{D}$. Ainsi π est un élément premier de l'anneau $\mathfrak{D}$. Réciproquement, soit (a) un diviseur $\neq \mathfrak{e}$ et non premier. Puisque (a) est divisible par

un certain diviseur premier $\mathfrak{p} = (\pi)$ qui ne lui est pas égal, alors α est divisible par le nombre premier π qui ne lui est pas associé. Par suite l'élément a n'est pas premier.

Ainsi, si tous les diviseurs sont principaux, le fait que le diviseur (π) soit premier équivaut au fait que l'élément π soit premier.

Soit maintenant a un élément quelconque de $\mathfrak{D}$. Si on a dans A la décomposition

$$a = \mathfrak{p}_1 \dots \mathfrak{p}_r \tag{1}$$

(les diviseurs $\mathfrak{p}_i$ sont premiers mais pas nécessairement distincts) et si

$$\mathfrak{p}_1 = (\pi_1), \dots, \mathfrak{p}_r = (\pi_r),$$

alors nous aurons dans l'anneau $\mathfrak{D}$ la décomposition

$$a = \varepsilon\pi_1 \dots \pi_r, \tag{2}$$

où ε est une unité de l'anneau $\mathfrak{D}$. Puisque, par passage aux diviseurs, toute décomposition du type (2) donne une décomposition du type (1), alors dans $\mathfrak{D}$ on a unicité de la décomposition en facteurs premiers.

Nous avons obtenu le résultat suivant.

THÉORÈME *2.* — ***Pour que dans un anneau $\mathfrak{D}$ la décomposition en facteurs premiers soit possible et unique, il faut et il suffit qu'il existe pour $\mathfrak{D}$ une théorie des diviseurs $\mathfrak{D}^* \to$ A et que, dans cette théorie, tous les diviseurs de* A *soient principaux.***

3) Nécessité d'être intégralement clos pour un anneau admettant une théorie des diviseurs

Nous avons déjà dit qu'il n'existe pas de théorie des diviseurs pour tout anneau. L'existence d'un homomorphisme $a \to (a)$ satisfaisant aux conditions de la définition d'une théorie des diviseurs impose des conditions sur l'anneau.

THÉORÈME *3.* — ***Si un anneau $\mathfrak{D}$ admet une théorie des diviseurs, alors cet anneau est intégralement clos (dans son corps des fractions*** K).

DÉMONSTRATION. — Supposons qu'un certain élément ξ du corps des fractions K de l'anneau $\mathfrak{D}$ qui satisfait à la relation

$$\xi^n + a_1\xi^{n-1} + \dots + a_{n-1}\xi + a_n = 0 \qquad (a_1, \dots, a_n \in \mathfrak{D})$$

n'appartient pas à $\mathfrak{D}$. Représentons-le sous la forme $\xi = \frac{\alpha}{\beta}$ où $\alpha \in \mathfrak{D}$ et $\beta \in \mathfrak{D}$ et décomposons les diviseurs principaux (a) et (β) en un produit de puis-

sances de diviseurs premiers. Puisque α n'est pas divisible par β dans l'anneau $\mathfrak{D}$ (par hypothèse $\xi \notin \mathfrak{D}$), alors (α) n'est pas divisible par (β) au sens des diviseurs (condition 1°). Cela signifie qu'il existe un diviseur premier $\mathfrak{p} \in A$ qui figure dans la décomposition de (β) avec une puissance plus grande que dans (IX). Supposons que $\mathfrak{p}$ figure dans (α) avec un exposant $k \geqslant 0$. Puisque (β) est divisible par $\mathfrak{p}^{k+1}$, alors la condition 2° entraîne que la partie droite de l'égalité

$$\alpha^n = a_1\beta\alpha^{n-1} - \ldots - a_n\beta^n$$

est divisible par $\mathfrak{p}^{kn+1}$. Mais $\mathfrak{p}$ figure dans le diviseur $(\alpha^n) = (\alpha)^n$ avec l'exposant kn et par suite α^n ne peut pas être divisible par $\mathfrak{p}^{kn+1}$. La contradiction obtenue montre que $\xi \in \mathfrak{D}$ et le théorème 3 est démontré.

Une autre condition nécessaire d'existence d'une théorie des diviseurs est donnée dans l'exercice 1.

Puisque parmi les ordres des corps de nombres algébriques, il n'y a que les ordres maxima qui sont intégralement clos, alors, d'après le théorème 3, on ne peut espérer une théorie des diviseurs que pour eux.

4) Théorie des diviseurs et valuations

Occupons-nous maintenant de la construction effective d'une théorie des diviseurs. Nous supposerons que l'anneau $\mathfrak{D}$ admet une théorie des diviseurs $\mathfrak{D}^* \to A$ et préciserons comment on peut construire cette théorie.

Choisissant un certain diviseur premier p, nous pouvons lui associer une fonction $\nu_p(\alpha)$, de même que dans le chapitre premier nous avons associé au nombre p une valuation p-adique. Pour tout $\alpha \neq 0$ de $\mathfrak{D}$, désignons par $\nu_p(\alpha)$ l'exposant de $\mathfrak{p}$ dans la décomposition du diviseur principal (α) en facteurs premiers. Il est évident que $\nu_p(\alpha)$ est caractérisé par le fait que

$$\mathfrak{p}^{\nu_p(\alpha)} \mid \alpha \qquad \text{et} \qquad \mathfrak{p}^{\nu_p(\alpha)+1} \nmid \alpha.$$

Puisque 0 est divisible par des puissances arbitrairement grandes de $\mathfrak{p}$, on peut poser $\nu_p(0) = \infty$.

Il résulte facilement de sa définition que la fonction $\nu_p(\alpha)$ possède les propriétés suivantes :

$$\nu_p(\alpha\beta) = \nu_p(\alpha) + \nu_p(\beta), \tag{3}$$

$$\nu_p(\alpha + \beta) \geqslant \min(\nu_p(\alpha), \nu_p(\beta)) \tag{4}$$

(pour la démonstration de la propriété (4), il faut utiliser la condition 2°).

Nous pouvons prolonger la fonction $\nu_p(\alpha)$ au corps des fractions K de l'anneau $\mathfrak{D}$ en conservant les propriétés (3) et (4). En effet, pour

$$\xi = \frac{\alpha}{\beta} \in \mathbf{K} \quad (\alpha, \beta \in \mathfrak{D}),$$

posons

$$\nu_{\mathfrak{p}}(\xi) = \nu_{\mathfrak{p}}(\alpha) - \nu_{\mathfrak{p}}(\beta).$$

II est clair que la valeur $\nu_{\mathfrak{p}}(\xi)$ ne dépend pas de la représentation de ξ sous la forme $\xi = \frac{\alpha}{\beta}$ et que la fonction $\nu_{\mathfrak{p}}(\xi)$ ainsi prolongée satisfait aux conditions (3) et (4).

Précisons maintenant l'ensemble des valeurs prises par la fonction $\nu_{\mathfrak{p}}(\alpha)$ quand a parcourt tous les éléments du corps K. Puisque les diviseurs $\mathfrak{p}$ et $\mathfrak{p}^2$ sont distincts, alors, d'après la condition 3°, il existe un élément $y \in \mathfrak{D}$ qui est divisible par $\mathfrak{p}$ et non divisible par $\mathfrak{p}^2$. Pour cet élément, nous avons $\nu_{\mathfrak{p}}(\gamma) = 1$. Mais alors $\nu_{\mathfrak{p}}(\gamma^k) = k$ pour tout entier k ce qui démontre que la fonction $\nu_{\mathfrak{p}}(\alpha)$ prend toutes les valeurs entières rationnelles.

DÉFINITION. — *Soit* K *un corps quelconque. Une fonction v(a) définie sur* K *s'appelle une valuation du corps* K *si elle satisfait aux conditions* :

1° v(a) *prend toutes les valeurs rationnelles entières quand a parcourt tous les éléments* $\neq 0$ *de* K; $\nu(0) = \infty$.

2° $$\nu(\alpha\beta) = \nu(\alpha)\nu(\beta).$$

3° $$\nu(\alpha + \beta) \geqslant \min(\nu(\alpha), \nu(\beta)).$$

Nous pouvons maintenant dire que tout diviseur premier $\mathfrak{p}$ de l'anneau $\mathfrak{D}$ définit une certaine valuation $\nu_{\mathfrak{p}}(\alpha)$ du corps des fractions K. Il est facile de voir que pour des diviseurs premiers distincts $\mathfrak{p}$ et q, les valuations correspondantes $\nu_{\mathfrak{p}}$ et $\nu_{\mathfrak{q}}$ sont aussi distinctes. En effet, d'après la condition 3°, il existe dans l'anneau $\mathfrak{D}$ un élément y divisible par $\mathfrak{p}$ et non divisible par q. Mais alors $\nu_{\mathfrak{p}}(\gamma) \geqslant 1$ et $\nu_{\mathfrak{q}}(\gamma) = 0$, ce qui signifie $\nu_{\mathfrak{p}} \neq \nu_{\mathfrak{q}}$.

Toutes les valuations du corps K qui sont de la forme $\nu_{\mathfrak{p}}$ possèdent la propriété :

$$\nu_{\mathfrak{p}}(\alpha) \geqslant 0 \qquad \text{pour tout } \alpha \in \mathfrak{D}. \tag{5}$$

La décomposition d'un diviseur principal *(a)* (défini par l'élément $a \in \mathfrak{D}^*$) en facteurs premiers s'exprime très simplement au moyen des valuations $\nu_{\mathfrak{p}}$. Les diviseurs premiers $\mathfrak{p}_i$ qui figurent dans cette décomposition sont caractérisés par la condition $\nu_{\mathfrak{p}_i}(\alpha) > 0$. Cette décomposition s'écrit

$$(\alpha) = \prod \mathfrak{p}_i^{\nu_{\mathfrak{p}_i}(\alpha)} \tag{6}$$

où $\mathfrak{p}_i$ parcourt tous les diviseurs premiers tels que $\nu_{\mathfrak{p}_i}(\alpha) > 0$.

Ainsi, le monoïde A des diviseurs et l'homomorphisme $\mathfrak{D}^* \to A$ sont complètement définis par la donnée de l'ensemble des valuations $\nu_{\mathfrak{p}}$ du

corps K qui correspondent aux diviseurs premiers $\mathfrak{p}$. En effet, l'ensemble de tous les diviseurs et leur loi de multiplication sont définis par la donnée des diviseurs premiers (tout diviseur est un produit de diviseurs premiers élevés à des puissances positives et, dans la multiplication des diviseurs, les exposants correspondants s'ajoutent). En ce qui concerne les diviseurs premiers, ce sont des objets $\mathfrak{p}$ qui correspondent biunivoquement aux valuations $\nu_{\mathfrak{p}}$. Enfin, l'importante égalité (6) dtfinit un homomorphisme $\mathfrak{D}^* \to A$.

Cela montre que la construction de la théorie des diviseurs peut s'appuyer sur la notion de valuation. C'est sur cette remarque que repose l'étude suivante.

Précisons tout d'abord l'importante question suivante : quelles sont les proprittés qui caractérisent l'ensemble $\mathfrak{R}$ de toutes les valuations ν du corps K qui correspondent à une théorie des diviseurs de l'anneau $\mathfrak{D}$. Puisque le produit (6) contient seulement un nombre fini de facteurs d'exposants non nuls, alors l'ensemble X'doit satisfaire à la condition $\nu(\alpha) = 0$ pour presque tout $\nu \in \mathfrak{R}$, pour a fixé dans $\mathfrak{D}^*$ (l'expression « pour presque tout ν » signifie : pour tout ν sauf pour un nombre fini).

De plus, d'après (5), pour tout $\nu \in \mathfrak{R}$, nous devons avoir $\nu(a) \geqslant 0$ si $a \in \mathfrak{D}$. Inversement, supposons que pour un certain $\xi \in K$ on ait $\nu(\xi) \geqslant 0$ pour tout $\nu \in \mathfrak{R}$. Si nous représentons ξ sous la forme $\xi = \frac{\alpha}{\beta}$ $(a, \beta \in \mathfrak{D})$, nos conditions s'écrivent $\nu(a) > \nu(\beta)$ pour tout $\nu \in \mathfrak{R}$. Mais cela est équivalent au fait que le diviseur principal (a) est divisible par le diviseur principal (β). D'après la condition 1° nous obtenons alors que a est divisible par β dans l'anneau $\mathfrak{D}$, i. e. $\xi \in \mathfrak{D}$. Nous avons ainsi obtenu une deuxième condition nécessaire : l'ensemble des valuations $\mathfrak{R}$ est tel que les inégalités $\nu(a) \geqslant 0$ pour tout $\nu \in \mathfrak{R}$ caractérisent les éléments de l'anneau $\mathfrak{D}$.

Pour mettre en évidence une dernière propriété de l'ensemble $\mathfrak{R}$, choisissons un nombre fini de valuations $\nu_1, \ldots, \nu_m$ qui correspondent aux diviseurs premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Fixant des nombres entiers positifs $k_1, \ldots, k_m$, considérons le diviseur $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m}$. D'après la condition 3°, il existe un élément $\alpha_i \in \mathfrak{D}$ divisible par $\mathfrak{a}_i = \mathfrak{a}\mathfrak{p}, \ldots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \ldots \mathfrak{p}_m$ et non divisible par $\mathfrak{a}_i\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$. Considérons la somme

$$a = \alpha_1 + \ldots + a_m.$$

D'après la condition 2°, l'élément a est divisible par $\mathfrak{p}_i^{k_i}$ et n'est pas divisible par $\mathfrak{p}_i^{k_i+1}$. Cela démontre que l'ensemble $\mathfrak{R}$ vérifie aussi la condition nécessaire suivante : pour des valuations quelconques $\nu_1, \ldots, \nu_m$ de $\mathfrak{R}$ et des nombres entiers positifs quelconques $k_1, \ldots, k_m$ il existe un élément $a \in \mathfrak{D}$ tel que $\nu_i(\alpha) = k_i$ $(1 \leqslant i \leqslant m)$.

Les conditions nécessaires ci-dessus sont aussi suffisantes pour qu'on

puisse construire la théorie des diviseurs de l'anneau $\mathfrak{D}$ à partir de l'ensemble $\mathfrak{K}$. Pour démontrer ce résultat, considérons un monoïde A à décomposition en facteurs premiers uniques dont les éléments premiers sont en correspondance biunivoque avec les éléments de $\mathfrak{R}$. La valuation $v \in \mathfrak{R}$ qui correspond à l'élément premier $\mathfrak{p} \in A$ sera désignée par $v_{\mathfrak{p}}$. D'après la première et la deuxième condition, pour tout $\alpha \in \mathfrak{D}^*$, le produit (6) a un sens (les nombres $v_{\mathfrak{p}_i}(\alpha)$ sont positifs et seuls un nombre fini d'entre eux sont non nuls). D'après la propriété $v(\alpha\beta) = v(a) + v(\beta)$, l'application $a \to (a)$ est un homomorphisme $\mathfrak{D}^* \to A$. Il découle facilement de la deuxième condition que la divisibilité de α par β dans l'anneau $\mathfrak{D}$ est équivalente aux inégalités $v(\alpha) \geqslant v(\beta)$ pour tout $v \in \mathfrak{R}$. Cela montre que la condition 1° est remplie. La condition 2° résulte immédiatement de l'inégalité

$$v(\alpha \pm \beta) \geqslant \min (v(\alpha), v(\beta)).$$

Si a et $\mathfrak{b}$ sont deux éléments distincts de A, il existe un certain élément premier $\mathfrak{p}$ qui figure dans leurs décompositions avec des exposants distincts, disons par exemple k et l. Soit $k < l$. D'après la troisième condition, il existe dans $\mathfrak{D}$ un élément α divisible par a et tel que $v_{\mathfrak{p}}(\alpha) = k$ par suite, cet élément n'est pas divisible par $\mathfrak{b}$. Cela démontre que la condition 3° est remplie. L'homomorphisme $\mathfrak{D}^* \to A$ définit donc une théorie des diviseurs pour l'anneau $\mathfrak{D}$.

Formulons ce résultat.

THÉORÈME *4. — Soient $\mathfrak{D}$ un anneau,* K *son corps des fractions et $\mathfrak{R}$ un certain ensemble de valuations du corps* K. *Pour que les valuations de $\mathfrak{R}$ définissent une théorie des diviseurs pour l'anneau $\mathfrak{D}$, il faut et il suffit que les conditions suivantes soient réalisées* :

1) *Pour $\alpha \neq 0$ de $\mathfrak{D}$ il existe au plus un nombre fini de valuations $v \in \mathfrak{R}$ telles que $v(\alpha) \neq 0$;*

2) Un élément $\alpha \in$ K appartient à $\mathfrak{D}$ si et seulement si $v(\alpha) \geqslant 0$ pour tout $v \in \mathfrak{R}$;

3) Pour tout système fini $v_1, \ldots, v_m$ de valuations distinctes de $\mathfrak{R}$ et pour des nombres entiers positifs quelconques $k_1, \ldots, k_m$, il existe un élément $\alpha \in \mathfrak{D}$ tel que

$$v,(a) = k,, \ldots, v_m(\alpha) = k_m.$$

La construction d'une théorie des diviseurs pour un anneau $\mathfrak{D}$ se réduit donc à la construction dans son corps de fractions K de l'ensemble $\mathfrak{R}$ des valuations correspondantes.

Nous n'étudierons pas en détail les anneaux intégralement clos pour lesquels une telle construction est possible (cf. par exemple le livre de Van der Waerden, ***Modern Algebra,*** t. **2**, § 105). Nous démontrerons dans

le paragraphe suivant que si pour un anneau $\mathfrak{O}$ de corps des fractions k il existe une théorie des diviseurs, alors il en existe aussi une pour toute fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{O}$ dans une extension finie K du corps k. Puisque pour l'anneau $\mathbf{Z}$ des nombres entiers rationnels la théorie des diviseurs est bien connue (ici il y a unicitt de la décomposition en facteurs premiers), alors cela démontre aussi l'existence d'une théorie des diviseurs pour les ordres maxima des corps de nombres algébriques.

Le choix des valuations ν du corps K que l'on doit prendre pour construire une théorie des diviseurs dépend essentiellement de l'anneau $\mathfrak{D}$ et ce choix n'épuise pas nécessairement toutes les valuations du corps K (cf. exercice 6). Montrons pourtant que, dans le cas de l'anneau Z des nombres rationnels, le choix des valuations correspondantes épuise toutes les valuations du corps des nombres rationnels (nous verrons par la suite que ce même phénomène se produit aussi pour tous les ordres maxima des corps de nombres algébriques).

A tout nombre premier $p \in Z$ (i. e. à tout diviseur premier de l'anneau Z) correspond une valuation ν_p dont la valeur sur tout nombre rationnel $\neq 0$

$$x = p^m \frac{a}{b} \tag{7}$$

(a et b sont entiers et non divisibles par p) est définie par

$$\nu_p(x) = m. \tag{8}$$

Cette valuation ν_p est appelée ***valuation p-adique*** du corps Q (il est évident que les valeurs de la valuation (8) coïncident avec les valeurs de la valuation p-adique sur le corps $\mathbf{Q}_p$ des nombres p-adiques (cf. chap. 1, § 3-2)).

THÉORÈME 5. — ***Toutes les valuations du corps des nombres rationnels sont épuisées par*** les valuations ***p-adiques*** ν_p (pour tout p prouvés).

DÉMONSTRATION. — Soit ν une valuation quelconque du corps Q. Puisque

$$\nu(1 + \ldots + 1) \geqslant \min (\nu(1), \ldots, \nu(1)) = 0,$$

alors $\nu(n) \geqslant 0$ pour tout entier naturel n. Si $\nu(p) = 0$ pour tout p premier, nous aurions aussi $\nu(a) = 0$ pour tout $a \neq 0$ de Q ce qui est impossible d'après la condition 1° de la définition des valuations. Par suite, on aura $\nu(p) = e > 0$ pour un certain p premier. Supposons que pour q premier, $q \neq p$, nous avons aussi $\nu(q) > 0$; alors de l'égalitépu $+ qv = 1$, u et v entiers, résulte

$$0 = \nu(pu + qv) \geqslant \min (\nu(pu), \nu(qv)) \geqslant \min (\nu(p), \nu(q)) > 0.$$

La contradiction obtenue montre que $v(q) = 0$ pour tous les nombres premiers $q \neq p$ et par suite $\nu(a) = 0$ pour tout entier a non divisible par p. Pour un nombre rationnel de la forme (7), nous aurons donc

$$v(x) = m\nu(p) + v(a) - v(b) = me = e\nu_p(x).$$

Puisque les valeurs de la valuation doivent parcourir tous les nombres entiers, alors e = 1 et par suite $\nu = \nu_p$, ce qui démontre le théorème 5.

Remarquons qu'on peut facilement déduire le théorème 5 du théorème 3 du chapitre premier, § 4 dont la deuxième partie de la démonstration coïncide, pour l'essentiel, avec la démonstration ci-dessus.

Considérons pour terminer un dernier cas particulier.

Supposons qu'un anneau $\mathfrak{D}$ admet une théorie des diviseurs $\mathfrak{D}^* \to A$ avec un nombre fini de diviseurs premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Désignons par $\nu_1, \ldots, \nu_m$ les valuations correspondantes du corps des fractions K. D'après la condition 3) du théorème 4, pour tout diviseur $a = \mathfrak{p}_1^{k_1}, \ldots, \mathfrak{p}_m^{k_m} \in A$ $(k_i \geqslant 0)$, il existe un élément α dans l'anneau $\mathfrak{D}$ tel que $\nu_1(\alpha) = k_1, \ldots, \nu_m(\alpha) = k_m$. Mais cela signifie que le diviseur a coïncide avec le diviseur principal (a). Ainsi tous les diviseurs de A sont principaux et par suite il y a unicité de la décomposition en facteurs premiers dans l'anneau $\mathfrak{D}$. Si $\mathfrak{p}_1 = (\pi_1), \ldots, \mathfrak{p}_m = (\pi_m)$, alors les éléments $\pi_1, \ldots, \pi_m$ forment un système complet d'éléments premiers non associés deux à deux de l'anneau $\mathfrak{D}$ et tout élément $a \in \mathfrak{D}^*$ s'écrit de manière unique

$$a = \varepsilon\pi_1^{k_1} \ldots \pi_m^{k_m},$$

ε unité de $\mathfrak{D}$. Les éléments premiers $\pi_1, \ldots, \pi_m$ sont évidemment caractérisés par les conditions :

$$\nu_i(\pi_i) = 1, \qquad \nu_j(\pi_i) = 0 \qquad \text{pour } j \neq i.$$

Nous avons ainsi démontré le résultat suivant :

THÉORÈME 6. — ***Si un anneau $\mathfrak{D}$ admet une théorie des diviseurs avec un nombre fini de diviseurs premiers, alors il y a unicité de la décomposition en facteurs premiers dans $\mathfrak{D}$.***

EXERCICES

1. Démontrer que si un anneau $\mathfrak{D}$ admet une théorie des diviseurs, alors tout élément de $\mathfrak{D}$ a seulement un nombre fini de diviseurs deux à deux non associés.

2. Démontrer que dans toute théorie des diviseurs tout diviseur est le plus grand commun diviseur de deux diviseurs principaux.

3. Soit K = $k(x)$ le corps des fonctions rationnelles sur un corps quelconque k et soit φ un polynôme irréductible de l'anneau $k[x]$. On peut alors représenter toute fonction rationnelle $u \neq 0$ de K sous la forme $u = \varphi^n \frac{f}{g}$, où f et g sont des polynômes de $k[x]$ non divisibles par φ. Montrer que la fonction ν_φ définie par $\nu_\varphi(u) = n$ est une valuation du corps K.

4. Si f et g sont des polynômes non nuls de l'anneau $k[x]$, de degrés respectifs m et n, posons $\nu^*(u) = m - n$ pour la fonction rationnelle $u = \frac{f}{g} \in k[x]$. Montrer que la fonction ν^* est une valuation du corps K = $k(x)$.

5. Montrer que les valuations ν_φ (pour tous les polynômes φ irréductibles de l'anneau $k[x]$ et la valuation ν^* (exercices 3 et 4) épuisent toutes les valuations ν du corps $k(x)$ telles que $\nu(a) \neq 0$ pour tout $a \neq 0$ de k.

6. Définir un ensemble $\mathfrak{R}$ de valuations du corps K = $k(x)$ satisfaisant aux conditions du théorème 4 si on prend $k[x]$ pour anneau $\mathfrak{D}$. Définir de même l'ensemble $\mathfrak{R}$ pour l'anneau $\mathfrak{D}' = k\left[\frac{1}{x}\right]$.

7. Soit K = $k(x, y)$ le corps des fonctions rationnelles en x et y sur le corps k. Pour tout entier naturel n, posons $x_n = \frac{x}{y^n}$ et représentons toute fonction rationnelle non nulle $u = u(x, y) \in$ K sous la forme

$$u = u(x_n y^n, y) = y^k \frac{f(x_n, y)}{g(x_n, y)}$$

où les polynômes f et g ne sont pas divisibles par y. Montrer que la fonction ν_n, définie par l'égalité $\nu_n(u) = k$ est une valuation du corps K. Montrer que toutes les valuations ν_n sont distinctes et que pour chacune d'elles $\nu_n(x) > 0$ $(n \geqslant 1)$.

8. Formuler et démontrer le critère d'irréductibilité d'Eisenstein (connu pour les polynômes à coefficients entiers) pour des polynômes à coefficients dans un anneau $\mathfrak{D}$ admettant une théorie des diviseurs.

9. Démontrer que si un anneau $\mathfrak{D}$ admet une théorie des diviseurs, alors son corps des fractions K admet des extensions algébriques de degré quelconque.

10. Pour tout polynôme $f \neq 0$ de l'anneau $\mathfrak{D} = k[x, y]$ des polynômes de deux variables sur un corps k, désignons part(f) le plus petit degré des monômes figurant dans f avec un coefficient non nul. Montrer que la valuation $\tilde{\nu}$ peut être prolongée en une valuation du corps $k(x, y)$ des fonctions rationnelles. Désignons par $\mathfrak{R}$ l'ensemble des valuations du corps $k(x, y)$ qui correspondent aux polynômes irréductibles de l'anneau $\mathfrak{D}$ et par $\mathfrak{R}_1$ l'ensemble obtenu en ajoutant à $\mathfrak{R}$ la valuation $\tilde{\nu}$. Quelle est la condition du théorème 4 qui n'est pas satisfaite pour l'anneau $\mathfrak{D}$ et l'ensemble $\mathfrak{R}_1$ de valuations ?

§ 4. — VALUATIONS

D'après le théorème § 3, la construction d'une théorie des diviseurs pour un anneau $\mathfrak{D}$ intégralement clos se réduit à la construction dans son corps des fractions K d'un ensemble de valuations possédant les propriétés énoncées dans ce théorème. Nous étudierons donc systématiquement les propriétés des valuations.

1) Propriétés élémentaires des valuations

De la définition d'une valuation ν sur un corps quelconque K (§ 3-4)) résultent facilement les propriétés suivantes :

$$\nu(\pm 1) = 0;$$
$$\nu(-\alpha) = \nu(a);$$
$$\nu\left(\frac{\alpha}{\beta}\right) = \nu(\alpha) - \nu(\beta), \qquad \beta \neq 0 :$$
$$\nu(\alpha^n) = n\nu(\alpha), \qquad n \in \mathbf{Z};$$
$$\nu(\alpha_1 + \ldots + a,) \geqslant min\ (\nu(\alpha_1), \ldots, \nu(\alpha_n)).$$

Supposons $\nu(\alpha) \neq \nu(\beta)$. Si $\nu(\alpha) > \nu(\beta)$ alors $\nu(\alpha + \beta) \geqslant \nu(\beta)$. D'autre part, l'égalité $\beta = (a + \beta) - \alpha$ entraîne $\nu(\beta) \geqslant \min\ (\nu(\alpha + \beta), \nu(\alpha))$ entraîne

$$\nu(\beta) \geqslant \nu(\alpha + \beta).$$

Ainsi

$$\nu(\alpha + \beta) = \min\ (\nu(\alpha)\ \nu(\beta)) \qquad \text{si} \qquad \nu(\alpha) \neq \nu(\beta). \tag{1}$$

Par récurrence, on obtient facilement

$$\nu(\alpha_1 + \ldots + \alpha_n) = \min\ (\nu(\alpha_1), \ldots, \nu(\alpha_n)),$$

si, parmi les valeurs $\nu(\alpha_1), \ldots, \nu(\alpha_n)$, il y en a une et une seule qui est strictement inférieure aux autres.

DÉFINITION. — ***Soit ν une valuation donnée d'un corps*** K. ***Le sous-anneau $\mathfrak{D}_\nu$ du corps*** K ***formé des éléments $a \in$ K tel que $\nu(a) \geqslant 0$ est appelé l'anneau de la valuation ν. Les éléments de $\mathfrak{D}_\nu$ sont dits entiers pour la valuation ν.***

Il est évident que pour l'anneau $\mathfrak{D}_\nu$ et l'ensemble $\mathfrak{R}$ formé de la seule valuation ν, les trois conditions du théorème **4**, § 3 sont satisfaites. Par suite, il existe pour l'anneau $\mathfrak{D}_\nu$ une théorie des diviseurs avec un unique diviseur premier. Les théorèmes 3 et 6 du § 3 donnent alors les résultats suivants :

THÉORÈME 1. — ***L'anneau $\mathfrak{D}_\nu$ de la valuation ν d'un corps*** K ***est intégralement fermé dans*** K.

THÉORÈME *2.* — ***A un élément associé près, il existe seulement un élément premier π dans l'anneau $\mathfrak{D}_\nu$ et tout élément $\alpha \neq 0$ de $\mathfrak{D}_\nu$ s'écrit de manière unique*** (pour π ***fixé) sous la forme $\alpha = \varepsilon\pi^m$, ε unité de $\mathfrak{D}_\nu$ ($m \geqslant 0$).***

Tout élément premier de l'anneau de la valuation ν est caractérisé par l'égalité $\nu(\pi) = 1$.

Dans l'anneau $\mathfrak{D}_\nu$, comme dans tout anneau, on peut considérer des

congruences modulo un élément (cf. appendice § 4-l)). Puisque les congruences modulo des éléments associés sont équivalentes, l'anneau des classes résiduelles de l'anneau $\mathfrak{D}_v$ modulo un nombre premier π ne dépend pas du choix de π et par suite est complètement défini par l'anneau $\mathfrak{D}_v$. Désignons par Σ_v cet anneau des classes résiduelles et montrons que c'est un corps. En effet, si $\alpha \in \mathfrak{D}_v$ et $\alpha \not\equiv 0 \pmod{\pi}$, alors $v(\alpha) = 0$ et par suit: α est une unité dans $\mathfrak{D}_v$. Mais alors, non seulement la congruence $\alpha\xi \equiv 1 \pmod{x}$, mais aussi l'équation $\alpha\xi = 1$ sont résolubles en $\xi \in \mathfrak{D}_v$.

Le corps Σ_v s'appelle le ***corps résiduel*** de la valuation v.

2) Indépendance des valuations

Supposons qu'un anneau $\mathfrak{D}$ admet une théorie des diviseurs $\mathfrak{D}^* \to A$ et soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ des diviseurs premiers distincts de A. D'après le théorème 4 du § 3, les valuations $v_1, \ldots, v_m$ du corps des fractions K qui correspondent à ces diviseurs premiers possèdent la propriété d'indépendance suivante : dans $\mathbf{K}^*$, il existe des éléments ξ sur lesquels ces valuations prennent respectivement des valeurs données quelconques $k_1, \ldots, k_m$. En effet, si pour tout $i = 1, \ldots, m$ nous posons $k_i' = \max(0, k_i)$ et $k_i'' = \min(0, k_i)$ alors, d'après la condition 3) du théorème 4 du § 3, il existe dans $\mathfrak{D}$ des éléments α et β tels que $v_i(\alpha) = k_i'$ et $v_i(\beta) = -k_i''$; par suite, pour $\xi = \frac{\alpha}{\beta}$, on aura $v_i(\xi) = k_i$ $(1 \leqslant i \leqslant m)$.

Montrons tout de suite que cette propriété d'indépendance n'est pas liée au fait que les valuations v_i correspondent à des diviseurs premiers pour une certaine théorie des diviseurs mais a lieu pour tout système fini de valuations.

THÉORÈME 3. — *Si $v_1, \ldots, v_m$ sont des valuations d'un corps* K *deux à deux distinctes, alors, pour tout système $k_1, \ldots, k_m$ de nombres entiers rationnels, il existe un élément $\xi \in \mathbf{K}$ tel que*

$$v_1(\xi) = k_1, \ldots, v_m(\xi) = k_m.$$

Désignons par $\mathfrak{D}_1, \ldots, \mathfrak{D}_m$ les anneaux des valuations $v_1, \ldots, v_m$ et par $\mathfrak{D}$ l'intersection $\bigcap_{i=1}^{m} \mathfrak{D}_i$. Pour l'anneau $\mathfrak{D}$ et pour l'ensemble $\mathfrak{R}$ des valuations $v_1, \ldots, v_m$ les conditions 1) et 2) du théorème 4 du § 3 sont trivialement satisfaites. Le théorème 3 montre que la condition 3° est aussi remplie et cela entraîne que l'anneau $\mathfrak{D}$ admet une théorie des diviseurs avec un nombre fini de diviseurs premiers. Le théorème 3 entraîne alors que tout système

fini $v_1, \ldots, v_m$ de valuations du corps K définit une théorie des diviseurs pour l'anneau $\mathfrak{D} = \bigcap_{i=1}^{m} \mathfrak{D}_i$. D'après le théorème 6 du § 3, nous obtenons donc le résultat suivant :

COROLLAIRE. — *Si $\mathfrak{D}_1, \ldots, \mathfrak{D}_m$ sont les anneaux des valuations $v_1, \ldots, v_m$ du corps K, deux à deux distinctes, alors l'intersection $\mathfrak{D} = \bigcap_{i=1}^{m} \mathfrak{D}_i$ est un anneau à décomposition unique en facteurs premiers. En particulier, tout élément $\alpha \neq 0$ de $\mathfrak{D}$ s'écrit de manière unique $\alpha = \varepsilon \pi_1^{k_1} \ldots \pi_m^{k_m}$ où ε est une unité de $\mathfrak{D}$ et $\pi_1, \ldots, \pi_m$ des éléments premiers fixés caractérisés par les conditions*

$$v_i(\pi_i) = 1, \qquad v_j(\pi_i) = 0 \qquad (j \neq i).$$

DÉMONSTRATION DU THÉORÈME 3. — Pour $m = 1$, le théorème résulte de la définition de la valuation d'un corps. Supposons $m \geqslant 2$ et le théorème démontré pour $(m - 1)$ valuations. Montrons alors qu'il n'existe pas d'entiers rationnels $c_1, \ldots, c_m$ non tous nuls simultanément tels que

$$c_1 v_1(\xi) + \ldots + c_m v_m(\xi) = 0 \tag{2}$$

pour tout $\xi \neq 0$ de K. Raisonnant par l'absurde, supposons que l'égalité *(2)* ait lieu. Parmi les coefficients, deux au moins sont non nuls et de même signe (en effet, si deux coefficients seulement sont $\neq 0$, par exemple c_1 et c_2, $c_1 > 0$ et $c_2 < 0$, alors l'égalité $c_1 v_1(\xi) + c_2 v_2(\xi) = 0$ entraîne $v_1(\xi) = e v_2(\xi)$, $e > 0$ et cela n'est possible que pour $e = 1$, d'où $v_1 = v_2$ ce qui contredit l'hypothèse). Changeant éventuellement l'ordre des termes, nous pouvons écrire la relation (2) sous la forme

$$v_1(\xi) = a_2 v_2(\xi) + \ldots + a_m v_m(\xi), \tag{3}$$

un au moins des coefficients rationnels a_i étant négatif. Par hypothèse de récurrence, on peut trouver dans le corps K des éléments β et β' tels que

$$v_i(\beta) = 0, \qquad v_i(\beta') = 1 \qquad \text{si} \qquad a_i \geqslant 0;$$
$$v_i(\beta) = 1, \qquad v_i(\beta') = 0 \qquad \text{si} \qquad a_i < 0,$$

pour tout $i = 2, \ldots, m$. Alors

$$v_1(\beta) < 0, \qquad v_1(\beta') \geqslant 0. \tag{4}$$

Considérons la somme $\beta + \beta'$. Puisqu'un des nombres $v_i(\beta)$ et $v_i(\beta')$ $(i = 2, \ldots, m)$ est égal à 0 et l'autre à 1, alors

$$v_i(\beta + \beta') = \min\,(v_i(\beta), v_i(\beta')) = 0.$$

D'après la relation (3), nous obtenons donc $\nu_1(\beta + \beta') = 0$. Mais, par ailleurs, les inégalités (4) nous donnent

$$\nu_1(\beta + \beta') = \min(\nu_1(\beta), \nu_1(\beta')) < 0.$$

La contradiction obtenue démontre que la relation (2) n'est pas possible.

Soient maintenant $\mathfrak{D}$ l'intersection des anneaux des valuations $\nu_2, \ldots, \nu_n$, E le groupe des unités de cet anneau et $\pi_2, \ldots, \pi_m$ les éléments premiers de l'anneau $\mathfrak{D}$ énumérés de telle sorte que $\nu_i(\pi_i) = 1$, $i = 2, \ldots, m$ (rappelons que le théorème 3 et aussi son corollaire sont vrais par hypothèse de récurrence pour $(m-1)$-valuations). Démontrons que les valeurs de la valuation ν_1 sur le groupe E ne peuvent pas être toutes égales à zéro. En effet tout élément $\xi \in K^*$ peut s'écrire

$$\xi = \varepsilon \pi_2^{k_2} \ldots \pi_m^{k_m} \tag{5}$$

pour $\varepsilon \in E$, $k_i = \nu_i(\xi)$ $(2 \leqslant i \leqslant m)$. Si $\nu_1(\varepsilon) = 0$ pour tout $\varepsilon \in E$, alors il résulterait de (5) que

$$\nu_1(\xi) = k_2\nu_1(\pi_2) + \ldots + k_m\nu_1(\pi_m),$$

que l'on peut aussi écrire sous la forme

$$\nu_1(\xi) = a_2\nu_2(\xi) + \ldots + a_m\nu_m(\xi),$$

où les entiers rationnels $a_i = \nu_1(\pi_i)$ ne dépendent pas de ξ; mais, comme nous l'avons vu, cette relation du type (2) est impossible pour tout $\xi \in K^*$. Ainsi, il existe dans le groupe E des éléments sur lesquels la valuation ν_1 prend une valeur non nulle.

Choisissons dans E un élément y tel que $\nu_1(y) = l$ soit la plus petite valeur positive prise par la valuation ν_1 sur le groupe E. Il est clair que toutes les valeurs de la valuation sur E sont alors des multiples du nombre 1. Il faut démontrer que $l = 1$. Si toutes les valeurs $a_2 = \nu_1(\pi_2), \ldots, a_m = \nu_1(\pi_m)$ sont divisibles par l, il résulte facilement de la représentation (5) que toutes les valeurs $\nu_1(\xi)$ de la valuation ν sont divisibles par l, ce qui n'est possible que pour $l = 1$. Il reste à étudier le cas où tous les a_i ne sont pas divisibles par l. Supposons par exemple a_2 non divisible par 1. Considérons alors l'élément

$$a = \pi_2(\pi_3 \ldots \pi_m)^l \gamma^s,$$

où l'entier s est choisi de telle sorte que le nombre

$$a_2 + l(a_3 + \ldots + a_m) + sl = l_1$$

satisfasse à l'inégalité $0 < l_1 < 1$. Il est clair que $\nu_1(a) = l_1$ et $\nu_i(a) > 0$ pour $i = 2, \ldots, m$. Posons

$$\varepsilon = \gamma + \alpha.$$

Puisque $\nu_i(\varepsilon) = \min(\nu_i(\gamma), \gamma_i(\alpha)) = 0$ pour tout $i = 2, \ldots, m$, alors $\varepsilon \in E$. De plus,

$$\nu_1(\varepsilon) = \min(l, l_1) = l_1,$$

et cela contredit le choix de y. Ainsi le cas où un des a_i n'est pas divisible par l est impossible et cela entraîne $l = 1$.

Nous pouvons maintenant supposer que les éléments premiers π_i $(2 \leqslant i \leqslant m)$ de l'anneau $\mathfrak{D}$ ont été choisis tels que $\nu_1(\pi_i) = a_i = 0$. En effet, on peut remplacer π_i par $\pi_i' = \pi_i \gamma^{-a_i}$, d'ou $\nu_1(\pi_i') = a_i - a_i \nu_1(\gamma) = 0$.

Posant $\pi_1 = y$, nous obtenons un système d'éléments $\pi_1, \ldots, \pi_m$ tels que

$$\nu_i(\pi_i) = 1 \qquad \text{et} \qquad \nu_j(\pi_i) = 0 \qquad \text{pour } i \neq j.$$

Si maintenant $k_1, \ldots, k_m$ sont des nombres entiers quelconques, alors, pour l'élément $\xi = \pi_1^{k_1} \ldots \pi_m^{k_m}$, nous avons

$$\nu_1(\xi) = k_1, \ldots, \nu_m(\xi) = k_m$$

Le théorème 3 est démontré.

Du théorème 3 découle facilement le résultat suivant :

THÉORÈME 4 (d'approximation). — ***Si*** $\nu_1, \ldots, \nu_m$ ***sont des valuations d'un corps*** K ***deux à deux distinctes, alors pour tout système d'éléments*** $\xi_1, \ldots, \xi_m$ ***de*** K ***et pour tout entier N, il existe dans le corps*** K ***un élément*** ξ ***tel que***

$$\gamma_1(\xi - \xi_1) \geqslant N, \ldots, \nu_m(\xi - \xi_m) \geqslant N.$$

DÉMONSTRATION. — Choisissons dans K des éléments $\alpha_1, \ldots, a$, tels que $\nu_i(\alpha_i) = -1$, $\nu_j(\alpha_i) = 1$ $(j \neq i)$ et posons

$$\xi = \frac{\alpha_1^k}{1 + \alpha_1^k} \xi_1 + \ldots + \frac{1 + \alpha_m^k}{\alpha_m^k} \xi_m.$$

Puisque $\nu_j(\alpha_i^k) \neq 0 = \nu_j(1)$ pour tout entier naturel k, alors, d'après la propriété (1), la valeur $\nu_j(1 + \alpha_i^k)$ est égale à 0 pour $i \neq j$ et à $-k$ pour $i = j$, d'où

$$\nu_j\left(\frac{\alpha_i^k}{1 + \alpha_i^k}\right) = k \text{ pour } i \neq j \text{ et } \nu_j\left(\frac{-1}{1 + \alpha_j^k}\right) = k.$$

Par suite .

$$\nu_j(\xi - \xi_j) \geqslant \min_j (k + \nu_j(\xi_i)).$$

Il est clair maintenant que ξ conviendra si on a pris k tel que

$$k \geqslant N - \min_{i,j} \nu_j(\xi_i).$$

3) Prolongement des valuations

Soient k un corps quelconque, K/k une extension finie et v une valuation du corps K. Considérant la restriction de v à k, il est clair que nous obtenons une fonction qui satisfait aux conditions 2° et 3° de la définition d'une valuation (§ 3-4)); la première condition, par contre peut ne pas être satisfaite, i. e. les valeurs de v sur k^* n'épuisent pas nécessairement **Z.** Pourtant $v(k^*)$ ne peut pas être réduit à 0; en effet, dans ce cas, le corps k serait entièrement contenu dans l'anneau de la valuation v et, puisque cet anneau est intégralement clos (théorème 1), il contiendrait aussi le corps K, ce qui est impossible. Ainsi il existe $a \in k^*$ tel que $v(a) \neq 0$ et $v(a) > 0$ (si $v(a) < 0$, alors $v(a^{-1}) > 0$).

Désignons par p un élément de k tel que v(p) $=$ e soit la plus petite valeur positive de la valuation v sur les éléments du corps k. Alors, pour tout $a \in k^*$ la valeur $v(a) = m$ est divisible par e. En effet, si $m = es + r$, $0 \leqslant r < e$, alors $v(ap^{-s}) = m - se = r$ ce qui entraîne $r = 0$, d'après la minimalité de e.

Posant maintenant

$$v_1(a) = \frac{v(a)}{e}, \qquad a \in k^*, \qquad v_0(0) = \infty \tag{6}$$

nous obtenons une fonction à valeurs entières qui est manifestement une valuation du corps k.

DÉFINITION. — *Soit* K *une extension finie d'un corps k. Si la valuation* v_0 *du corps k est liée à la valuation* v *du corps* K *par la relation* (6), *on dit que* v_0 *est induite sur k par la valuation* v *et que* v *est un prolongement de* v_0 *au corps* K. *L'entier naturel e défini de manière unique par la relation (6) est appelé l'indice de ramification de* v *par rapport à* v_0 *(ou par rapport au sous-corps k)* .

Attirons l'attention sur le fait que, dans cette définition, le terme « prolongement d'une valuation », pour $e > 1$, ne coïncide avec le sens habituel de prolongement d'une fonction à un domaine de définition plus grand.

D'après ce qui a été vu ci-dessus, toute valuation v sur K induit une valuation (unique) sur k. La réciproque est aussi vraie, i. e. toute valuation v_0 sur k admet un prolongement à K (qui en général n'est pas unique). La démonstration de ce fait est compliquée et nous l'étudierons dans le point suivant. Ici, nous étudierons les prolongements d'une valuation donnée, en supposant qu'ils existent.

Soient $k \subset K \subset K'$ une chaîne d'extensions finies et v_0, v, v' des valuations des corps k, K, K' respectivement. Il est évident que si v est un prolongement

de ν_0, d'indice de ramification e et ν' un prolongement de ν d'indice de ramification e', alors ν' est un prolongement de ν_0 au corps K', d'indice de ramification ee' par rapport à ν_0. Il est aussi facile de voir que si ν_0 et ν sont induites sur les sous-corps k et K par la valuation ν', alors v est un prolongement de ν_0.

LEMME 1. — *Si* K *est une extension finie de degré n du corps k, alors pour toute valuation* ν_0 *du corps k, il existe au plus n prolongements à* K.

DÉMONSTRATION. — Soient $\nu_1, \ldots, \nu_m$ des prolongements distincts de ν_0 au corps K. D'après le théorème 3, on peut trouver dans le corps K des éléments $\xi_1, \ldots, \xi_m$ tels que $\nu_i(\xi_i) = 0$ et $\nu_j(\xi_i) = 1$ pour $j \neq i$. Montrons que ces éléments sont linéairement indépendants sur k. Considérons une combinaison linéaire

$$\gamma = a_1\xi_1 + \ldots + a_m\xi_m$$

à coefficients $a_j \in k$ non tous nuls. Soit $p = \min(\nu_0(a_1), \ldots, \nu_0(a_m))$ et soit i_0 un indice tel que $\nu_0(a_{i_0}) = p$. Désignons par e l'indice de ramification de la valuation ν_{i_0} par rapport à k; alors

$$\nu_{i_0}(a_{i_0}\xi_{i_0}) = e\nu_0(a_{i_0}) + \nu_{i_0}(\xi_{i_0}) = ep$$
$$\nu_{i_0}(a_j\xi_j) = e\nu_0(a_j) + \nu_{i_0}(\xi_j) \geqslant ep + 1 \quad (j \neq i_0),$$

c'est pourquoi

$$\nu_{i_0}(\gamma) = \min(\nu_{i_0}(a_1\xi_1), \ldots, \nu_{i_0}(a_m\xi_m)) = ep,$$

et par suite $\gamma \neq 0$, ce qui démontre notre argument. De l'indépendance linéaire des éléments $\xi_1, \ldots, \xi_m$ résulte que $m \leqslant (K : k)$ et par suite le nombre des prolongements de ν_0 ne peut pas dépasser n. Le lemme 1 est démontré.

Supposons maintenant que $\nu_1, \ldots, \nu_m$ sont les prolongements d'une valuation fixée ν_0 d'un corps k à une extension finie K de k. Désignons par $\mathfrak{O}$ l'anneau de la valuation ν_0, par $\mathfrak{D}$ sa clôture intégrale dans K et par $\mathfrak{D}_1, \ldots, \mathfrak{D}_m$ les anneaux des valuations $\nu_1, \ldots, \nu_m$ respectivement. Puisque $\mathfrak{O} \subset \mathfrak{D}_i$ et puisque l'anneau $\mathfrak{D}_i$ est intégralement fermé dans K, alors $\mathfrak{D} \subset \mathfrak{D}_i$ pour tout $i = 1, \ldots, m$ et cela entraîne

$$\mathfrak{D} \subset \bigcap_{i=1}^{m} \mathfrak{D}_i.$$

Nous verrons dans la suite qu'en fait, cette inclusion est une égalité. S'il en est ainsi, d'après le corollaire du théorème 3, $\mathfrak{D}$ est un anneau à décomposition unique en facteurs premiers avec un nombre fini d'éléments premiers non associés. Puisque les éléments premiers non associés $\pi_1, \ldots, \pi_m$ de l'anneau $\mathfrak{D}$ sont en correspondance biunivoque avec les valuations

$\nu_1, \ldots, \nu_m$, nous avons obtenu ainsi une construction effective des valuations de K qui prolongent ν_0.

Supposons maintenant connu le fait que la fermeture intégrale $\mathfrak{D}$ dans K de l'anneau de la valuation ν_0 admet une décomposition unique en facteurs premiers avec un nombre fini d'éléments premiers non associés. D'après le théorème 6 du § 3, cette affirmation équivaut au fait que $\mathfrak{D}$ admet une théorie des diviseurs avec un nombre fini de diviseurs premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Montrons qu'alors la valuation ν_0 admet exactement m prolongements distincts au corps K qui sont les valuations $\nu_1, \ldots, \nu_m$ du corps K qui correspondent aux diviseurs premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$.

Soit p un certain élément premier de l'anneau $\mathfrak{O}$ de la valuation ν_0 (i. e. un élément de k tel que $\nu_0(p) = 1$) et soit $\pi_1, \ldots, \pi_m$ un système complet d'éléments premiers non associés de l'anneau $\mathfrak{D}$ (ordonnés de telle sorte que $\nu_i(\pi_i) = 1$). Puisque $\mathfrak{O} \subset \mathfrak{D}$, alors l'élément p admet dans l'anneau $\mathfrak{D}$ la décomposition

$$p = \varepsilon \pi_1^{e_1} \ldots \pi_m^{e_m}, \tag{7}$$

avec des exposants e_i positifs (ε est une unité de $\mathfrak{D}$). Si maintenant a est un certain élément de k^* tel que $\nu_0(a) = s$, i. e. $a = p^s u$, où u est une unité de $\mathfrak{O}$ et par suite aussi de $\mathfrak{D}$, alors

$$\nu_i(U) = e_i s = e_i \nu_0(a). \tag{8}$$

Si $e_i = 0$; alors toutes les valeurs de la valuation ν_i sur k^* seraient nulles et c'est impossible comme nous l'avons vu; par suite $e_i > 0$. La formule (8) montre alors que toutes les valuations ν_i $(i = 1, \ldots, m)$ sont des prolongements de ν_0 au corps K. Nous avons obtenu en même temps que l'indice de ramification de la valuation ν_i par rapport à ν_0 est défini par la décomposition (7).

Supposons maintenant que ν est un prolongement de la valuation ν_0 au corps K. Puisque $\mathfrak{O}$ est contenu dans l'anneau de la valuation Y, alors cet anneau contient aussi $\mathfrak{D}$, i. e. $\nu(\alpha) \geqslant 0$ pour tout $\alpha \in \mathfrak{D}$ et par suite $\nu(\varepsilon) = 0$ pour toute unité $\varepsilon \in \mathfrak{D}$. Si la valuation ν était différente de $\nu_1, \ldots, \nu_m$ alors, d'après le théorème 3, il existe une unité ε de l'anneau $\mathfrak{D}$ telle que $\nu(\varepsilon) \neq 0$. La contradiction obtenue montre que ν est égal à un des ν_i.

Ainsi, les seuls prolongements de la valuation ν_0 au corps K sont les valuations $\nu_1, \ldots, \nu_m$. D'après la condition 2) du théorème 4 du § 3, nous obtenons ainsi que la fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{O}$ dans le corps K est l'ensemble des éléments $\alpha \in K$ tels que $\nu_i(\alpha) \geqslant 0$ pour tous les prolongements ν_i. Si on désigne, comme ci-dessus, par $\mathfrak{D}_i$ l'anneau de la valuation ν_i, alors on peut écrire ce dernier résultat sous la forme

$$\mathfrak{D} = \bigcap_{i=1}^{m} \mathfrak{D}_i. \tag{9}$$

Le raisonnement ci-dessus nous montre que pour démontrer l'existence de prolongements de la valuation ν_0 au corps K et les décrire complètement, il suffit d'établir qu'il y a unicité de la décomposition en facteurs premiers dans l'anneau $\mathfrak{D}$ (avec un nombre fini d'éléments premiers non associés).

4) Existence des prolongements

Soient comme ci-dessus k un corps quelconque, ν_0 une valuation de k, $\mathfrak{O}$ l'anneau de la valuation ν_0 et p un élément premier de l'anneau $\mathfrak{O}$. Pour tout élément $a \in \mathfrak{O}$, nous désignerons par $\bar{a}$ la classe résiduelle modulo p. L'égalité $\bar{a} = \bar{b}$ dans le corps Σ_0 équivaut donc à $a \equiv b \pmod{p}$ dans l'anneau $\mathfrak{O}$.

Soit maintenant K une extension finie quelconque du corps k et désignons par $\mathfrak{D}$ la fermeture intégrale de l'anneau $\mathfrak{O}$ dans le corps K.

LEMME 2. — *Si le nombre d'éléments du corps résiduel Σ_0 de la valuation ν_0 est supérieur ou égal au degré de l'extension* $(K : k)$ *(en particulier si le corps Σ_0 est infini), alors l'anneau $\mathfrak{D}$ est euclidien et par suite cet anneau il y a unicité de la décomposition en facteurs premiers; de plus, dans l'anneau $\mathfrak{D}$, il existe un nombre fini d'éléments premiers non associés deux à deux.*

DÉMONSTRATION. — Pour tout élément $\alpha \in K^*$, définissons la fonction $\| \alpha \|$ en posant

$$\| \alpha \| = 2^{\nu_0(N_{K/k}(\alpha))}.$$

Il est clair que cette fonction possède la propriété $\| \alpha\beta \| = \| \alpha \| . \| \beta \|$ *(a,* $\beta \in K^*$). En outre, $\| \alpha \|$ prend des valeurs entières pour tout $\alpha \in \mathfrak{D}^*$. Il faut démontrer que pour tout couple α et $\beta \neq 0$ de $\mathfrak{D}$, il existe $\xi \in \mathfrak{D}$ et $\rho \in \mathfrak{D}$ tels que

$$\alpha = \beta\xi + \rho \tag{10}$$

avec $\rho = 0$ ou bien $\| \rho \| < \| \beta \|$.

Si dans l'anneau $\mathfrak{D}$ l'élément α est divisible par β, i. e. $a = \beta\gamma$ avec $y \in \mathfrak{D}$, alors l'égalité (10) sera réalisée pour $\xi = y$ et $\rho = 0$. Supposons maintenant que α n'est pas divisible par β, i. e. que l'élément $y = \alpha\beta^{-1}$ n'appartient pas à $\mathfrak{D}$. Soit

$$f(t) = t^n + c_1 t^{n-1} + \ldots + c_n \qquad (c \in k)$$

le polynôme caractéristique de l'élément y dans l'extension K/k. Puisque $\gamma \notin \mathfrak{D}$, les coefficients c_i n'appartiennent pas tous à $\mathfrak{O}$. Si $\min\limits_{1 \leqslant i \leqslant n} \nu_0(c) = -r < 0$, alors tous les coefficients du polynôme $\varphi(t) = p^r f(t)$ appartiendront à l'anneau $\mathfrak{O}$ et l'un d'entre eux au moins est une unité dans $\mathfrak{O}$. Remplaçons tous les coefficients de $\varphi(t)$ par les classes résiduelles correspondantes

modulo p. Puisque le coefficient du terme de plus haut degré, égal à p^r, est divisible par p, nous obtenons ainsi un polynôme $\bar{\varphi}(t)$ de l'anneau $\Sigma_0[t]$ de degré $\leqslant n-1$ et dont tous les coefficients ne sont pas nuls. Le corps Σ_0, par hypothèse, contient au moins n éléments; il existe donc un élément $a \in \mathfrak{O}$ tel que sa classe résiduelle $\bar{a}$ ne soit pas une racine du polynôme $\bar{\varphi}(t)$. Ceci signifie que $\varphi(a) \not\equiv 0 \pmod{p}$, i. e. $\varphi(a)$ est une unité de l'anneau $\mathfrak{O}$. Calculons maintenant la valeur $\| y - a \|$. Le polynôme caractéristique de $y - a$ est égal à $f(t+a)$; par suite

$$N_{K/k}(\gamma - a) = (-1)^n f(a) = (-1)^n \varphi(a) p^{-r},$$

d'où

$$\| y - a \| = 2^{-r} < 1,$$
$$\| \alpha - \alpha\beta \| < \| \beta \|.$$

L'égalité (10) sera satisfaite si nous posons $\xi = a$, $\rho = \alpha - \alpha\beta$.

Nous avons ainsi démontré que $\mathfrak{D}$ est un anneau euclidien et par suite, d'après le théorème 2 du § 2 la décomposition en facteurs premiers y est définie de manière unique.

Soit π un élément premier quelconque de l'anneau $\mathfrak{D}$. Puisque, pour tout $a \in a>^*$, la norme $N_{K/k}(\alpha)$ est toujours divisible par a, alors $N_{K/k}(\pi) = p^f u$ est divisible par π (u est une unité dans $\mathfrak{O}$ etf $\geqslant 1$). Mais dans ce cas, puisque π est premier et que la décomposition en facteurs premiers est unique, p est divisible par π. Ceci démontre que si la décomposition de p en facteurs premiers dans l'anneau $\mathfrak{D}$ est de la forme

$$p = \varepsilon \pi_1^{e_1} \dots \pi_m^{e_m}$$

(ε est une unité de $\mathfrak{D}$), alors les éléments premiers $\pi_1, \dots, \pi_m$ forment un système complet d'éléments premiers non associés de $\mathfrak{D}$.

La démonstration du lemme 2 est terminée.

Démontrons maintenant les résultats fondamentaux de ce point.

THÉORÈME 5. — *Toute valuation v_0 d'un corps k admet un prolongement à toute extension finie K/k.*

THÉORÈME 6. — *Soit $\mathfrak{O}$ l'anneau de la valuation v_0 et soit $\mathfrak{D}$ la fermeture intégrale de l'anneau $\mathfrak{O}$ dans le corps K. Si $v_1, \dots, v_m$ sont tous les prolongements possibles de la valuation v_0 au corps K et $\mathfrak{D}_1, \dots, \mathfrak{D}_m$ leurs anneaux, alors*

$$\mathfrak{D} = \bigcap_{i=1}^{m} \mathfrak{D}_i.$$

THÉORÈME 7. -*Pour les mêmes notations, il y a unicité de la décomposition en facteurs premiers dans l'anneau $\mathfrak{D}$ et les valuations du corps K qui correspondent aux éléments premiers de $\mathfrak{D}$ coïncident avec les prolongements $v, \dots, v_m$*

de la valuation ν_0 au corps K. *Si $\pi_1, \ldots, \pi_m$ sont des éléments premiers de $\mathfrak{D}$ énumérés de telle sorte que $\nu_i(\pi_i) = 1$ et si l'élément premier $p \in \mathfrak{O}$ admet dans $\mathfrak{D}$ la décomposition*

$$p = \varepsilon_1 \pi_1^{e_1} \ldots \pi_m^{e_m} \qquad (\varepsilon \text{ est une unité de } \mathfrak{D}),$$

alors e_i est l'indice de ramification de ν_i par rapport à ν_0.

DÉMONSTRATION. — Si nous supposons que les théorèmes 5 et 6 ont déjà été démontrés, alors, d'après le corollaire du théorème 3, il y a unicité de la décomposition en facteurs premiers dans $\mathfrak{D}$ (avec un nombre fini de facteurs premiers non associés) et par suite tous les résultats obtenus dans la seconde partie de 3) s'appliquent à l'anneau $\mathfrak{D}$. Ces résultats constituent le théorème 7.

Nous démontrerons les théorèmes 5 et 6 par récurrence sur le degré n de l'extension K/k. Pour $n = 1$, il n'y a rien à démontrer. Soit $n > 1$ et supposons que les théorèmes 5 et 6 sont démontrés pour toute extension de degré $< n$ du corps fondamental k.

Si le corps résiduel Σ_0 de la valuation ν_0 contient au moins n éléments, alors, d'après le lemme 2, la décomposition en facteurs premiers dans l'anneau $\mathfrak{D}$ est définie de manière unique et, d'après 3), les théorèmes 5 et 6 sont démontrés (cf. égalité (9)). Il suffit donc de considérer le cas où le nombre q d'éléments du corps Σ_0 est fini et $< n$.

Nous ramènerons le cas général à celui-ci en construisant un corps $k' \supset k$ tel que le degré $(k' : k)$ soit égal à $n - 1$ (par hypothèse de récurrence, il existe alors une valuation ν_0' de k' qui prolonge ν_0) et tel que le corps résiduel Σ' de la valuation ν_0' contienne au moins n éléments. Si on désigne par K' le plus petit corps contenant à la fois K et k', alors les hypothèses du lemme 2 sont satisfaites pour l'extension K'/k' et la valuation ν_0', d'où le théorème.

Nous savons (cf. appendice § 3) que sur tout corps fini il existe des polynômes irréductibles de degré quelconque. Soit $\varphi(t)$ un polynôme irréductible de degré $n - 1$ à coefficients dans le corps Σ_0 et dont le coefficient du terme de plus haut degré est égal à $\bar{1}$. Chacun de ces coefficients est une classe résiduelle de l'anneau $\mathfrak{O}$ modulo p. Remplaçons chacune de ces classes par un de ses représentants (en prenant 1 pour coefficient dominant); nous obtenons un polynôme $\varphi(t) \in \mathfrak{O}[t]$ qui est irréductible sur le corps k. En effet, si $\varphi(t)$ était réductible sur k, alors il serait décomposable en facteurs à coefficients dans $\mathfrak{O}$ et, par passage au corps résiduel Σ_0, nous obtiendrons pour $\bar{\varphi}(t)$ une décomposition à coefficients dans Σ_0, ce qui contredit le choix de $\bar{\varphi}(t)$. Construisons l'extension K' = K(8) du corps K, θ racine du polynôme $\varphi(t)$. Le degré de l'extension K'/K ne dépasse pas $n - 1$ (le polynôme $cp(t)$ n'est

pas nécessairement irréductible sur le corps K). Considérons dans K' le corps conjugué $k' = k(\theta)$. Puisque $\varphi(t)$ est irréductible sur k, alors

$$(k' : k) = n - 1.$$

Soit ν_0' une valuation du corps k' qui prolonge ν_0 au corps k' (ν_0' existe par hypothèse de récurrence). Désignons par $\mathfrak{O}'$ l'anneau de la valuation ν_0', par p' un élément premier dans $\mathfrak{O}'$ et par Σ' le corps résiduel de l'anneau $\mathfrak{O}'$ modulo p'. Deux éléments a et b de $\mathfrak{O}$ sont congrus modulo p' (dans l'anneau 0') si et seulement s'ils sont congrus modulo p dans l'anneau $\mathfrak{O}$. Par suite, les classes résiduelles de l'anneau $\mathfrak{O}'$ modulo p' qui contiennent des éléments de $\mathfrak{O}$ forment un sous-corps du corps Σ', isomorphe à Σ_0. Ayant choisi un isomorphisme $\Sigma_0 \to \Sigma'$, on peut considérer que $\Sigma_0 \subset 8'$. Puisque l'élément θ' est une racine d'un polynôme à coefficients dans $\mathfrak{O}$, de coefficient dominant 1, alors $\theta \in \mathfrak{O}'$ (puisque $\mathfrak{O}'$ est intégralement clos). L'égalité $\varphi(\theta) = 0$ donne, par passage aux classes résiduelles modulo p', $\varphi(\theta) = \bar{0}$. Mais $\bar{\varphi}(t)$ a été choisi irréductible sur le corps Σ_0 et par suite les éléments $1, \theta, \ldots, \bar{\theta}^{n-2}$ sont linéairement indépendants sur Σ_0. Il en résulte facilement que le corps Σ' (i. e. le corps résiduel de la valuation ν_0') contient au moins q^{n-1} éléments (rappelons que q est le nombre d'éléments du corps Σ_0). Par ailleurs,

$$(K' \cdot k') = \frac{(K' : K)(K : k)}{(k' : k)} \leqslant \frac{(n-1)n}{n-1} = n.$$

Mais pour $q \geqslant 2$ et $n \geqslant 2$, on a l'inégalité

$$q^{n-1} \geqslant n;$$

par suite, le nombre d'éléments du corps résiduel Σ' de la valuation ν_0' n'est pas inférieur au degré (K' : k'). D'après ce qui a déjà été vu, il existe un prolongement ν' au corps K'. Puisque Y' est un prolongement de ν_0' au corps K', alors la valuation ν induite par la valuation ν' sur le sous-corps K est un prolongement de la valuation ν_0 (cf. 3)). Cela termine la démonstration du théorème 5.

Pour démontrer le théorème 6, il faut vérifier tout d'abord que ν_0' est l'unique prolongement de la valuation ν_0 au corps k'. Supposons donc qu'il existe un autre prolongement ν_0'' de ν_0 au corps k'. D'après le théorème 3, il existe un élément $y \in k'$ tel que $\nu_0'(\gamma) = 0$ et $\nu_0''(\gamma) > 0$. Puisque les puissances $1, \theta, \ldots. \theta^{n-2}$ forment une base de k' sur k, nous écrirons l'élément y sous la forme

$$\gamma = p^k(c_0 + c_1\theta + \ldots + c_{n-2}\theta^{n-2}) = p^k\alpha,$$

où tous les coefficients $c_i \in \mathfrak{O}$, l'un d'eux au moins étant une unité dans $\mathfrak{O}$. Nous avons vu ci-dessus que $\theta \in \mathfrak{O}'$ et que les classes résiduelles $1, \bar{\theta}, \ldots, \bar{\theta}^{n-2}$

de Σ' sont linéairement indépendantes sur Σ_0. Par suite, la classe résiduelle

$$a = \bar{c}_0 + \bar{c}_1\bar{\theta} + \ldots + \bar{c}_{n-2}\bar{\theta}^{n-2}$$

n'est pas nulle (puisqu'un au moins des coefficients $\bar{c}_i$ n'est pas nul). Cela signifie que α n'est pas divisible par p' (dans l'anneau $\mathfrak{O}'$) i. e. $v_0'(\alpha) = 0$. De manière analogue, on obtiendrait $v_0''(\alpha) = 0$. Rapprochant maintenant les conditions $v_0'(\gamma) = 0$, $v_0'(\alpha) = 0$ de l'égalité $y = p^k\alpha$, nous voyons que $k = 0$ et par suite $v_0''(\gamma) = v_0''(\alpha) = 0$, en contradiction avec le choix de y. Ainsi la valuation v_0 admet un seul prolongement au corps k'.

Puisque le théorème 6 est vrai par hypothèse de récurrence pour l'extension k'/k, alors l'anneau $\mathfrak{O}'$ de la valuation v_0' coïncide avec la fermeture intégrale de l'anneau $\mathfrak{O}$ dans le corps k'. Désignons par $\mathfrak{D}'$ la fermeture intégrale de l'anneau $\mathfrak{O}$ dans le corps K'. Puisque $\mathfrak{O}' \subset \mathfrak{D}'$ et puisque l'anneau $\mathfrak{D}'$ est intégralement fermé dans K' (appendice § 4-3)), alors $\mathfrak{D}'$ est aussi la fermeture intégrale de l'anneau $\mathfrak{O}'$ dans le corps K'. Soient $v_1', \ldots, v_r'$ tous les prolongements de la valuation v_0' au corps K' et $\mathfrak{D}_1', \ldots, \mathfrak{D}_r'$ leurs anneaux. Puisque le théorème 6 est vrai pour l'extension K'/k' et la valuation v_0' (les hypothèses du lemme 2 sont satisfaites), alors

$$\mathfrak{D}' = \bigcap_{j=1}^{r} \mathfrak{D}_j'. \tag{11}$$

Le système des valuations v_j' est aussi l'ensemble de tous les prolongements de la valuation v_0 au corps K'. C'est pourquoi l'égalité (11) est l'argument du théorème 6 pour l'extension K'/k (et pour la valuation v).

Désignons par $v_1, \ldots, v_m$ toutes les valuations du corps K induites sur K par une des valuations v_j' et par $\mathfrak{D}_1, \ldots, \mathfrak{D}_m$ leurs anneaux. Si v_j' est un prolongement de v_i, il est clair que $\mathfrak{D}_j' \cap K = \mathfrak{D}_i$. Remarquant maintenant que l'intersection $\mathfrak{D}' \cap K$ coïncide avec la fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{O}$ dans le corps K, nous obtenons

$$\mathfrak{D} = \mathfrak{D}' \cap K = \bigcap_{j=1}^{r} (\mathfrak{D}_j' \cap K) = \bigcap_{i=1}^{m} \mathfrak{D}_i. \tag{12}$$

S'il existait dans le corps K une valuation v différente de $v_1, \ldots, v$, et qui soit un prolongement de v_0, alors, d'après le théorème 3, il existerait dans K un élément a tel que $v_1(\alpha) \geqslant 0, \ldots, v_m(\alpha) \geqslant 0$ (cela signifie que $\alpha \in \mathfrak{D}$) et $v(\alpha) < 0$. Cela contredit l'inclusion $\mathfrak{D} \subset \mathfrak{D}_v$, $\mathfrak{D}_v$ anneau de la valuation v. Ainsi $v_1, \ldots, v_m$ épuisent tous les prolongements de la valuation v_0 au corps K. La formule (12) coïncide avec l'argument du théorème 6.

EXERCICES

1. Démontrer que sur les corps algébriquement clos il n'existe pas de valuation.

2. Soient K = k(x) le corps des fonctions rationnelles sur un corps k et ν la valuation du corps K qui correspond au polynôme $x - a$ $(a \in k)$. Démontrer que le corps résiduel Σ_ν de la valuation v est isomorphe à k. Démontrer que deux éléments f(x) et g(x) de l'anneau de la valuation ν appartiennent à la même classe résiduelle si et seulement si $f(a) = g(u)$.

3. Soit K = $k(x)$ le corps des fonctions rationnelles sur le corps k des nombres réels et soit ν la valuation de K qui correspond au polynôme irréductible $x^2 + 1$. Déterminer le corps résiduel Σ_ν de la valuation Y.

4. Soient $\mathfrak{D}_1$ et $\mathfrak{D}_2$ les anneaux de deux valuations ν_1 et ν_2 d'un corps K. Montrer que si $\mathfrak{D}_1 \subset \mathfrak{D}_2$, alors $\nu_1 = \nu_2$.

5. Trouver la fermeture intégrale de l'anneau des nombres entiers 3-adiques dans le corps $\mathbf{Q}(\sqrt{-5})$ et déterminer tous les prolongements de la valuation 3-adique à ce corps.

6. Pour tout nombre premier p, déterminer tous les prolongements de la valuation p-adique ν_p au corps $\mathbf{Q}(\sqrt{-1})$ et trouver les indices de ramification correspondants.

7. Soient K/k une extension normale et ν_0 une valuation du corps k. Montrer que si ν est un certain prolongement de ν_0 au corps K, alors tous les autres prolongements sont de la forme

$$\nu'(\alpha) = \nu(\sigma(\alpha)), \qquad \alpha \in K,$$

où σ parcourt tous les automorphismes de K/k.

8. Soit k un corps de Caractéristique~. Démontrer que si une extension finie K/k est strictement non séparable, alors toute valuation du corps k admet un seul prolongement au corps K (une extension K/k est dite strictement non séparable si tout élément de K est racine d'ordre p^s d'un certain élément du corps k).

9. Soit $k = k_0(x, y)$ le corps des fonctions rationnelles en x et y sur un corps k_0. Dans le corps $k_0\{t\}$ des séries formelles (cf. exercice 7, chap. I[er], § 4 ou chap. IV, §1-5)), choisissons une série $\xi(t) = \sum_{n=0}^{\infty} c_n t^n$ (c, $\in k$,) transcendante sur le corps $k_0(t)$ des fonctions rationnelles (l'existence de telles séries résulte du fait que la puissance de l'ensemble $k_0\{t\}$ est supérieure à la puissance de k,(t) et par suite à la puissance de l'ensemble des éléments de $k_0\{t\}$ qui sont algébriques sur $k_0(t)$). D'après le choix de ξ, pour tout polynôme non nul $f = f(x, y) \in k[x, y]$ la série $f(t, \xi(t))$ est aussi non nulle. Si t^n est la plus petite puissance de t figurant dans cette série, posons $\nu_0(f) = n$. Montrer que la fonction ν_0 est une valuation du corps k et que le corps résiduel de cette valuation est isomorphe au corps k_0.

§ 5. — THEORIE DES DIVISEURS POUR UNE EXTENSION FINIE

1) Existence

THÉORÈME 1. — ***Soit un anneau*** $\mathfrak{O}$, ***de corps des fractions k, admettant une théorie des diviseurs*** $\mathfrak{O}^* \to A$,, ***définie par un ensemble*** $\mathfrak{R}_0$ ***de valuations. Si*** K ***est une extension finie du corps k, alors l'ensemble*** $\mathfrak{R}$ ***de toutes les valuations du corps*** K ***qui sont des prolongements des valuations de*** $\mathfrak{R}_0$ ***définit une théorie des diviseurs pour la fermeture intégrale*** $\mathfrak{D}$ ***de l'anneau*** $\mathfrak{O}$ ***dans le corps*** K.

DÉMONSTRATION. — D'après le théorème 4 du § 3, il suffit de vérifier que l'ensemble $\mathfrak{R}$ satisfait aux trois conditions de ce théorème. Vérifions tout d'abord la seconde. Pour toute valuation $\nu \in \mathfrak{R}$ et tout $a \in \mathfrak{O}$, il est clair que l'on a $\nu(a) \geqslant 0$. Cela signifie que $\mathfrak{O}$ est contenu dans l'anneau de la valuation Y. Mais alors, d'après le théorème 1 du § 4, la fermeture intégrale de l'anneau $\mathfrak{O}$ dans le corps K est aussi contenu dans l'anneau de la valuation v. Autrement dit, v(a) $\geqslant$ 0 pour tout a $\in \mathfrak{D}$. Réciproquement, soit $a \in$ K tel que $\nu(a) \geq 0$ pour toutes les valuations $\nu \in \mathfrak{R}$. Désignons par

$$t^r + a_1 t^{r-1} + \ldots + a_r$$

le polynôme minimal de a sur k; soit ν_0 une valuation du corps k appartenant à l'ensemble $\mathfrak{R}_0$ et soient $\nu_1, \ldots, \nu_m$ tous ses prolongements au corps K. Puisque $\nu_1(\alpha) \geqslant 0, \ldots, \nu_m(a) \geqslant 0$, alors, d'après le théorème 6 du § 4 l'élément a appartient à la fermeture intégrale dans K de l'anneau de la valuation ν_0. Mais alors tous les coefficients $a_1, \ldots, a_r$ appartiennent à l'anneau de la valuation ν_0 (cf. appendice § 4-3)), i. e. $\nu_0(a_1) \geqslant 0, \ldots, \nu_0(a_r) \geqslant 0$. Puisque ces inégalités sont satisfaites pour tout $\nu_0 \in \mathfrak{R}_0$, les coefficients $a_1, \ldots, a_r$ appartiennent à $\mathfrak{O}$, i. e. $a \in \mathfrak{D}$.

Revenons à la première condition. Soit $a \in \mathfrak{D}$, $a \neq 0$. Il existe seulement un nombre fini de valuations $\nu_0 \in \mathfrak{R}_0$ telles que $\nu_0(a_r) \neq 0$. Il en résulte qu'il existe seulement un nombre fini de valuations $\nu \in \mathfrak{R}$ telles que $\nu(a_r) \neq 0$. Mais si $\nu(a_r) = 0$, l'inégalité $\nu(a) \geqslant 0$ entraîne aussi

$$\nu(\alpha^{-1}) = \nu(a_r^{-1}(\alpha^{r-1} + \ldots + a_{r-1})) \geqslant 0,$$

et par suite $\nu(a) = 0$. Ainsi $\nu(a) = 0$ pour presque tout $\nu \in \mathfrak{R}$.

Il reste à vérifier que la troisième condition est remplie. Supposons que $\nu_1, \ldots, \nu_m$ sont des valuations distinctes de $\mathfrak{R}$ et $k_1, \ldots, k_m$ des nombres entiers positifs. Désignons par $\nu_{01}, \ldots, \nu_{0m}$ les valuations de $\mathfrak{R}_0$ correspondantes (certaines de ces valuations peuvent être égales). Ajoutons à notre

système initial de valuations tous les prolongements des ν_{0i} au corps K, soient $\nu_1, \ldots, \nu_m, \nu_{m+1}, \ldots, \nu_s$. D'après le théorème 3 du § 4, il existe un élément $y \in K$ tel que $\nu_1(\gamma) = k_1, \ldots, \nu_m(y) = k_m, \nu_{m+1}(\gamma) = 0, \ldots, \nu_s(\gamma) = 0$. Si cet élément y appartient à l'anneau $\mathfrak{D}$, nous poserons $\alpha = y$. Si $y \notin \mathfrak{D}$, désignons par $\nu'_1, \ldots, \nu'_r$ toutes les valuations de $\mathfrak{R}$ qui prennent des valeurs négatives sur l'élément y :

$$\nu'_1(\gamma) = -l_1, \ldots, \nu'_r(\gamma) = -l_r,$$

et par $\nu'_{01}, \ldots, \nu'_{0r}$ les valuations correspondantes de $\mathfrak{R}_0$ (certaines de ces valuations peuvent être égales). Puisque chacune des valuations ν'_{0j} est différente de chacune des ν_{0i}, il existe dans $\mathfrak{O}$ un élément a tel que

$$\nu_{0i}(a) = 0 \ (1 \leqslant i \leqslant m), \qquad \nu'_{0j}(a) = l \ (1 \leqslant j \leqslant r),$$

où $l = \max(l_1, \ldots, l_r)$. Posons $\alpha = \gamma a$. Puisque

$$\nu'_j(\alpha) = \nu_j(\gamma) + \nu'_j(a) \geqslant -l_j + \nu'_{0j}(a) = -l_j + l \geqslant 0,$$

alors $\alpha \in \mathfrak{D}$. Ainsi, dans ces deux cas, on a trouvé un élément $a \in \mathfrak{D}$ tel que $\nu_1(\alpha) = k_1, \ldots, \nu_m(\alpha) = k_m$; la condition 3 du théorème 4 du § 3 est satisfaite pour l'ensemble des valuations $\mathfrak{R}$. Ceci termine la démonstration du théorème 1.

Appliquons le théorème 1 au cas d'un corps de nombres algébriques.

L'ordre maximum $\mathfrak{D}$ d'un corps K de nombres algébriques est, comme nous le savons, la fermeture intégrale dans K de l'anneau $\mathbf{Z}$ des nombres entiers rationnels. Puisqu'il existe pour $\mathbf{Z}$ une théorie des diviseurs (unicité de la décomposition en facteurs premiers), alors, d'après le théorème 1, il existe une théorie des diviseurs pour $\mathfrak{D}$. D'après le théorème 5 du § 3, la théorie des diviseurs pour $\mathbf{Z}$ est liée à l'ensemble de toutes les valuations du corps Q des nombres rationnels et puisque toute valuation du corps K est un prolongement d'une certaine valuation du corps $\mathbf{Q}$, nous obtenons que l'ensemble de toutes les valuations du corps K définit une théorie des diviseurs pour l'anneau $\mathfrak{D}$. Nous avons établi le résultat suivant.

THÉORÈME 2. — *L'ordre maximum $\mathfrak{D}$ d'un corps* K *de nombres algébriques admet une théorie des diviseurs $\mathfrak{D}^* \to \Delta$ et cette théorie est définie par l'ensemble de toutes les valuations du corps* K.

2) Norme des diviseurs

Soit k le corps des fractions d'un anneau $\mathfrak{O}$ admettant une théorie des diviseurs $\mathfrak{O}^* \to A$,; soient K une extension finie du corps k, $\mathfrak{D}$ la fermeture intégrale de l'anneau $\mathfrak{O}$ dans le corps K et $\mathfrak{D}^* \to \mathbf{A}$ une théorie des diviseurs

pour l'anneau $\mathfrak{D}$. Nous mettrons ici en évidence certains liens entre les monoïdes $A_{,,}$ et A.

Puisque $\mathfrak{O} \subset \mathfrak{D}$, aux éléments de $\mathfrak{O}^*$ correspondent des diviseurs principaux à la fois dans le monoïde $A_{,,}$ et dans le monoïde A. Pour les distinguer, nous désignerons par $(a)_k$ le diviseur principal de $A_{,,}$ correspondant à $a \in \mathfrak{O}^*$ et par $(\alpha)_K$ le diviseur principal de A correspondant à $\alpha \in a)^*$.

Nous avons l'inclusion $\mathfrak{O}^* \to \mathfrak{D}^*$. Puisque les unités de l'anneau $\mathfrak{D}$ contenues dans $\mathfrak{O}$ coïncident avec les unités de l'anneau $\mathfrak{O}$, cette inclusion définit un isomorphisme $(a)_k \to (a)_K$, $a \in \mathfrak{O}^*$, du monoïde des diviseurs principaux de l'anneau $\mathfrak{O}$ dans le monoïde des diviseurs principaux de l'anneau $\mathfrak{D}$. Montrons que cet isomorphisme se prolonge en un isomorphisme $\Delta_0 \to A$.

THÉORÈME 3. — *Il existe un isomorphisme du monoïde Δ_0 dans le monoïde* A *qui coïncide sur les diviseurs principaux avec l'isomorphisme $(a)_k \to (a)_{,,}$ $a \in \mathfrak{O}^*$.*

L'isomorphisme $\Delta_0 \to A$ est caractérisé par la commutativité du diagramme

$$\begin{array}{ccc} \mathfrak{O}^* & \to & \mathfrak{D}^* \\ \downarrow & & \downarrow \\ A_{,,} & \to & A \end{array}$$

i. e. les isomorphismes composés $\mathfrak{O}^* \to \mathfrak{D}^* \to A$ et $\mathfrak{O}^* \to \Delta_0 \to A$ coïncident (les flèches verticales indiquent les isomorphismes des monoïdes multiplicatifs des anneaux sur les monoïdes des diviseurs principaux correspondants).

Soient $\mathfrak{p}$ un diviseur premier de l'anneau $\mathfrak{O}$, $\nu_\mathfrak{p}$ la valuation correspondante du corps k et $\nu_{\mathfrak{P}_1}, \ldots \nu_{\mathfrak{P}_m}$ tous les prolongements de $\nu_\mathfrak{p}$ au corps K ($\mathfrak{P}_1, \ldots \mathfrak{P}_m$ sont des diviseurs premiers de l'anneau $\mathfrak{D}$). Désignons par $e_1, \ldots e_m$ respectivement les indices de ramification des valuations $\nu_{\mathfrak{P}_1}, \ldots \nu_{\mathfrak{P}_m}$ par rapport à $\nu_\mathfrak{p}$. Puisque $\nu_{\mathfrak{P}_i}(a) = e_i \nu_\mathfrak{p}(a)$ pour tout $a \in \mathfrak{O}^*$, alors au facteur $\mathfrak{p}^{\nu_\mathfrak{p}(a)}$ du diviseur principal $(a)_k \in A_{,,}$ correspondra le produit $(\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_m^{e_m})^{\nu_\mathfrak{p}(a)}$. L'isomorphisme $A_{,,} \to A$, défini par l'application

$$\mathfrak{p} \to \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_m^{e_m} \tag{1}$$

(pour tout p), satisfait aux conditions du théorème 3.

Il est facile de démontrer que l'isomorphisme $A_{,,} \to A$ satisfaisant aux exigences du théorème 3 est unique (exercice 5).

D'après l'isomorphisme $\Delta_0 \to A$, on peut identifier le monoïde Δ_0 à son image dans le monoïde A. Dans une telle identification cependant, les diviseurs premiers de $A_{,,}$ cessent en général d'être premiers dans A. En fait,

d'après (1), tout diviseur premier $\mathfrak{p} \in A_{\mathfrak{p}}$ admet dans le monoïde A la décomposition :

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_m^{e_m}. \tag{2}$$

En utilisant l'inclusion $A_{\mathfrak{p}} \to A$ on peut parler de divisibilité des diviseurs de l'anneau $\mathfrak{O}$ par des diviseurs de l'anneau $\mathfrak{D}$. En particulier, d'après (2), nous obtenons que les diviseurs premiers $\mathfrak{P}$ de l'anneau $\mathfrak{D}$ qui divisent un diviseur premier $\mathfrak{p}$ de l'anneau $\mathfrak{O}$ sont caractérisés par le fait que les valuations $v_{\mathfrak{P}}$ qui leur correspondent sont des prolongements de la valuation $v_{\mathfrak{p}}$. Il est clair que des diviseurs premiers entre eux dans Δ_0 restent aussi premiers entre eux dans A.

DÉFINITION. — ***Soit $\mathfrak{P}|\mathfrak{p}$. L'indice de ramification $e = e_{\mathfrak{P}}$ de la valuation $v_{\mathfrak{P}}$ par rapport à la valuation $v_{\mathfrak{p}}$ est aussi appelé l'indice de ramification du diviseur premier $\mathfrak{P}$ par rapport*** à p (ou par rapport à ***k).***

Ainsi, l'indice de ramification est le plus grand entier naturel e tel que $\mathfrak{P}^e | \mathfrak{p}$.

Pour tout élément $\alpha \in \mathfrak{D}^*$, sa norme $N(a) = N_{K/k}(\alpha)$ appartient à $\mathfrak{O}^*$. L'application $a \to N(a)$, $a \in \mathfrak{D}^*$, est un homomorphisme du monoïde multiplicatif $\mathfrak{D}^*$ dans le monoïde $\mathfrak{O}^*$. Puisque la norme de toute unité de l'anneau $\mathfrak{D}^*$ est une unité de $\mathfrak{O}^*$, cet homomorphisme définit de manière unique un homomorphisme $(a) \to (N(\alpha))_k$ du monoïde des diviseurs principaux de l'anneau $\mathfrak{D}$ dans le monoïde des diviseurs principaux de l'anneau $\mathfrak{O}$. Montrons que l'on peut le prolonger en un homomorphisme de tout le monoïde A dans $A_{\mathfrak{p}}$.

THÉORÈME 4. — ***Il existe un homomorphisme $N : A \to A_{\mathfrak{p}}$, des monoïdes de diviseurs*** A ***et*** A, ***tel que***

$$N((\alpha)_K) = (N_{K/k}(\alpha))_k \tag{3}$$

pour tout $\alpha \in \mathfrak{D}^*$.

La propriété (3) de l'homomorphisme N exprime que le diagramme

$$\begin{array}{ccc} \mathfrak{D}^* & \xrightarrow{N} & \mathfrak{O}^* \\ \downarrow & & \downarrow \\ \Delta & \xrightarrow{N} & \Delta_0 \end{array}$$

est commutatif.

Pour un diviseur premier $\mathfrak{p} \in A_{\mathfrak{p}}$, désignons par $\mathfrak{O}_{\mathfrak{p}}$ l'anneau de la valuation $v_{\mathfrak{p}}$ et par $\mathfrak{D}_{\mathfrak{p}}$ sa fermeture intégrale dans le corps K. D'après le théorème 7 du paragraphe 4, tous les diviseurs premiers $\mathfrak{P}_1, \dots, \mathfrak{P}_m$ de l'anneau $\mathfrak{D}$ qui divisent $\mathfrak{p}$ sont en correspondance biunivoque avec des éléments premiers $\pi_1, \dots, \pi_m$ non associés deux à deux de l'anneau $\mathfrak{D}_{\mathfrak{p}}$. Cette correspondance $\mathfrak{P}_i \leftrightarrow \pi_i$ est telle que, si un élément $a \neq 0$ de K admet la décomposition

$$a = \varepsilon \pi_1^{k_1} \dots \pi_m^{k_m}, \tag{4}$$

où ε est unité de l'anneau $\mathfrak{D}_\mathfrak{p}$, alors

$$k_i = \nu_{\mathfrak{P}_i}(\alpha). \tag{5}$$

Soit $\mathfrak{P}$ un des diviseurs premiers $\mathfrak{P}_i$ qui divisent p et soit π l'élément premier de l'anneau $\mathfrak{D}_\mathfrak{p}$ qui lui correspond. Posons

$$d_\mathfrak{P} = \nu_\mathfrak{p}(N_{K/k}(\pi)). \tag{6}$$

II est clair que $d_\mathfrak{P}$ ne dépend pas du choix de π. Prenant les normes dans l'égalité (4) et appliquant (5) et (6), nous obtenons

$$\nu_\mathfrak{p}(N_{K/k}(\alpha)) = \sum_{\mathfrak{P}\mid\mathfrak{p}} d_\mathfrak{P}\nu_\mathfrak{P}(\alpha) \tag{7}$$

($\mathfrak{P}$ parcourt tous les diviseurs premiers de l'anneau $\mathfrak{D}$ qui divisent p).

Nous pouvons maintenant facilement construire l'homomorphisme

$$N : A \to \Delta_0$$

défini dans le théorème 4. Nous écrirons tout diviseur $\mathfrak{U} = \mathfrak{P}_1^{A_1} \ldots \mathfrak{P}_r^{A_r}$ du monoïde A sous forme d'un produit formel infini

$$\mathfrak{U} = \prod_\mathfrak{P} \mathfrak{P}^{A(\mathfrak{P})}$$

étendu à tous les diviseurs premiers $\mathfrak{P}$ de A, un nombre fini seulement des valuations positives A(Q) étant différentes de zéro (A(!@) est égal à A_i si $\mathfrak{P} = \mathfrak{P}_i$ et à zéro si le diviseur $\mathfrak{P}$ est différent de $\mathfrak{P}_i, \ldots, \mathfrak{P}_r$). On peut écrire de manière analogue les diviseurs de l'anneau $\mathfrak{O}$.

Pour l'élément $a \in \mathfrak{D}^*$, considérons le diviseur principal $(\alpha)_K$. Puisque le diviseur premier $\mathfrak{P}$ figure dans $(\alpha)_K$ avec l'exposant $\nu_\mathfrak{p}(\alpha)$, alors

$$(a), = \prod_\mathfrak{P} \mathfrak{P}^{\nu_\mathfrak{P}(\alpha)}. \tag{8}$$

D'après (7), les exposants c(p) du diviseur principal

$$(N(\alpha))_k = \prod_P p^{c(p)} \tag{9}$$

sont donnés par la formule

$$c(p) = \sum_{\mathfrak{P}\mid\mathfrak{p}} d_\mathfrak{P}\nu_\mathfrak{P}(\alpha). \tag{10}$$

Cela nous conduit à la définition suivante.

DÉFINITION. *Soit* $\mathfrak{U} = \prod_{\mathfrak{P}} \mathfrak{P}^{A(\mathfrak{P})}$ *un diviseur de l'anneau* $\mathfrak{D}$. *Pour tout diviseur premier* $\mathfrak{p}$ *de l'anneau* $\mathfrak{O}$, *posons*

$$a(\mathfrak{p}) = \sum_{\mathfrak{P} \mid \mathfrak{p}} d_{\mathfrak{P}} A(\mathfrak{P}).$$

Le diviseur $\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ *de l'anneau* $\mathfrak{O}$ *est appelé norme du diviseur* $\mathfrak{U}$ *pour l'extension* K/k *et est désigné par* $N_{K/k}(\mathfrak{U})$ *ou plus simplement par* $N(\mathfrak{U})$.

Puisque les nombres $A(\mathfrak{P})$ sont nuls pour presque tout $\mathfrak{P}$ (i. e. pour tous sauf un nombre fini) alors les $a(\mathfrak{p})$ sont nuls pour presque tout $\mathfrak{p}$ et par suite $\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ est un diviseur de l'anneau $\mathfrak{O}$.

Il résulte de manière évidente de la définition que

$$N(\mathfrak{U}\mathfrak{P}) = N(\mathfrak{U})N(\mathfrak{P}),$$

pour des diviseurs quelconques 'U et $\mathfrak{P}$ de A. L'application $\mathfrak{U} \to N(\mathfrak{U})$ est donc un homomorphisme du monoïde A dans le monoïde A,,.

Dans le cas d'un diviseur premier $\mathfrak{U} = \mathfrak{P}$, nous avons

$$N(\mathfrak{r})) = \mathfrak{p}^{d_{\mathfrak{P}}} \qquad (\mathfrak{P} \mid \mathfrak{p}). \tag{11}$$

Puisque, d'après l'égalité (10), la norme du diviseur (8) est égale au diviseur (9), nous avons établi l'existence d'un homomorphisme N : A $\to$ A,, satisfaisant à la condition (3).

Un des problèmes essentiels de la théorie des diviseurs est l'étude des lois de décomposition des diviseurs premiers $\mathfrak{p}$ de l'anneau $\mathfrak{O}$ en facteurs premiers par passage à la fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{O}$ dans une extension finie. Dans le cas général, on connaît peu de résultats à ce sujet (cf. fin du § 8-2)). Toute décomposition du type (2) est caractérisée par le nombre m de diviseurs premiers $\mathfrak{P}_i$ et par les indices de ramifications $e_i = e_{\mathfrak{P}_i}$. Les nombres naturels $e_{\mathfrak{P}}$ ne sont pas arbitraires (pour une extension K/k donnée); en fait, ils sont liés aux nombres $d_{\mathfrak{P}}$ (cf. 6)) par la relation

$$\sum_{\mathfrak{P} \mid \mathfrak{p}} d_{\mathfrak{P}} e_{\mathfrak{P}} = n = (K : k), \tag{12}$$

dont la démonstration s'obtient en appliquant la formule (7) à l'élément premier $\mathfrak{p}$ de l'anneau $\mathfrak{O}_{\mathfrak{p}}$ (rappelons que $v_{\mathfrak{P}_i}(\mathfrak{p}) = e_i$).

3) Degrés résiduels

La définition de l'homomorphisme N : A $\to$ A, utilise les nombres $d_{\mathfrak{P}}$ qui sont définis par la formule (6). Nous allons préciser ici la signification arithmétique de ces nombres.

Soit $\mathfrak{P}|\mathfrak{p}$. Désignons par $\mathfrak{O}_{\mathfrak{p}}$ et par $\mathfrak{D}_{\mathfrak{P}}$ respectivement les anneaux des valuations $v_{\mathfrak{p}}$ et $v_{\mathfrak{P}}$, et par p et π des éléments premiers de ces anneaux. Puisque pour des éléments a et b de $\mathfrak{O}_{\mathfrak{p}}$ les congruences $a \equiv b \pmod{p}$ dans l'anneau $\mathfrak{O}_{\mathfrak{p}}$ et $a \equiv b \pmod{\pi}$ dans l'anneau $\mathfrak{D}_{\mathfrak{P}}$ sont équivalentes, alors, toute classe résiduelle modulo p dans $\mathfrak{O}_{\mathfrak{p}}$ est entièrement contenue dans une classe résiduelle de $\mathfrak{O}_{\mathfrak{P}}$ modulo π. Ceci définit une inclusion isomorphe du corps résiduel $\Sigma_{\mathfrak{p}} = \mathfrak{O}_{\mathfrak{d}}/(p)$ de la valuation $v_{\mathfrak{p}}$ dans le corps résiduel $\Sigma_{\mathfrak{P}} = \mathfrak{D}_{\mathfrak{P}}/(\pi)$ de la valuation $v_{\mathfrak{P}}$; nous considérerons donc que $\Sigma_{\mathfrak{p}} \subset \Sigma_{\mathfrak{P}}$. Pour tout $\xi \in \mathfrak{D}_{\mathfrak{P}}$, désignons par $\bar{\xi}$ la classe résiduelle de ξ modulo π. Le sous-corps $\Sigma_{\mathfrak{p}}$ du corps $\Sigma_{\mathfrak{P}}$ est formé des classes résiduelles de la forme a, $\bar{a} \in \mathfrak{O}_{\mathfrak{p}}$. Supposons que les classes résiduelles $\bar{\omega}_1, \ldots, \bar{\omega}_m$ de $\Sigma_{\mathfrak{P}}$ ($\omega_i \in \mathfrak{D}_{\mathfrak{P}}$) sont linéairement indépendantes sur le corps $\Sigma_{\mathfrak{p}}$ et montrons qu'alors les représentants $\omega_1, \ldots, \omega_m$ de ces classes sont linéairement indépendants sur le corps k. Supposons qu'il n'en soit pas ainsi, i. e. que pour certains coefficients $a_i \in k$ non tous nuls on ait

$$a_1\omega_1 + \ldots + a_m\omega_m = 0.$$

Multipliant cette relation par une puissance convenable de p, nous pouvons supposer que tous les a_i appartiennent à l'anneau $\mathfrak{O}$ et que l'un au moins d'entre eux n'est pas divisible par p. Passant au corps résiduel $\Sigma_{\mathfrak{P}}$ nous obtenons alors l'égalité

$$\bar{a}_1\bar{\omega}_1 + \ldots + \bar{a}_m\bar{\omega}_m = \bar{0},$$

dans laquelle tous les $\bar{a}_i \in \Sigma_{\mathfrak{P}}$ ne sont pas nuls. La contradiction obtenue démontre notre argument.

De l'indépendance linéaire de $\omega_1, \ldots, \omega_m$ sur le corps k résulte que

$$m \leqslant n = (\mathrm{K} : k).$$

Ainsi, ***le corps résiduel $\Sigma_{\mathfrak{P}}$ est une extension finie du corps $\Sigma_{\mathfrak{p}}$ et pur suite***

$$(\Sigma_{\mathfrak{P}} : \Sigma_{\mathfrak{p}}) \leqslant (\mathrm{K} : k).$$

DÉFINITION. — ***Supposons que le diviseur premier $\mathfrak{P}$ de l'anneau $\mathfrak{D}$ divise le diviseur premier $\mathfrak{p}$ de l'anneau $\mathfrak{O}$. Le degré $f = f_{\mathfrak{P}} = (\Sigma_{\mathfrak{P}} : \Sigma_{\mathfrak{p}})$ du corps résiduel de lu valuation $v_{\mathfrak{p}}$ pur rapport au corps résiduel de lu valuation $v_{\mathfrak{p}}$ s'appelle le degré résiduel du diviseur premier $\mathfrak{P}$ pur rapport à $\mathfrak{p}$ (ou pur rapport à k).***

Désignons, comme dans 2), par $\mathfrak{D}_\mathfrak{p}$ la fermeture intégrale de l'anneau $\mathfrak{O}_\mathfrak{p}$ dans le corps K. Par analogie avec la notion de base fondamentale dans un corps de nombres algébriques, introduisons la définition suivante :

DÉFINITION. — ***Une base*** $\omega_1, \ldots, \omega_n$ ***de l'extension*** K/k ***sera appelée une base fondamentale de l'anneau*** $\mathfrak{D}_\mathfrak{p}$ ***sur*** $\mathfrak{O}_\mathfrak{p}$ ***si tous ses éléments appartiennent à*** $\mathfrak{D}_\mathfrak{p}$ ***et si tout élément*** $\alpha \in \mathfrak{D}_\mathfrak{p}$ ***s'écrit sous la forme***

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n \tag{13}$$

à coefficients $a_i \in \mathfrak{O}_\mathfrak{p}$.

Nous verrons ci-dessous que, dans le cas d'une extension K/k séparable, il existe toujours une base fondamentale de l'anneau $\mathfrak{D}_\mathfrak{p}$ (pour tout p). Par contre, d'après les exercices 11 et 12, pour certaines extensions non séparables, l'anneau $\mathfrak{D}_\mathfrak{p}$ peut ne pas avoir de base fondamentale sur $\mathfrak{O}_\mathfrak{p}$.

L'importance de la notion de base fondamentale est mise en évidence par le théorème suivant.

THÉORÈME 5. — ***Soit*** $\mathfrak{P}$ ***un diviseur de l'anneau*** $\mathfrak{D}$ ***qui divise*** $\mathfrak{p}$ ***et soit*** π ***l'élément premier de l'anneau*** $\mathfrak{D}_\mathfrak{p}$ ***qui lui correspond. Si l'anneau*** $\mathfrak{D}_\mathfrak{p}$ ***admet une base fondamentale sur l'anneau*** $\mathfrak{O}_\mathfrak{p}$ ***alors***

$$f_\mathfrak{P} = d_\mathfrak{P} = v_\mathfrak{p}(N_{K/k}(\pi)).$$

DÉMONSTRATION. — **L'élément premier** $\pi \in \mathfrak{D}_\mathfrak{p}$ **est aussi un élément premier de l'anneau** $\mathfrak{D}_\mathfrak{P}$. Montrons que, toute classe résiduelle $\bar{\xi}$ de l'anneau $\mathfrak{D}_\mathfrak{P}$ modulo π contient un représentant qui appartient à $\mathfrak{D}_\mathfrak{p}$, i. e. pour tout $\xi \in \mathfrak{D}_\mathfrak{P}$ il existe un élément $a \in \mathfrak{D}_\mathfrak{p}$ tel que

$$\xi \equiv \alpha \pmod{\pi}.$$

Soient $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_m$ les diviseurs premiers de l'anneau $\mathfrak{D}$ qui divisent $\mathfrak{p}$. D'après le théorème 6 du § 4, la condition $\gamma \in \mathfrak{D}_\mathfrak{p}$ équivaut au fait que $v_{\mathfrak{P}_i}(\gamma) \geqslant 0$ pour tout $i = 1, \ldots, m$. Ainsi, l'élément a cherché est défini par les conditions

$$v_\mathfrak{P}(\xi - \alpha) \geqslant 1,$$

$$v_{\mathfrak{P}_i}(\alpha) \geqslant 0 \qquad (i = 2, \ldots, m),$$

et pour établir son existence, il suffit d'appliquer le théorème 4 du § 4.

Soit maintenant $\omega_1, \ldots, \omega_n$ une base fondamentale de l'anneau $\mathfrak{D}_\mathfrak{p}$ sur $\mathfrak{O}_\mathfrak{p}$. D'après ce qui précède, tout élément de $\Sigma_\mathfrak{P}$ peut s'écrire sous la forme $\bar{w}, + \ldots + a_n\omega_n$, $a_i \in \mathfrak{O}_\mathfrak{p}$ et par suite $\bar{a}_i \in \Sigma_\mathfrak{p}$. Cela signifie que les classes résiduelles $\overline{\omega_1}, \ldots, \overline{\omega_n}$ sont des générateurs de l'espace vectoriel $\Sigma_\mathfrak{P}$ sur $\Sigma_\mathfrak{p}$. Si $f = (\Sigma_\mathfrak{P} : \Sigma_\mathfrak{p}) = f_\mathfrak{P}$, alors nous pouvons choisir f de ces classes qui soient

linéairement indépendantes sur $\Sigma_\mathfrak{p}$; supposons que ce soient $\overline{\omega_1}, \ldots, \overline{\omega_f}$. Il est clair qu'alors la congruence

$$a_1\omega_1 + \ldots + a_f\omega_f \equiv 0 \pmod{\pi}$$

pour $a_i \in \mathfrak{O}_\mathfrak{p}$ n'est satisfaite dans $\mathfrak{D}$ que si $a_i \equiv 0 \pmod{p}$ (p élément premier de l'anneau $\mathfrak{O}$).

Puisque toutes les classes résiduelles $\omega_j \in \Sigma_\mathfrak{P}$ pour $j = f + 1, \ldots, n$ s'expriment comme combinaisons linéaires de $\overline{\omega_1}, \ldots, \omega_f$, alors

$$\omega_j \equiv \sum_{s=1}^{f} b_{js}\omega_s \pmod{\pi} \qquad j = (f+1, \ldots, n)$$

pour des coefficients $b_{js} \in \mathfrak{O}_\mathfrak{p}$. Posons

$$\theta_i = \omega_i \qquad \text{pour} \quad i = 1, \ldots, f,$$

$$\theta_j = -\sum_{s=1}^{f} b_{js}\omega_s + \omega_j \quad \text{pour} \quad j = f+1, \ldots, n,$$

Il est clair que $\theta_1, \ldots, \theta_n$ forment aussi une base fondamentale de $\mathfrak{D}_\mathfrak{p}$ sur $\mathfrak{O}_\mathfrak{p}$ (puisque les ω_s s'expriment comme combinaison linéaire des θ_s à coefficients dans $\mathfrak{O}_\mathfrak{p}$). Tous les éléments $\theta_{f+1}, \ldots, \theta_n$ sont divisibles par π dans l'anneau $\mathfrak{D}_\mathfrak{p}$ par suite, la congruence

$$a_1\theta_1 + \ldots + a_n\theta_n \equiv 0 \pmod{\pi}$$

a lieu si et seulement si

$$a_1 \equiv \ldots \equiv a_f \equiv 0 \pmod{p}.$$

Considérons l'ensemble m de tous les éléments de l'anneau $\mathfrak{D}_\mathfrak{p}$ qui sont divisibles par π. D'après ce qui vient d'être démontré, l'ensemble m coïncide avec toutes les combinaisons linéaires des éléments

$$p\theta_1, \ldots, p\theta_f, \qquad \theta_{f+1}, \ldots, \theta_n \tag{14}$$

à coefficients dans $\mathfrak{O}_\mathfrak{p}$. D'autre part, il est clair que m coïncide aussi avec toutes les combinaisons linéaires des éléments

$$\pi\theta_1, \ldots, \pi\theta_n, \tag{15}$$

à coefficients dans $\mathfrak{O}_\mathfrak{p}$. Désignons par C la matrice de passage de la base (14) à la base (15) ; puisque chaque élément $\pi\theta_j$ a des composantes sur la base (14) qui appartiennent à $\mathfrak{O}_\mathfrak{p}$, alors $\det C \in \mathfrak{O}_\mathfrak{p}$. Par symétrie, c'est aussi vrai pour $\det(C^{-1})$. Ainsi, $\det C$ est une unité de l'anneau $\mathfrak{O}_\mathfrak{p}$, i. e. $\nu_\mathfrak{p}(\det C) = 0$.

Si nous multiplions par p lesfpremières colonnes de C, nous obtenons alors la matrice A = (a_{ij}) telle que

$$\pi\theta_i = \sum_{j=1}^{n} a_{ij}\theta_j ;$$

par suite

$$N_{K/k}(\pi) = \det A = pf \det C,$$

d'où

$$\nu_p(N_{K/k}(\pi)) = f,$$

ce qui démontre le théorème 5.

THÉORÈME 6. — ***Si l'extension K/k est séparable, il existe toujours une base fondamentale de $\mathfrak{D}_p$ sur $\mathfrak{O}_p$.***

Avant de donner la démonstration de ce théorème, remarquons qu'elle est tout à fait analogue à celle du théorème 6, § 2, chapitre II.

Puisque tout élément de K par multiplication par une puissance convenable d'un élément premier de l'anneau $\mathfrak{O}_p$ devient entier sur $\mathfrak{O}_p$, il existe une base $\alpha_1, \ldots, \alpha_n$ de l'extension K/k dont tous les éléments appartiennent à $\mathfrak{D}_p$. Considérons la base duale $\alpha_1^*, \ldots, \alpha_n^*$ (cf. appendice § 2-3)); nous utilisons ici la séparabilité de K/k). Si $\alpha \in \mathfrak{D}_p$ et

$$\alpha = c_1\alpha_1^* + \ldots + c_n\alpha_n^* \tag{16}$$

avec $c_i \in k$, alors $c_i = \mathrm{Tr}(\alpha\alpha_i)$, d'où $c_i \in \mathfrak{O}_p$ (puisque $\alpha\alpha_i \in \mathfrak{D}_p$). Pour tout $s = 1, \ldots, n$ considérons dans l'anneau $\mathfrak{D}_p$ les éléments qui s'écrivent sous la forme

$$c_s\alpha_s^* + \ldots c_n\alpha_n^* \qquad (c_i \in \mathfrak{O}_p) \tag{17}$$

et choisissons parmi eux un élément

$$\omega_s = c_{ss}\alpha_s^* + \ldots + c_{sn}\alpha_n^*, \qquad c_{sj} \in \mathfrak{O}_p,$$

tel que $\nu_p(c_s) \geqslant \nu_p(c_{ss})$ pour tous les coefficients c_s des éléments de la forme (17) appartiennent à $\mathfrak{D}_p$. Il est clair que $c_{ss} \neq 0$ pour tout s puisque les éléments $\omega_1, \ldots, \omega_n$ de $\mathfrak{D}_p$ sont linéairement indépendants sur k. Soit maintenant α un élément de $\mathfrak{D}_p$ écrit sous la forme (16); alors $c_1 = c_{11}a_1$ avec a, $\in \mathfrak{O}_p$, d'après le choix de ω_1. La différence $a - a_1\omega_1 \in \mathfrak{D}_p$ admet la décomposition

$$a - a_1\omega_1 = c_2'\alpha_2^* + \ldots + c_n'\alpha_n^* \qquad (c_i' \in \mathfrak{O}_p),$$

d'ou $c_2' = c_{22}a_2$, d'après le choix de ω_2. Répétant n fois ce raisonnement, nous obtenons finalement une décomposition du type (13) dans laquelle

tous les coefficients a_i appartiennent à $\mathfrak{O}_\mathfrak{p}$. Ainsi, la base $\omega_1, \ldots, \omega_n$ est fondamentale par rapport à $\mathfrak{O}_\mathfrak{p}$ et le théorème 6 est ainsi démontré.

Des théorèmes 5 et 6 et de la formule (12) découlent de manière évidente le résultat suivant :

THÉORÈME 7. — ***Si l'extension K/k est séparable, les indices de ramification $e_\mathfrak{P}$ et les degrés résiduels $f_\mathfrak{P}$ des diviseurs premiers $\mathfrak{P}$ de l'anneau $\mathfrak{D}$ qui divisent un diviseur premier fixé $\mathfrak{p}$ de l'anneau $\mathfrak{O}$ sont liés entre eux par la relation***

$$\sum_{\mathfrak{P}\mid\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P} = n = (K : k).$$

Dans le cas d'une extension séparable K/k, la formule (7) peut s'écrire

$$v_\mathfrak{p}(N_{K/k}(\alpha)) = \sum_{\mathfrak{P}\mid\mathfrak{p}} f_\mathfrak{P} v_\mathfrak{P}(\alpha). \tag{18}$$

Remarque. — Pour des extensions non séparables, l'égalité du théorème 7 peut ne pas avoir lieu. Cependant, on a toujours l'inégalité $\sum_{\mathfrak{P}\mid\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P} \leqslant n$ (cf. exercice 13). On peut aussi montrer qu'on a toujours $f_\mathfrak{P} \leqslant d_\mathfrak{P}$.

4) Finitude du nombre des diviseurs premiers ramifiés

DÉFINITION. — ***Un diviseur premier $\mathfrak{p}$ de l'anneau $\mathfrak{O}$ est dit ramifié dans l'anneau $\mathfrak{D}$ s'il est divisible par le carré d'un diviseur premier de l'anneau $\mathfrak{D}$ et est dit non ramifié dans le cas contraire.***

Les $\mathfrak{p}$ non ramifiés sont donc caractérisés par le fait que dans la décomposition (2) correspondante, tous les e_i sont égaux à 1. Supposant l'extension K/k séparable nous allons donner une importante condition de non-ramification de p.

Supposons qu'il existe dans l'anneau $\mathfrak{D}_\mathfrak{p}$ un élément θ primitif (pour l'extension K/k) tel que le discriminant D(f) de son polynôme minimal $f(t)$ soit une unité dans $\mathfrak{O}_\mathfrak{p}$. Montrons qu'alors les puissances $1, \theta, \ldots, \theta^{n-2}$, où $n = (K : k)$ forment une base fondamentale de l'anneau $\mathfrak{D}_\mathfrak{p}$ sur $\mathfrak{O}_\mathfrak{p}$. En effet, sort $\omega_1, \ldots, \omega_n$ une base fondamentale de $\mathfrak{D}_\mathfrak{p}$ et C la matrice de passage de la base ω_i à la base θ^j. Alors,

$$D(f) = D(1, \theta, \ldots, \theta^{n-1}) = (\det C)^2 D(\omega_1, \ldots, \omega_n)$$

(cf. § 2 de l'appendice, formule (12)). Puisque $D(f)$ est une unité de $\mathfrak{O}_\mathfrak{p}$ et puisque les facteurs de droite appartiennent à l'anneau 0, alors det C est une unité dans $\mathfrak{O}_\mathfrak{p}$ et par suite $1, \theta, \ldots, \theta^{n-1}$ est aussi une base fondamentale.

Soient p un élément premier de l'anneau $\mathfrak{O}_\mathfrak{p}$ et $\Sigma_\mathfrak{p}$ le corps résiduel de la valuation $\nu_\mathfrak{p}$. Pour tout polynôme g(t) à coefficients dans $\mathfrak{O}_\mathfrak{p}$ nous désignerons par $\bar{g}(t)$ le polynôme de l'anneau $\Sigma_\mathfrak{p}[t]$ obtenu en remplaçant chaque coefficient de g(t) par sa classe résiduelle modulo p. Puisque le discriminant D(f) du polynôme f(t) $\in \Sigma_\mathfrak{p}[t]$ est égal à la classe résiduelle modulo p du discriminant D(f) $\in \mathfrak{O}_\mathfrak{p}$, alors, d'après la condition ci-dessus, ce discriminant $D(\bar{f})$ est différent de zéro. Par suite, dans la décomposition

$$\bar{f}(t) = \bar{\varphi}_1(t) \dots \bar{\varphi}_m(t) \tag{19}$$

en facteurs irréductibles dans l'anneau $\Sigma_\mathfrak{p}[t]$, les polynômes $\bar{\varphi}_i$ sont tous distincts (ici $\varphi_i \in \mathfrak{O}_\mathfrak{p}[t]$). Si on désigne par d_i le degré de $\bar{\varphi}_i$, alors il est clair que

$$d_1 + \dots + d_m = n = (\mathrm{K} : \mathrm{k}). \tag{20}$$

THÉORÈME 8. — *Si le discriminant du polynôme minimal $f(t)$ d'un élément primitif $\theta \in \mathfrak{D}_\mathfrak{p}$ est une unité de $\mathfrak{O}_\mathfrak{p}$, alors le diviseur premier $\mathfrak{p}$ n'est pas ramifié dans $\mathfrak{D}$ et tous les diviseurs premiers $\mathfrak{P}_i$ de la décomposition*

$$\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_m$$

sont en correspondance biunivoque avec les polynômes irréductibles $\bar{\varphi}_i \in \Sigma_\mathfrak{p}[t]$ de la décomposition (19). Le degré résiduel f_i du diviseur premier $\mathfrak{P}_i$ est égal au degré d_i du polynôme correspondant $\bar{\varphi}_i(t)$.

DÉMONSTRATION. — Soit g(t) un polynôme quelconque de $\mathfrak{O}_\mathfrak{p}[t]$. Démontrons que si les polynômes $\bar{g}$ et $\bar{\varphi}_i$ sont premiers entre eux dans l'anneau $\Sigma_\mathfrak{p}[t]$ alors les éléments g(0) et $\varphi_i(\theta)$ sont premiers entre eux dans l'anneau $\mathfrak{D}_\mathfrak{p}$. En effet, il existe alors des polynômes u(t), v(t), $l(t) \in \mathfrak{O}_\mathfrak{p}[t]$ tels que

$$g(t)u(t) + \varphi_i(t)v(t) = 1 + pl(t)$$

(puisque les polynômes $\bar{g}$ et $\bar{\varphi}_i$ sont premiers entre eux). Si g(0) et $\varphi_i(\theta)$ étaient divisibles par un élément premier π dans l'anneau $\mathfrak{D}_\mathfrak{p}$, alors, puisque $\pi | p$ (théorème 7 du § 4), il résulterait de la dernière égalité (pour $t = \theta$) que $\pi | 1$ et la contradiction obtenue démontre notre affirmation.

Puisque les polynômes irréductibles $\bar{\varphi}_i$ sont distincts, nous obtenons en particulier que $\varphi_1(\theta), \dots, \varphi_m(\theta)$ sont premiers entre eux deux à deux.

Supposons que $\varphi_i(\theta)$ soit une unité dans $\mathfrak{D}_\mathfrak{p}$, i. e. que $\varphi_i(\theta)\xi = 1$, $\xi \in \mathfrak{D}^\mathfrak{p}$. Puisque $1, \theta, \dots, \theta^{n-1}$ forment une base fondamentale de $\mathfrak{D}_\mathfrak{p}$ sur $\mathfrak{O}_\mathfrak{p}$, alors $\xi = h(O)$, avec $h(t) \in \mathfrak{O}_\mathfrak{p}[t]$. L'égalité $\varphi_i(\theta)h(\theta) = 1$ indique que

$$\varphi_i(t)h(t) = 1 + f(t)q(t), \qquad q(t) \in \mathfrak{O}_\mathfrak{p}[t]$$

(puisque le coefficient dominant de $f(t)$ est égal à 1). Par passage au corps résiduel $\Sigma_\mathfrak{p}$, nous obtenons l'égalité $\bar{\varphi}_i\bar{h} = 1 + \bar{\varphi}_1 \dots \bar{\varphi}_m\bar{q}$, d'où une contra-

diction. Ainsi, les éléments $\varphi_1(\theta), \ldots, \varphi_m(\theta)$ ne sont pas des unités dans $\mathfrak{D}_\mathfrak{p}$.

Pour tout i, choisissons dans $\mathfrak{D}_\mathfrak{p}$ un élément premier $\pi_i | \varphi_i(\theta)$. Puisque, d'après ce qui précède, les $\varphi_i(\theta)$ sont premiers deux à deux, les éléments premiers $\pi_1, \ldots, \pi_m$ ne sont pas associés deux à deux. Désignons par $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ les diviseurs premiers correspondants de l'anneau $\mathfrak{D}$ et par $f_1, \ldots, f_m$ les degrés résiduels de ces diviseurs. Dans le corps résiduel $\Sigma_{\mathfrak{P}_i}$ de la valuation $v_{\mathfrak{P}_i}$, les classes résiduelles $\bar{1}, \bar{\theta}, \ldots, \bar{\theta}^{d_i-1}$ sont linéairement indépendantes sur $\Sigma_\mathfrak{p}$ (d_i est le degré de $\bar{\varphi}_i$). En effet, si pour un polynôme $g(t) \in \mathfrak{O}_\mathfrak{p}(t)$ de degré $< d_i$ on a l'égalité $\bar{g}(\bar{\theta}) = 0$, alors l'élément $g(\theta)$ est divisible par π_i dans l'anneau $\mathfrak{D}_\mathfrak{p}$ et par suite $g(0)$ et $\varphi_i(\theta)$ ne sont pas premiers entre eux. Mais alors, comme nous l'avons vu au début de la démonstration, $\bar{g}(t)$ est divisible par $\bar{\varphi}_i(t)$ et par suite tous les coefficients de $\bar{g}(t)$ sont nuls.

Nous avons ainsi démontré que

$$d_i \leqslant f_i \qquad (i = 1, \ldots, m).$$

Rapprochant ces inégalités de l'égalité (20) et appliquant le théorème 7, nous obtenons que $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ sont tous les diviseurs premiers qui divisent p, que leurs indices de ramification sont tous égaux à 1 et enfin que $d_i = f_i$. Ces résultats constituent l'argument du théorème 8. Remarquons de plus que, puisque $\varphi_i(\theta)$ étant divisible par π_i n'est pas divisible par les autres éléments premiers π_j, π_i peut être défini comme le plus grand diviseur commun des éléments $\varphi_i(\theta)$ et p dans l'anneau $\mathfrak{D}_\mathfrak{p}$.

COROLLAIRE. — ***Si*** K/k ***est séparable, il existe dans l'anneau*** $\mathfrak{O}$ ***seulement un nombre fini de diviseurs premiers*** $\mathfrak{p}$ ***ramifiés dans*** $\mathfrak{D}$.

Soit θ un élément primitif de l'extension K/k qui soit contenu dans $\mathfrak{D}$. Le discriminant $D = D(1, \theta, \ldots, \theta^{n-1})$ est un élément de $\mathfrak{O}^*$. Si $\mathfrak{p} \nmid D$, alors d'après le théorème, $\mathfrak{p}$ n'est pas ramifié dans $\mathfrak{D}$. Ainsi, les seuls éléments éventuellement ramifiés dans $\mathfrak{D}$ sont les diviseurs premiers de l'anneau $\mathfrak{O}$ qui divisent D.

EXERCICES

1. Soient $\mathfrak{O}$ un anneau admettant une théorie des diviseurs, k son corps des fractions et $k \subset \mathrm{K} \subset \mathrm{K}'$ une chaîne d'extensions finies. Désignons par $\mathfrak{D}$ et $\mathfrak{D}'$ les fermetures intégrales de l'anneau $\mathfrak{O}$ respectivement dans les corps K et K'. Pour tout diviseur premier $\mathfrak{P}'$ de l'anneau $\mathfrak{D}'$, désignons par $\mathfrak{P}$ le diviseur premier de l'anneau $\mathfrak{D}$ qui est divisible par $\mathfrak{P}'$ et par $\mathfrak{p}$ le diviseur premier de l'anneau $\mathfrak{O}$ qui est divisible par $\mathfrak{P}$. Démontrer que le degré résiduel de $\mathfrak{P}'$ par rapport à k est égal au produit du degré résiduel de $\mathfrak{P}'$ par rapport à K et du degré résiduel de $\mathfrak{P}$ par rapport à k. Formuler et démontrer un résultat analogue pour l'indice de ramification.

2. Soit $\mathfrak{O}$ un anneau, de corps des fractions k, admettant une théorie des diviseurs avec un nombre fini de diviseurs premiers; soit $\mathfrak{p}$ un diviseur premier et soit p l'élément premier correspondant de l'anneau $\mathfrak{O}$. Démontrer que l'anneau quotient $\mathfrak{O}|(p)$ est isomorphe au corps résiduel $\Sigma_\mathfrak{p}$ de la valuation $\nu_\mathfrak{p}$.

3. Soient $\nu_\mathfrak{p}$ une valuation d'un corps k, $\mathfrak{O}_\mathfrak{p}$ son anneau, K/k une extension finie séparable, $\mathfrak{D}_\mathfrak{p}$ la fermeture intégrale de l'anneau $\mathfrak{O}_\mathfrak{p}$ dans le corps K et $\omega_1, \ldots, \omega_n$ une base de K sur k dont tous les éléments appartiennent à l'anneau $\mathfrak{D}_\mathfrak{p}$. Démontrer que si le discriminant $D(\omega_1, \ldots, \omega_n)$ est une unité de l'anneau $\mathfrak{O}_\mathfrak{p}$, alors $\omega_1, \ldots, \omega_n$ est une base fondamentale de l'anneau $\mathfrak{D}_\mathfrak{p}$ sur $\mathfrak{O}_\mathfrak{p}$.

4. Démontrer l'unicité de l'homomorphisme $N : \mathfrak{D} \to \mathfrak{D}_0$ satisfaisant à la condition du théortme 4.

5. Démontrer l'unicité du plongement isomorphe $\mathfrak{D}_0 \to \mathfrak{D}$ satisfaisant à la condition du théorème 3.

6. Soit a un diviseur de l'anneau $\mathfrak{O}$. Le considérant comme un diviseur de l'anneau $\mathfrak{D}$ (en vertu du plongement $\mathfrak{D}_0 \to \mathfrak{D}$), démontrer

$$N_{K/k}(\mathfrak{a}) = \mathfrak{a}^n \qquad (n = (K : k)).$$

7. Soit K/k une extension séparable de degré n. Démontrer que si un diviseur a de l'anneau $\mathfrak{O}$ devient un diviseur principal dans l'anneau $\mathfrak{D}$, alors $\mathfrak{a}^n$ est un diviseur principal dans $\mathfrak{O}$.

8. Supposons K/k séparable. Démontrer que la norme $N_{K/k}(u)$ d'un diviseur $\mathfrak{U}$ de l'anneau $\mathfrak{D}$ est le plus grand commun diviseur des diviseurs principaux $(N_{K/k}(\alpha))_k$, où a parcourt tous les éléments de $\mathfrak{D}^*$ qui sont divisibles par $\mathfrak{U}$.

9. Un polynôme $f(t) = t^n + a_1 t^{n-1} + \ldots + a_n$, à coefficients dans l'anneau $\mathfrak{O}$ est appelé un polynôme d'Eisenstein par rapport à un diviseur premier $\mathfrak{p}$ si $a_1, \ldots, a_n$ sont tous divisibles par $\mathfrak{p}$ et a_n (qui est divisible par $\mathfrak{p}$) non divisible par $\mathfrak{p}^2$. Démontrer que s'il existe dans l'anneau $\mathfrak{D}$ un élément θ primitif pour l'extension K/k de degré n, dont le polynôme minimal est un polynôme d'Eisenstein par rapport à p, alors $\mathfrak{p}$ est divisible par un seul diviseur premier $\mathfrak{P}$ de l'anneau $\mathfrak{D}$ et

$$\mathfrak{p} = \mathfrak{P}^n$$

(le degré résiduel de $\mathfrak{P}$ par rapport à $\mathfrak{p}$ est par suite égal à 1).

10. Sous les mêmes hypothèses, démontrer que la base $1, \theta, \ldots, \theta^{n-1}$ est une base fondamentale de l'anneau $\mathfrak{D}_\mathfrak{p}$ sur $\mathfrak{O}_\mathfrak{p}$.

11. Soient k_0 un corps de caractéristique p et $k = k_0(x, y)$ le corps des fonctions rationnels en x et y sur le corps k_0. Considérons sur k la valuation ν_0, introduite dans l'exercice 9 du § 4, relative à une série $\xi(t) \in k_0\{t\}$ (transcendante sur $k_0(t)$) de la forme

$$\xi(t) = \eta(t)^p = \left(\sum_{n=0}^{\infty} a_n t^n\right)^p = \sum_{n=0}^{\infty} a_n^p t^{np}, \qquad a_n \in k_0.$$

D'après l'exercice 8 du §4, la valuation ν_0 admet un seul prolongement à l'extension strictement non séparable $K = k(\sqrt[p]{y})$, de degré p sur k. Démontrer que l'indice de ramification de ν par rapport à ν_0 est égal à 1 et que le corps résiduel de la valuation ν_0 coïncide avec le corps résiduel de la valuation v. Il résulte alors du théorème 5 et de l'égalité (12) que, pour l'anneau $\mathfrak{D}$ de la valuation v, qui est la fermeture intégrale dans K de l'anneau $\mathfrak{O}$ de la valuation ν_0, il n'existe pas de base fondamentale sur $\mathfrak{O}$.

12. Avec les notations et hypothèses de l'exercice précédent, démontrer directement (sans utiliser le théorème 5) qu'il n'existe pas de base fondamentale de $\mathfrak{D}$ sur $\mathfrak{O}$.

13. Soient $\mathfrak{O}$ un anneau admettant une théorie des diviseurs, k son corps des fractions, K/k une extension finie de degré n, $\mathfrak{D}$ la fermeture intégrale de l'anneau $\mathfrak{O}$ dans le corps K, $\mathfrak{p}$ un diviseur premier de l'anneau $\mathfrak{O}$, $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ les diviseurs premiers de l'anneau $\mathfrak{D}$ qui divisent p, $e_1, \ldots, e_m$ leurs indices de ramification et $f_1, \ldots, f_m$ leurs degrés résiduels par rapport à p. Pour tout $s = 1, \ldots, m$, nous désignerons par $\bar{\alpha}^{\mathfrak{P}_s}$ la classe résiduelle du corps $\Sigma_{\mathfrak{P}_s}$ de représentant $\alpha \in \mathfrak{D}_{\mathfrak{P}_s}$. Soient $\omega_{si} \in \mathfrak{D}_p$ des éléments dont les classes résiduelles $\bar{\omega}_{si}^{\mathfrak{P}_s}$ forment une base de l'extension $\Sigma_{\mathfrak{P}_s}|\Sigma_{\mathfrak{p}}$ et tels que, de plus, $v_{\mathfrak{P}_j}(\omega_{si}) \geqslant e_j$ pour $j \neq s$, $1 \leqslant j \leqslant m$. Nous désignerons par $\pi_1, \ldots, \pi_m$ les éléments premiers de l'anneau $\mathfrak{D}_{\mathfrak{p}}$ qui correspondent aux diviseurs premiers $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$. Démontrer que les éléments

$$\omega_{si}\pi_s^j \qquad (s = 1, \ldots, m; i = 1, \ldots, f_s; j = 0, 1, \ldots, e_s - 1) \quad (*)$$

sont linéairement indépendants sur k.

Indication. — Considérer les combinaisons linéaires

$$\alpha = \Sigma c_{sij}\omega_{si}\pi_s^j$$

à coefficients dans $\mathfrak{O}_{\mathfrak{p}}$, l'un au moins d'entre eux étant une unité de?,. Supposons $v_{\mathfrak{p}}(c_{s_0i_0j_0}) = 0$, j_0 étant choisi de telle sorte que $v_{\mathfrak{p}}(c_{s_0ij}) > 0$ pour tout i et pour $j < j_0$. Alors

$$v_{\mathfrak{P}_{s_0}}(\alpha) = j_0.$$

14. Démontrer que si l'extension K/k est séparable, alors le système (*) est une base fondamentale de $\mathfrak{D}_{\mathfrak{p}}$ sur $\mathfrak{O}_{\mathfrak{p}}$.

15. Démontrer que, dans le cas où K/k est séparable, pour tout $\alpha \in \mathfrak{D}_{\mathfrak{p}}$, on a la formule

$$\overline{\mathrm{Tr}_{K/k}(\alpha)}^{\mathfrak{p}} = \sum_{s=1}^{m} e_s \,\mathrm{Tr}_{\Sigma_{\mathfrak{P}_s}/\Sigma_{\mathfrak{p}}}(\bar{\alpha}^{\mathfrak{P}_s}).$$

16. Soit $f(t)$ le polynôme caractéristique d'un élément $\alpha \in \mathfrak{D}_{\mathfrak{p}}$ pour l'extension K/k d'un élément $\alpha \in \mathfrak{D}_{\mathfrak{p}}$. Remplaçant chaque coefficient par la classe résiduelle correspondante de $\Sigma_{\mathfrak{p}}$, nous obtenons un polynôme $f(t) \in \Sigma_{\mathfrak{p}}[t]$. Pour tout $s = 1, \ldots, m$, désignons par $\varphi_s(t)$ le polynôme caractéristique de l'élément $\bar{a\alpha}^{\mathfrak{P}_s} \in \Sigma_{\mathfrak{P}_s}$ pour l'extension $\Sigma_{\mathfrak{P}_s}|\Sigma_{\mathfrak{p}}$. Généralisant l'exercice précédent (pour K/k séparable), démontrer que

$$\bar{f}(t) = \varphi_1(t)^{e_1} \ldots \varphi_m(t)^{e_m}$$

17. Soit K/k une extension séparable. Pour tout p, choisissons une base fondamentale $\alpha_1, \ldots, \alpha_n$ de l'anneau $\mathfrak{D}_{\mathfrak{p}}$ sur $\mathfrak{O}_{\mathfrak{p}}$ et posons

$$d_{\mathfrak{p}} = v_{\mathfrak{p}}(D(\alpha_1, \ldots, \alpha_n)).$$

Démontrer que les entiers naturels $d_{\mathfrak{p}}$ sont presque tous nuls. Le diviseur entier

$$\mathfrak{d}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}}$$

est appelé le discriminant de l'extension K/k (par rapport à l'anneau $\mathfrak{O}$).

18. Demontrer qu'un diviseur premier $\mathfrak{p}$ de l'anneau $\mathfrak{O}$ ne figure pas dans le discriminant $\mathfrak{d}_{K/k}$ (i. e. $d_{\mathfrak{p}} = 0$) si et seulement si $\mathfrak{p}$ n'est pas ramifié dans $\mathfrak{D}$ (i. e. tous les indices de ramification e_i sont égaux à 1) et toutes les extensions $\Sigma_{\mathfrak{P}_s}|\Sigma_{\mathfrak{p}}$ ($s = 1, \ldots, m$) sont séparables.

19. Supposons qu'il existe une base fondamentale $\omega_1, \ldots, \omega_n$ de l'anneau $\mathfrak{D}$ sur $\mathfrak{O}$. Démontrer que, dans ce cas, le discriminant $\mathfrak{d}_{K/k}$ est égal au diviseur principal $(D(o_{\omega_1}, \ldots, \omega_n))$.

§6. — ANNEAUX DE DEDEKIND

1) Congruences modulo un diviseur

Considérons un anneau $\mathfrak{D}$, de corps des fractions K, admettant une théorie des diviseurs $\mathfrak{D}^* \to \mathbf{A}$.

DÉFINITION. — ***Nous dirons que deux éléments α et β de l'anneau $\mathfrak{D}$ sont congrus modulo un diviseur $\mathfrak{a} \in \mathbf{A}$ et nous écrirons***

$$\alpha \equiv \beta \pmod{\mathfrak{a}}$$

si la différence $\alpha - \beta$ est divisible par a.

Dans le cas d'un diviseur principal (μ), la congruence $\alpha \equiv \beta \pmod{(\mu)}$ équivaut à la congruence $\alpha \equiv \beta \pmod{\mu}$ au sens de la définition du § 4-1) de l'appendice.

Énumérons quelques propriétés élémentaires des congruences (qui découlent facilement de la définition).

1° On peut additionner et multiplier terme à terme les congruences modulo a.

2° Si on a une congruence modulo a, alors cette congruence est aussi vraie modulo tout diviseur $\mathfrak{b}$ qui divise le diviseur a.

3° Si on a une congruence modulo les diviseurs a et $\mathfrak{b}$, elle est aussi satisfaite modulo leur plus petit commun multiple.

4° Si un élément $\alpha \in \mathfrak{D}$ est premier avec a (i. e. les diviseurs (α) et a sont premiers entre eux), alors la congruence $\alpha\beta \equiv 0 \pmod{\mathfrak{a}}$ entraîne $\beta \equiv 0 \pmod{\mathfrak{a}}$.

5° On peut simplifier les deux parties d'une congruence modulo a par un facteur premier avec a.

6° Si $\mathfrak{p}$ est un diviseur premier et $\alpha\beta \equiv 0 \pmod{\mathfrak{p}}$, alors ou bien $\alpha \equiv 0 \pmod{\mathfrak{p}}$ ou bien $\beta \equiv 0 \pmod{\mathfrak{p}}$.

D'après la propriété (1), on peut définir une structure d'anneau sur l'en-

semble des classes résiduelles modulo a; cet anneau est appelé ***l'anneau des classes résiduelles modulo le diviseur*** a et est désigné par $\mathfrak{D}/\mathfrak{a}$.

La propriété (6) exprime que, pour un diviseur premier $\mathfrak{p}$, l'anneau $\mathfrak{D}/\mathfrak{p}$ n'a pas de diviseur de zéro.

Supposons maintenant que $\mathfrak{D}$ est l'ordre maximum d'un corps K de nombres algébriques. Nous appellerons alors les diviseurs de l'anneau $\mathfrak{D}$ les ***diviseurs du corps*** K.

Puisque tout diviseur a du corps K divise un certain nombre $\alpha \in \mathfrak{D}$, $\alpha \neq 0$ et puisque le nombre α, à son tour, divise un entier naturel a (par exemple, $|N(\alpha)|$ est divisible par a), nous obtenons que, tout diviseur a divise au moins un entier naturel a. D'après la propriété (2), les nombres de deux classes résiduelles distinctes modulo a appartiennent à des classes résiduelles distinctes modulo a. Rappelant maintenant que, dans l'ordre $\mathfrak{D}$, le nombre des classes résiduelles modulo a est fini (et égal à a^n, *où* n est le degré du corps K, cf. démonstration du théorème 5, § 2, chap. II), nous obtenons le résultat suivant :

THÉORÈME 1. — ***Pour tout diviseur*** a ***d'un corps*** K ***de nombres algébriques, l'anneau*** $\mathfrak{D}/\mathfrak{a}$ ***est fini.***

Soit $\mathfrak{p}$ un diviseur premier quelconque du corps K. La valuation $v^{\mathfrak{p}}$ correspondante induit sur $\mathbf{Q}$ la valuation p-adique v_p pour un certain p premier. Puisque $v_{\mathfrak{p}}(p) = 1$, $v_{\mathfrak{p}}(p) > 0$, i. e. $p \equiv 0 \pmod{\mathfrak{p}}$. Si q est un nombre premier rationnel différent de p, alors $v_{\mathfrak{p}}(q) = 0$ et par suite $v_{\mathfrak{p}}(q) = 0$, i. e. $q \not\equiv 0 \pmod{\mathfrak{p}}$.

L'anneau résiduel $\mathfrak{D}|\mathfrak{p}$ étant fini et sans diviseur de zéro est un corps fini (cf. appendice § 3). Puisque pour tout $a \in \mathfrak{D}$, nous avons $pa \equiv 0 \pmod{\mathfrak{p}}$, la caractéristique de ce corps est égale à p, d'où le théorème suivant.

THÉORÈME 2. — ***Tout diviseur premier*** $\mathfrak{p}$ ***d'un corps de nombres algébriques divise un nombre premier rationnel et un seul p. L'anneau résiduel*** $\mathfrak{D}/\mathfrak{p}$ ***est un corps fini de caractéristique p.***

Les théories des diviseurs pour les corps de nombres algébriques possèdent la propriété que l'anneau des classes résiduelles modulo tout diviseur premier est un corps. Il n'en est pas toujours ainsi dans le cas général. Par exemple, dans l'anneau $k[x, y]$ des polynômes de deux variables sur un corps k, l'anneau résiduel modulo le diviseur premier (x) est isomorphe à l'anneau des polynômes $k[y]$ qui n'est pas un corps.

Le fait que l'anneau $\mathfrak{D}/\mathfrak{p}$ soit un corps équivaut à la résolubilité de la congruence $\alpha\xi \equiv 1 \pmod{\mathfrak{p}}$ pour tout $a \not\equiv 0 \pmod{\mathfrak{p}}$. Cela montre que les propriétés habituelles des congruences usuelles sont encore valables ici.

2) Congruences dans les anneaux de Dedekind

DÉFINITION. — *Un anneau $\mathfrak{D}$ est dit de Dedekind s'il admet une théorie des diviseurs $\mathfrak{D} \to \Delta$ telle que pour diviseur premier $\mathfrak{p} \in A$ l'anneau résiduel $\mathfrak{D}/\mathfrak{p}$ soit un corps.*

En dehors des ordres maxima des corps de nombres algébriques, on peut donner comme exemples d'anneaux de Dedekind les fermetures intégrales de l'anneau *k[x]* des polynômes à une variable dans toute extension finie du corps *k(x)* des fractions rationnelles (exercices 1 et 2). L'anneau $\mathfrak{D}_v$ d'une valuation v d'un corps (cf. § 4-l)) et plus généralement tout anneau admettant une théorie des diviseurs avec un nombre fini de diviseurs premiers sont des anneaux de Dedekind (exercice 3).

LEMME *1.* — *Soit $\mathfrak{D}$ un anneau de Dedekind. Pour tout $\alpha \in \mathfrak{D}$ non divisible par un diviseur premier $\mathfrak{p}$, la congruence $\alpha\xi \equiv 1 \pmod{\mathfrak{p}^m}$ est résoluble dans $\mathfrak{D}$ pour tout entier naturel m.*

DÉMONSTRATION. — Pour $m = 1$, la résolubilité de la congruence résulte de la définition. Dans le cas général, on procède par récurrence sur *m*. Soit $\xi_0 \in \mathfrak{D}$ tel que $\alpha\xi_0 \equiv 1 \pmod{\mathfrak{p}^m}$. Choisissons un élément $\omega \in \mathfrak{D}$ tel que $\nu_\mathfrak{p}(\omega) = m$. Le diviseur principal (ω) s'écrit $(w) = \mathfrak{p}^m\mathfrak{a}$, a non divisible par $\mathfrak{p}$. Choisissons maintenant un élément $y \in \mathfrak{D}$ tel que $\nu_\mathfrak{p}(\gamma) = 0$ et $y \equiv 0 \pmod{a}$. Le produit $\gamma(a\xi_0 - 1)$ est alors divisible par $\mathfrak{p}^m\mathfrak{a} = (\omega)$ et par suite $\gamma(a\xi_0 - 1) = \omega\mu$, $\mu \in \mathfrak{D}$. Essayons de satisfaire la congruencc $\alpha\xi \equiv 1 \pmod{\mathfrak{p}^{m+1}}$ en prenant pour ξ un élément de la forme $\xi = \xi_0 + \omega\lambda$, où $\lambda \in \mathfrak{D}$ est convenablement choisi. Puisque

$$\gamma(\alpha\xi - 1) = y(\& - 1) + \gamma\alpha\omega\lambda = \omega(\mu + \gamma\alpha\lambda)$$

et $\omega \equiv 0 \pmod{\mathfrak{p}^m}$, alors il suffit que λ satisfasse à la congruence

$$\lambda\alpha\gamma \equiv -\mu \pmod{\mathfrak{p}}.$$

Mais, puisque $\alpha\gamma$ n'est pas divisible par $\mathfrak{p}$, cette congruence est résoluble. Ainsi, il existe un élément $\xi \in \mathfrak{D}$ tel que $\gamma(\alpha\xi - 1) \equiv 0 \pmod{\mathfrak{p}^{m+1}}$ et puisque $\nu_\mathfrak{p}(\gamma) = 0$, on obtient, après simplification par y, $\alpha\xi - 1 \equiv 0 \pmod{p}$. Le lemme 1 est démontré.

THÉORÈME *3.* — *Soit $\mathfrak{D}$ un anneau de Dedekind. Il existe un élément $\xi \in \mathfrak{D}$ qui satisfait aux congruences*

$$\left.\begin{aligned} \xi &\equiv \beta_1 \pmod{\mathfrak{p}_1^{k_1}} \\ &\cdots \\ \xi &\equiv \beta_m \pmod{\mathfrak{p}_m^{k_m}} \end{aligned}\right\}$$

pour tous $\beta_1, \ldots, \beta_m \in \mathfrak{D}$ et tous les diviseurs premiers deux à deux distincts $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ ($k_1, \ldots, k_m$ sont des entiers naturels).

DÉMONSTRATION. — Pour chacun des diviseurs

$$\mathfrak{a}_i = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_{i-1}^{k_{i-1}} \mathfrak{p}_{i+1}^{k_{i+1}} \dots \mathfrak{p}_m^{k_m} \qquad (i = 1, \dots m)$$

on peut trouver un élément $\alpha_i \in \mathfrak{D}$ divisible par $\mathfrak{a}_i$ et non divisible par $\mathfrak{p}_i$. D'après le lemme 1, la congruence $\alpha_i \xi_i \equiv \beta_i \pmod{\mathfrak{p}_i^{k_i}}$ est résoluble avec $\xi_i \in \mathfrak{D}$. Il est facile de vérifier maintenant que l'élément

$$\xi = \alpha_1 \xi_1 + \dots + \alpha_m \xi_m$$

satisfait aux exigences du théorème.

THÉORÈME *4. — Soient $a \neq 0$ et β des éléments d'un anneau de Dedekind $\mathfrak{D}$. La congruence*

$$\alpha\xi \equiv \beta \pmod{a} \qquad (1)$$

est résoluble si et seulement si β est divisible par le plus grand commun diviseur des diviseurs (a) et a.

DÉMONSTRATION. — Supposons tout d'abord que les diviseurs (a) et a sont premiers entre eux; démontrons qu'alors la congruence (1) est résoluble pour tout β. Soit $a = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_m^{k_m} = \mathfrak{p}_i^{k_i} \mathfrak{a}_i$, les diviseurs premiers $\mathfrak{p}_i$ étant deux à deux distincts. D'après le lemme 1, pour tout $i = 1, \dots, m$, il existe un élément $\xi_i' \in \mathfrak{D}$ tel que $\alpha\xi_i' \equiv \beta \pmod{\mathfrak{p}_i^{k_i}}$. Nous pouvons maintenant, d'après le théorème 3, trouver pour tout i un élément ξ_i tel que $\xi_i \equiv \xi_i' \pmod{\mathfrak{p}_i^{k_i}}$ et $\xi_i \equiv 0 \pmod{\mathfrak{a}_i}$. Il est évident maintenant que la somme

$$4 = \mathrm{El} + \dots + \xi_m$$

satisfait à la congruence $\alpha\xi \equiv \beta \pmod{\mathfrak{p}_i^{k_i}}$ pour tout $i = 1, \dots, m$ et par suite satisfait à la congruence (1).

Demontrons maintenant le théorème dans le cas général. Soit

$$\mathfrak{d} = \mathfrak{p}_1^{l_1} \dots \mathfrak{p}_m^{l_m}$$

le plus grand diviseur commun des diviseurs (a) et a. Si la congruence (1) est résoluble modulo a, elle est aussi résoluble modulo $\mathfrak{d}$ et puisque $a \equiv 0 \pmod{b}$, on a $\beta \equiv 0 \pmod{b}$. Ainsi, la condition du théorème est nécessaire.

Supposons maintenant que β est divisible par $\mathfrak{d}$. D'après le théorème 3 du § 4, il existe dans le corps K un élément μ tel que

$$v_{\mathfrak{p}_i}(\mu) = -l_i \qquad (i = 1, \dots, m). \qquad (2)$$

Montrons qu'on peut choisir l'élément μ satisfaisant aux conditions (2) tel que, de plus

$$v_{\mathfrak{q}}(\mu) \geqslant 0 \qquad (3)$$

pour tout diviseur premier $\mathfrak{q} \in A$ différent de $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Supposons que μ ne satisfait pas aux conditions 3 et soient $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ tous les diviseurs premiers distincts de $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ tels que $\nu_{\mathfrak{q}_j}(\mu) = -r < 0$. Choisissons un élément $\gamma \in \mathfrak{D}$ tel que $\nu_{\mathfrak{q}_j}(\gamma) = r_j$ $(1 \leqslant j \leqslant s)$ et $\nu_{\mathfrak{p}_i}(\gamma) = 0$ $(1 \leqslant i \leqslant m)$. Il est clair que l'élément $\mu' = \mu\gamma$ satisfait aux conditions (2) et (3). Soit alors b le diviseur défini par l'égalité $a = \mathfrak{d}\mathfrak{b}$. Si μ satisfait aux conditions (2) et (3), l'élément $\alpha\mu \in \mathfrak{D}$ est premier avec b. Puisque, par hypothèse, β est divisible par b, alors $\beta\mu \in \mathfrak{D}$. Il existe alors, d'après ce qui précède, un élément $\xi \in \mathfrak{D}$ tel que $\alpha\mu\xi \equiv \beta\mu \pmod{b}$. Pour tout $i = 1, \ldots, m$ nous avons alors

$$\nu_{\mathfrak{p}_i}(\alpha\xi - \beta) = \nu_{\mathfrak{p}_i}(\alpha\mu\xi - \beta\mu) + l_i \geqslant k_i - l_i + l_i + k_i,$$

et par suite ξ satisfait à la congruence (1).

3) Diviseurs et idéaux

Nous montrerons ici que pour un anneau de Dedekind, les diviseurs sont en correspondance biunivoque avec les idéaux non nuls.

Pour tout diviseur a, nous désignerons par $\bar{a}$ l'ensemble de tous les éléments de l'anneau $\mathfrak{D}$ qui sont divisibles par a. Il est évident que $\bar{a}$ est un idéal non nul de l'anneau $\mathfrak{D}$.

THÉORÈME 5. — *Pour un anneau de Dedekind $\mathfrak{D}$, l'application* $a \to \bar{a}$ $(a \in A)$ ***est un isomorphisme du monoïde*** A ***des diviseurs sur le monoïde de tous les idéaux non nuls de l'anneau*** $\mathfrak{D}$.

Énonçons tout d'abord le lemme suivant.

LEMME 2. — *Si $\alpha_1, \ldots,$ a, sont des éléments quelconques $\neq 0$ d'un anneau de Dedekind $\mathfrak{D}$ et $\mathfrak{d}$ le plus grand diviseur commun des diviseurs principaux $(\alpha_1), \ldots, (\alpha_s)$, alors tout élément $a \in \mathfrak{D}$ divisible par $\mathfrak{d}$ peut s'écrire sous la forme*

$$\alpha = \xi_1\alpha_1 + \ldots + \xi_s\alpha_s \qquad (\xi_i \in \mathfrak{D}).$$

DÉMONSTRATION DU LEMME. — La démonstration s'effectue par récurrence sur s. Pour $s = 1$, le lemme est trivial. Soit $s \geqslant 2$ et désignons par $\mathfrak{d}_1$ le plus grand commun diviseur des diviseurs $(\alpha_1), \ldots, (\alpha_{s-1})$. Il est clair qu'alors $\mathfrak{d}$ est le plus grand commun diviseur des diviseurs $\mathfrak{d}_1$ et (α_s). Supposons que a est divisible par $\mathfrak{d}$. D'après le théorème 4, la congruence $\alpha_s\xi \equiv \alpha \pmod{\mathfrak{d}_1}$ admet une solution $\xi \in \mathfrak{D}$. Par hypothèse de récurrence, il existe des éléments $\xi_1, \ldots, \xi_{s-1}$ dans l'anneau $\mathfrak{D}$ tels que $a - \xi\alpha_s = \xi_1\alpha_1 + \ldots + \xi_{s-1}\alpha_{s-1}$ et le lemme 2 est démontré.

DÉMONSTRATION DU THÉORÈME 5. — D'après la condition 3° de la définition d'une théorie des diviseurs, l'application $a \to \bar{a}$ est injective.

Soit A un idéal non nul quelconque de l'anneau $\mathfrak{D}$. Pour tout diviseur premier $\mathfrak{p}$, posons

$$a(\mathfrak{p}) = \min_{\alpha \in A} \nu_{\mathfrak{p}}(\alpha).$$

Il est clair que a(p) est différent de 0 seulement pour un nombre fini de diviseurs premiers p. Le produit

$$a = \prod_{P} \mathfrak{p}^{a(\mathfrak{p})},$$

dans lequel $\mathfrak{p}$ parcourt tous les diviseurs premiers $\mathfrak{p}$ tels que $a(\mathfrak{p}) \neq 0$, est par suite un diviseur. Montrons que $\bar{a} = A$. Soit α un élément quelconque de $\bar{a}$; il est clair qu'on peut trouver dans A un ensemble fini d'éléments $\alpha_1, \ldots, \alpha_s$ tels que $a(\mathfrak{p}) = \min(\nu_{\mathfrak{p}}(\alpha_1), \ldots, \nu_{\mathfrak{p}}(\alpha_s))$. Cela exprime que le diviseur a est le plus grand commun diviseur des diviseurs principaux $(\alpha_1), \ldots, (\alpha_s)$. D'après le lemme 2, l'élément $a \in \bar{a}$ peut donc s'écrire $a = \xi_1\alpha_1 + \ldots + \xi_s\alpha_s$, $\xi_i \in \mathfrak{D}$; ainsi $a \in A$, d'où $\bar{a} \subset A$. Rapprochant ce résultat de l'inclusion triviale $A \subset \bar{a}$, nous obtenons l'égalité $A = \bar{a}$. Nous avons donc montré que l'application $a \to \bar{a}$ établit une correspondance biunivoque entre les diviseurs et l'ensemble des idéaux non nuls de l'anneau $\mathfrak{D}$.

Il reste à vérifier que cette application est un isomorphisme, i. e. que pour tous les diviseurs a et $\mathfrak{b}$ nous avons

$$ab = \bar{a}\bar{b}. \tag{4}$$

Désignons par C le produit $\bar{a}\bar{b}$. Puisque C est un idéal non nul de $\mathfrak{D}$, il existe un diviseur c tel que $C = \bar{c}$. Il faut montrer que $c = a.\mathfrak{b}$. Soit $\mathfrak{p}$ un diviseur premier figurant dans a et $\mathfrak{b}$ avec des exposants a et *b;* alors

$$\min_{\gamma \in C} \nu_{\mathfrak{p}}(\gamma) = \min_{\alpha \in \bar{a}, \beta \in \bar{b}} \nu_{\mathfrak{p}}(\alpha\beta) = \min_{\alpha \in \bar{a}} \nu_{\mathfrak{p}}(\alpha) + \min_{\beta \in \bar{b}} \nu_{\mathfrak{p}}(\beta) = a + b.$$

Puisque cette relation est vraie pour tout diviseur premier $\mathfrak{p}$, on a $c = a.\mathfrak{b}$ et l'égalité (4) est démontrée.

Il résulte en particulier de l'isomorphisme ci-dessus que tous les idéaux non nuls de l'anneau $\mathfrak{D}$ forment un monoïde avec décomposition unique en facteurs premiers. Pour construire une théorie des diviseurs pour un anneau de Dedekind (et en particulier pour l'ordre maximum d'un corps de nombres algébriques), on peut prendre comme monoïde A le monoïde des idéaux non nuls. L'image d'un élément $a \in \mathfrak{D}^*$ par l'homomorphisme $\mathfrak{D}^* \to A$ est alors l'idéal principal *(a)* engendré par cet élément. C'est à Dedekind que nous devons cette construction.

4) Diviseurs fractionnaires

Pour un anneau $\mathfrak{D}$, la construction d'une théorie des diviseurs $\mathfrak{D}^* \to A$ donne des indications sur la structure du monoïde a)*. Pour étudier la structure du groupe multiplicatif K* du corps des fractions K de $\mathfrak{D}$ on est amené à étendre la notion de diviseur.

Selon l'usage, nous conserverons le terme « diviseur » pour cette extension; les diviseurs au sens précédent seront désormais appelés diviseurs entiers.

DÉFINITION. — *Soit $\mathfrak{D}$ un anneau et* K *son corps des fractions. Nous supposerons que $\mathfrak{D}$ admet une théorie des diviseurs et soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ un système fini de diviseurs premiers. L'expression*

$$a = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m} \tag{5}$$

avec des exposants entiers $k_1, \ldots, k_m$ (non nécessairement positifs) est appelée un diviseur du corps K. *Si aucun des exposants k_i n'est négatif, le diviseur $\mathfrak{a}$ est dit entier (ou diviseur de l'anneau $\mathfrak{D}$); dans le cas contraire, il est dit fractionnaire.*

Il sera commode d'écrire le diviseur (5) comme un produit formel infini

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}, \tag{6}$$

étendu à tous les diviseurs premiers $\mathfrak{p}$ de l'anneau $\mathfrak{D}$, un nombre fini seulement des exposants $a(\mathfrak{p})$ étant différents de 0.

La multiplication des diviseurs sera définie par la formule

$$\left(\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}\right)\left(\prod_{\mathfrak{p}} \mathfrak{p}^{b(\mathfrak{p})}\right) = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})+b(\mathfrak{p})}.$$

Dans le cas des diviseurs entiers, on retrouve bien la loi de multiplication dans le monoïde A. Il est facile de voir que pour cette opération, l'ensemble des diviseurs du corps K forme un groupe abélien que nous désignerons dans la suite par $\widehat{\Delta}$. L'élément unité de ce groupe est le diviseur unité e pour lequel tous les exposants $a(\mathfrak{p})$ sont nuls dans la représentation (6).

Puisque tout élément $\xi \neq 0$ du corps K est le quotient de deux éléments de $\mathfrak{D}$, alors, d'après la condition 1° du théorème 4, § 3, il existe seulement un nombre fini de valuations $v_{\mathfrak{p}}$ du corps K, correspondant aux diviseurs premiers p, telles que $v_{\mathfrak{p}}(\xi) \neq 0$; soient $v_{\mathfrak{p}}, \ldots, v_{\mathfrak{p}_m}$ ces valuations. Le diviseur

$$\prod_{i=1}^{m} \mathfrak{p}_i^{v_{\mathfrak{p}_i}(\xi)} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\xi)}$$

est appelé le ***diviseur principal*** correspondant à l'élément $\xi \in K^*$ et est désigné par (ξ). Cette nouvelle notion de diviseur principal, appliquée aux éléments de $\mathfrak{D}$, coïncide bien entendu avec celle déjà connue (cf. § 3-4)). D'après la condition 2^o du théorème 4, § 3, le diviseur principal (ξ) est entier si et seulement si $\xi \in \mathfrak{D}$.

Il résulte facilement de la condition 2^o de la définition d'une valuation (§ 3-4)) que l'application $\xi \to (\xi)$, $\xi \in K^*$ est un homomorphisme du groupe multiplicatif K^* du corps K dans le groupe des diviseurs $\widehat{\Delta}$. D'après le théorème 2 du § 3, cet homomorphisme est surjectif (épimorphisme) si et seulement s'il y a unicité de la décomposition en facteurs premiers dans $\mathfrak{D}$. Son noyau est le groupe des unités de l'anneau $\mathfrak{D}$, i. e. pour des éléments $\xi, \eta \in K^*$, l'égalité $(\xi) = (\eta)$ est équivalente à l'égalité $\xi = \eta\varepsilon$, ε unité de l'anneau $\mathfrak{D}$.

Étendons la notion de divisibilité aux diviseurs quelconques. Soient

$$a = \prod_P \mathfrak{p}^{a(\mathfrak{p})} \qquad \text{et} \qquad \mathfrak{b} = \prod_P \mathfrak{p}^{b(\mathfrak{p})}$$

deux diviseurs quelconques (pas nécessairement entiers). Nous dirons que a est divisible par b (b divise a, ou a est un multiple de b), s'il existe un diviseur entier c tel que a = bc. La divisibilité de a par b est donc caractérisée par les inégalités $a(\mathfrak{p}) \geqslant b(\mathfrak{p})$ pour tout $\mathfrak{p}$.

Pour a et b quelconques, posons $d(\mathfrak{p}) = \min(a(\mathfrak{p}), b(\mathfrak{p}))$; puisque les nombres entiers rationnels $d(\mathfrak{p})$ sont nuls pour presque tout p, l'expression

$$\mathfrak{d} = \prod_P \mathfrak{p}^{d(\mathfrak{p})},$$

est un diviseur. Ce diviseur $\mathfrak{d}$ est appelé le plus grand commun diviseur des diviseurs a et b (il divise a et b et est divisible par tout diviseur commun à a et b). De manière analogue, on définit le plus petit commun multiple de deux diviseurs.

Un élément $\alpha \in K$ est dit divisible par le diviseur

$$a = \prod_P \mathfrak{p}^{a(\mathfrak{p})}$$

si, ou bien $a = 0$, ou bien le diviseur principal (a) est divisible par a; cela équivaut aux inégalités $v_{\mathfrak{p}}(\alpha) \geqslant a(\mathfrak{p})$ pour tout p.

On peut étendre la correspondance étudiée au point ci-dessus (entre les diviseurs entiers d'un anneau de Dedekind et les idéaux non nuls) aux diviseurs fractionnaires en généralisant la notion d'idéal.

Comme au point 3), désignons par $\bar{a}$ l'ensemble de tous les éléments du corps K qui sont divisibles par le diviseur a (pas nécessairement entier).

La condition 3° de la définition d'une valuation entraîne que si α et β sont divisibles par a, alors $\alpha \pm \beta$ est aussi divisible par a. Cela signifie que $\bar{\mathfrak{a}}$ est groupe pour l'addition. Il est évident de plus que pour tout $\alpha \in \bar{\mathfrak{a}}$ et $\xi \in \mathfrak{D}$ le produit $\xi\alpha$ appartient aussi à $\bar{\mathfrak{a}}$. Avant d'obtenir une dernière propriété des groupes $\bar{\mathfrak{a}}$, vérifions tout d'abord la formule

$$(\gamma)\mathfrak{a} = \gamma\bar{\mathfrak{a}} \qquad (\gamma \in \mathbf{K}^*,\ \mathfrak{a} \in \widehat{\Delta}). \tag{7}$$

En effet, la divisibilité d'un élément ξ par (y)a équivaut aux conditions : $\nu_{\mathfrak{p}}(\xi) \geqslant \nu_{\mathfrak{p}}(\gamma) + a(p)$ pour tout $\mathfrak{p}$, $\nu_{\mathfrak{p}}\frac{\xi}{\gamma} \geqslant a(p)$ pour tout p, $\frac{\xi}{\gamma} \in \bar{\mathfrak{a}}$, $\xi \in \gamma\bar{\mathfrak{a}}$ (ici, $a(p)$ dtsigne l'exposant de $\mathfrak{p}$ dans la décomposition de a). Il est clair que pour tout diviseur, nous pouvons trouver un élément $y \in \mathfrak{D}^*$ tel que le diviseur (y)a soit entier. La formule (7) montre que pour un tel y on a l'inclusion $\gamma\bar{\mathfrak{a}} \subset \mathfrak{D}$.

DÉFINITION. — ***Soit $\mathfrak{D}$ un anneau de Dedekind, de corps des fractions*** K. ***Un sous-ensemble*** $A \subset K$, ***contenant des éléments différents de 0, est appelé un idéal du corps*** K (par rapport à l'anneau $\mathfrak{D}$) ***s'il possède les propriétés suivantes*** :

1° A ***est un groupe pour l'addition*** ;

2° ***pour tout*** $\alpha \in A$ ***et tout*** $\xi \in \mathfrak{D}$ ***le produit*** $\xi\alpha$ ***appartient à*** A;

3° ***il*** existe ***dans le*** *corps* K ***un élément*** $y \neq 0$ ***tel que*** $\gamma A \subset \mathfrak{D}$.

L'idéal A ***est dit entier s'il est contenu dans*** $\mathfrak{D}$ ***et fractionnaire dans le cas contraire.***

Ainsi, la notion d'idéal entier dans K coïncide avec la notion d'idéal non nul de l'anneau $\mathfrak{D}$.

Si A et B sont deux idéaux du corps K, par définition, leur produit A. B est l'ensemble de tous les éléments $y \in K$ qui s'écrivent sous la forme

$$\gamma = \alpha_1\beta_1 + \ldots + \alpha_m\beta_m,\ m \geqslant 1,\ \alpha_i \in A,\ \beta_i \in B\ (1 \leqslant i \leqslant m).$$

Il est clair que le produit de deux idéaux du corps K est encore un idéal du corps K (dans le cas des idéaux entiers, cette multiplication coïncide avec la multiplication habituelle des idéaux dans les anneaux).

Nous avons vérifié ci-dessus que l'ensemble $\bar{\mathfrak{a}}$ est un idéal du corps K pour tout diviseur a. Supposons que pour deux diviseurs a et $\mathfrak{b}$ on ait l'égalité $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$. Choisissons un élément $y \neq 0$ tel que les diviseurs (y)a et (y)b soient entiers. D'après la formule (7), nous avons $\overline{(\gamma)\mathfrak{a}} = \overline{(\gamma)\mathfrak{b}}$, d'ou (y)a=(y)b et par suite a = b. Ainsi, l'application $a \to \bar{\mathfrak{a}}$ est injective. Soit maintenant A un idéal quelconque du corps K et soit $y \neq 0$ tel que $\gamma A \subset \mathfrak{D}$, alors γA est un idéal non nul de l'anneau et, d'après le théorème 5, il existe un diviseur

entier c tel que $\bar{c} = \gamma A$. Posons $a = c(\gamma^{-1})$; alors $\gamma A = (\gamma)a = \gamma\bar{a}$, d'où $A = \bar{a}$. Ainsi l'application $a \to \bar{a}$ est biunivoque. Si a et $\mathfrak{b}$ sont deux diviseurs, choisissons des éléments $y \neq 0$ et $y' \neq 0$ tels que les diviseurs $(\gamma)a$ et $(\gamma')\mathfrak{b}$ soient entiers; nous aurons, d'après le théorème 5 et la formule (7),

$$\gamma\gamma'\overline{ab} = \overline{(\gamma)a \cdot (\gamma')\mathfrak{b}} = \overline{(\gamma)a} \cdot \overline{(\gamma')\mathfrak{b}} = \gamma a \cdot \gamma'\bar{b} = yy'\bar{a}\bar{b}$$

d'où a. b = $\bar{a}$ b. L'application $a \to \bar{a}$ est donc un isomorphisme. Il en résulte en particulier que les idéaux du corps K forment un groupe pour la multiplication. L'élément unité de ce groupe est l'anneau $\mathfrak{D} = ë$. L'inverse de l'idéal $\bar{a}$ est l'idéal a^{-1}. Formulons le théorème obtenu (qui généralise le théorème 5).

THÉORÈME *6. — Soit $\mathfrak{D}$ un anneau de Dedekind de corps des fractions* K. *Pour tout diviseur* a, *désignons par $\bar{a}$ l'ensemble de tous les éléments du corps* K *qui sont divisibles par* a. *L'application* $a \to \bar{a}$ *est un isomorphisme du groupe des diviseurs du corps* K *sur le groupe des idéaux du corps* K. *Par cet isomorphisme les diviseurs entiers correspondent à des idéaux entiers et vice versa.*

EXERCICES

1. Démontrer que l'anneau $k[x]$ des polynômes à une variable sur un corps quelconque k est de Dedekind.

2. Soient $\mathfrak{O}$ un anneau de Dedekind et k son corps des fractions. Démontrer que la fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{O}$ dans une extension finie quelconque du corps k est aussi un anneau de Dedekind.

3. Démontrer que tout anneau qui admet une théorie des diviseurs avec un nombre fini de diviseurs premiers est un anneau de Dedekind.

4. Démontrer que, dans un anneau de Dedekind, le système des congruences

$$\left.\begin{array}{ll} \xi \equiv \alpha_1 & (\mathrm{mod}\ \mathfrak{a}_1) \\ \cdot\ \cdot\ \cdot & \cdot\ \cdot \\ \xi \equiv \alpha_m & (\mathrm{mod}\ \mathfrak{a}_m) \end{array}\right\}$$

est résoluble si et seulement si $\alpha_i \equiv \alpha_j \pmod{\mathfrak{d}_{ij}}$, $i \neq j$, en désignant par $\mathfrak{d}_{ij}$ le plus grand commun diviseur des diviseurs $\mathfrak{a}_i$ et $\mathfrak{a}_j$.

5. Soient $\mathfrak{D}$ un anneau de Dedekind et a un diviseur de l'anneau $\mathfrak{D}$. Démontrer que l'ensemble des classes résiduelles de $\mathfrak{D}/\mathfrak{a}$ qui sont formées d'éléments premiers avec a constitue un groupe multiplicatif.

6. Démontrer que si f(x) est un polynôme de degré m à coefficients dans un anneau de Dedekind et dont tous les coefficients ne sont pas divisibles par un diviseur premier $\mathfrak{p}$, alors la congruence $f(x) \equiv 0 \pmod{p}$ a au plus m solutions dans $\mathfrak{D}$.

7. Soient $\mathfrak{D}$ un anneau de Dedekind, $\mathfrak{p}$ un diviseur premier de l'anneau $\mathfrak{D}$ et f(x) un polynôme à coefficients dans $\mathfrak{D}$. Démontrer que si pour un élément $\alpha \in \mathfrak{D}$ on a

$$f(u) \equiv 0 \pmod{\mathfrak{p}}, \qquad f'(\alpha) \not\equiv 0 \pmod{\mathfrak{p}},$$

alors pour tout $m \geqslant 2$ il existe un élément $\xi \in \mathfrak{D}$ tel que

$$f(\xi) \equiv 0 \pmod{\mathfrak{p}^m}, \qquad \xi \equiv \alpha \pmod{\mathfrak{p}}.$$

8. Démontrer que, dans un anneau de Dedekind, un idéal est soit principal, soit engendré par deux éléments.

9. Soit $\mathfrak{D}$ un anneau de Dedekind, de corps des fractions K. Démontrer que par l'isomorphisme $a \to \bar{a}$ du groupe des diviseurs du corps K dans le groupe des idéaux du corps K, au plus petit commun multiple des diviseurs correspond l'intersection des idéaux et au plus grand commun multiple la somme des idéaux (La somme A + B de deux idéaux A et B est l'ensemble de toutes les sommes $\alpha + \beta$ pour $a \in A$ et $\beta \in B$).

10. Dans l'anneau $\mathfrak{D} = k[x, y]$ des polynômes à deux variables sur le corps k, la décomposition en facteurs premiers est définie de manière unique et par suite cet anneau admet une théorie des diviseurs. Démontrer que l'idéal A = (x, y) de l'anneau $\mathfrak{D}$, engendré par les variables x et y, ne correspond à aucun diviseur.

11. Démontrer que si un anneau $\mathfrak{D}$ admettant une théorie des diviseurs $\mathfrak{D}^* \to A$ est tel que tout idéal non nul soit de la forme $\bar{a}$ (pour $a \in A$), alors cet anneau est de Dedekind.

12. Démontrer que si dans un anneau $\mathfrak{D}$ tous les idéaux non nuls forment un monoïde à décomposition unique en facteurs premiers (pour la multiplication des idéaux), alors $\mathfrak{D}$ est de Dedekind.

13. Soient $\mathfrak{D}$ un anneau de Dedekind et K son corps des fractions. Si A et B sont des idéaux du corps K (par rapport à $\mathfrak{D}$) on dit que A est divisible par B s'il existe un idéal entier C tel que A = BC. Montrer que A est divisible par B si et seulement si $A \subset B$.

14. Soient $\mathfrak{D}$ un diviseur quelconque admettant une théorie des diviseurs et $\mathfrak{p}$ un diviseur premier de l'anneau $\mathfrak{D}$. Démontrer que l'ensemble $\bar{\mathfrak{p}}$ de tous les éléments $a \in \mathfrak{D}$ qui sont divisibles par $\mathfrak{p}$ est un idéal premier minimal de l'anneau $\mathfrak{D}$ (Un idéal P est dit premier si l'anneau quotient $\mathfrak{D}/\mathbf{P}$ n'a pas de diviseurs de **zéros,** i. e. si le produit de deux éléments de $\mathfrak{D}$ qui n'appartiennent pas à $\mathfrak{p}$ n'appartient pas à $\mathfrak{p}$. Un idéal premier $\mathfrak{p}$ est dit minimal s'il ne contient pas d'autres idéaux premiers que l'idéal nul).

15. Soit $\mathfrak{D}$ un anneau admettant une théorie des diviseurs. Montrer que tout idéal premier P non nul contient un idéal premier de la forme $\bar{\mathfrak{p}}$, où $\mathfrak{p}$ est un diviseur premier de l'anneau $\mathfrak{D}$.

§ 7. — DIVISEURS DANS LES CORPS DE NOMBRES ALGÉBRIQUES

1) Norme absolue d'un diviseur

D'après le théorème 2 du § 5, l'ordre maximum $\mathfrak{D}$ d'un corps K de nombres algébriques est un anneau qui admet une théorie des diviseurs. De plus, dans le § 6, 1), nous avons vu que l'anneau résiduel $\mathfrak{D}/\mathfrak{p}$, modulo un diviseur premier p, est un corps fini et par suite $\mathfrak{D}$ est un anneau de Dedekind.

Considérons un corps K de nombres algébriques comme une extension

(de degré fini) du corps Q des nombres rationnels. Puisque les diviseurs de l'anneau Z des nombres entiers rationnels peuvent être identifiés aux entiers naturels, nous pouvons identifier le groupe de tous les diviseurs (entiers et fractionnaires) du corps Q au groupe multiplicatif des nombres rationnels positifs. On a défini dans le § 5, 2) la notion de norme d'un diviseur d'un anneau $\mathfrak{D}$ pour une extension donnée K/k. Dans le cas d'un corps de nombres algébriques, nous appellerons la norme $N(a) = N_{K/Q}(a)$ du diviseur a de l'ordre $\mathfrak{D}$ pour l'extension K/Q la ***norme absolue*** de a. Nous étendrons cette notion de norme absolue aux diviseurs fractionnaires en posant

$$N_{0^{tt}}^{\mathfrak{m}} = \frac{N(\mathfrak{m})}{N(\mathfrak{n})},$$

pour des diviseurs entiers $\mathfrak{m}$ et n. Il est clair que l'application $a \to N(a)$ est toujours un homomorphisme du groupe de tous les diviseurs du corps K dans le groupe multiplicatif des nombres rationnels positifs.

La norme absolue d'un diviseur principal (ξ), $\xi \in K^*$ est égale à la valeur absolue de la norme du nombre ξ :

$$N((\xi)) = |N(\xi)|. \tag{1}$$

En effet, pour ξ entier, c'est l'égalité (3) du § 5; si maintenant $\xi = \frac{\alpha}{\beta}$, a et β entiers, alors

$$N((\xi)) = \frac{N((\alpha))}{N((\beta))} = \frac{|N(\alpha)|}{|N(\beta)|} = |N(\xi)|.$$

Le degré résiduel f d'un diviseur premier $\mathfrak{p}$ du corps K par rapport à Q est appelé le ***degré résiduel absolu*** ou, plus simplement, le ***degré de*** $\mathfrak{p}$; l'indice de ramification du diviseur premier $\mathfrak{p}$ par rapport à Q est appelé ***l'indice absolu de ramification*** de p. Si $\mathfrak{p}$ divise le nombre premier rationnel p et si le degré de $\mathfrak{p}$ est égal à f, alors, d'après l'égalité (11) du § 5,

$$N(\mathfrak{p}) = p^f. \tag{2}$$

Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ tous les diviseurs premiers du corps K qui divisent p ete,, ... e_m leurs indices de ramification. Alors p admet dans le corps K la décomposition

$$p = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_m^{e_m}.$$

D'après le théorème 7 du § 5, les indices de ramification e_i sont liés aux degrés f_i des diviseurs $\mathfrak{p}_i$ par la relation

$$f_1 e_1 + \ldots + f_m e_m = n = (K : Q). \tag{3}$$

THÉORÈME 1. — ***La norme absolue d'un diviseur entier*** $\mathfrak{a}$ ***d'un corps*** K ***de nombres algébriques est égale au nombre de classes résiduelles de l'ordre maximum*** $\mathfrak{D}$ ***modulo a.***

DÉMONSTRATION. — Démontrons tout d'abord le théorème pour un diviseur premier p. Soit p un nombre premier rationnel divisible par $\mathfrak{p}$; le degré résiduel f du diviseur $\mathfrak{p}$ (d'après la définition du § 5-3)) est égal au degré du corps résiduel $\Sigma_\mathfrak{p}$ de la valuation $\nu_\mathfrak{p}$ sur le corps résiduel Σ_p de la valuation ν_p. Mais Σ_p contient p éléments et par suite $\Sigma_\mathfrak{p}$ est un corps fini à p^f éléments. Il suffit donc de montrer que le corps résiduel $\mathfrak{D}/\mathfrak{p}$ est isomorphe au corps $\Sigma_\mathfrak{p}$, i. e. que l'inclusion isomorphe $\mathfrak{D}/\mathfrak{p} \to \Sigma_\mathfrak{p}$ est surjective. Il suffit donc de montrer que pour tout $\xi \in K$ tel que $\nu_\mathfrak{p}(\xi) \geqslant 0$, il existe $\alpha \in \mathfrak{D}$ tel que

$$\nu_\mathfrak{p}(\xi - \alpha) \geqslant 1.$$

Désignons par $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ tous les diviseurs premiers du corps K tels que

$$\nu_{\mathfrak{q}_i}(\xi) = -k_i < 0;$$

d'après le théorème 3, § 6, il existe un élément y de l'ordre $\mathfrak{D}$ tel que

$$\gamma \equiv 1 \pmod{\mathfrak{p}}$$
$$\gamma \equiv 0 \pmod{\mathfrak{q}_i^{k_i}}, \quad i = 1, \ldots, s.$$

Il est clair que $\alpha = \gamma\xi \in \mathfrak{D}$ et $\nu_\mathfrak{p}(\xi - a) \geqslant 1$. Le théorème 1 est donc démontré pour un diviseur premier.

Pour démontrer le théorème 1 dans le cas général, il suffit maintenant de montrer que s'il est vrai pour deux diviseurs entiers a et $\mathfrak{b}$, il est aussi vrai pour le produit ab. D'après la condition 3° du théorème 4 du § 3, il existe un élément $y \neq 0$ de l'ordre maximum $\mathfrak{D}$ tel que $\mathfrak{a} | y$, les diviseurs $(\gamma)\mathfrak{a}^{-1}$ et b étant premiers entre eux. Soient $\alpha_1, \ldots, a$, ($r = N(a)$) un système complet de résidus de l'anneau $\mathfrak{D}$ modulo a et $\beta_1, \ldots, \beta_s$ ($s = N(b)$) un système complet de résidus modulo b. Montrons alors que les rs nombres

$$\alpha_i + \beta_j\gamma \tag{4}$$

forment un système complet de résidus modulo ab. Soit α un élément quelconque $\mathfrak{D}$; pour un certain i ($1 \leqslant i \leqslant r$), on a

$$a \equiv \alpha_i \pmod{a}.$$

Considérons la congruence

$$\gamma\xi \equiv \alpha - \alpha_i \pmod{ab}. \tag{5}$$

Puisque, d'après le choix de y, le plus grand commun diviseur des diviseurs (y) et ab, égal à a, divise $a - \alpha_i$, alors, d'après le théorème 4 du $6,

cette congruence a une solution $\xi \in \mathfrak{D}$. Soit j ($1 \leqslant j \leqslant s$) tel que $\xi \equiv \beta_j \pmod{\mathfrak{b}}$; on a alors $\gamma\xi \equiv \gamma\beta_j \pmod{ab}$. D'après (5), nous avons donc la congruence

$$\alpha \equiv \alpha_i + \gamma\beta_j \pmod{ab}.$$

Ainsi, toute classe résiduelle modulo ab contient un représentant de la forme (4). Il reste à vérifier que les nombres (4) sont deux à deux non congrus modulo ab. Supposons

$$\alpha_i + \gamma\beta_j \equiv \alpha_k + \gamma\beta_l \pmod{ab}.$$

Puisque cette congruence est aussi satisfaite modulo a, alors $y \equiv 0 \pmod{a}$ entraîne $\alpha_i \equiv \alpha_k \pmod{a}$ d'où $i = k$. Nous obtenons donc

$$\gamma(\beta_j - \beta_l) \equiv 0 \pmod{ab}. \qquad (6)$$

Soit $\mathfrak{p}$ un diviseur premier figurant respectivement dans les diviseurs a et b avec des exposants a et $b > 0$. D'après la condition $\nu_\mathfrak{p}(\gamma) = a$, (6) entraîne $\nu_\mathfrak{p}(\beta_j - \beta_l) \geqslant b$. Puisque cette inégalité a lieu pour tout diviseur premier $\mathfrak{p}$ qui figure dans b avec un exposant > 0, alors $\beta_j \equiv \beta_l \pmod{b}$, d'où $j = 1$.

Ainsi les nombres (4) forment bien un système complet de résidus modulo ab et par suite le nombre des classes résiduelles de $\mathfrak{D}$ modulo ab est égal à $rs = N(a)N(b) = N(ab)$.

Le théorème 1 est complètement démontré.

Comme dans le § 6-3), pour un diviseur quelconque a (entier ou fractionnaire) du corps K, désignons par $\bar{\mathfrak{a}}$ l'idéal correspondant du corps K formé de tous les nombres $a \in K$ divisibles par a. Soit y choisi tel que $\gamma\bar{\mathfrak{a}} \subset \mathfrak{D}$. D'après le corollaire du théorème 2 du § 2, chapitre II, l'ensemble $\gamma\bar{\mathfrak{a}}$ est un module du corps K (sous-module de l'anneau $\mathfrak{D}$); mais alors l'idéal $\bar{\mathfrak{a}}$ est aussi un module du corps K. Si $\alpha \in \bar{\mathfrak{a}}$, $\alpha \neq 0$ et si $\omega_1, \ldots, \omega_n$ est une base de l'anneau $\mathfrak{D}$, tous les produits $\alpha\omega_1, \ldots, \alpha\omega_n$ appartiennent à $\bar{\mathfrak{a}}$ et par suite $\bar{\mathfrak{a}}$ contient $n = (K : Q)$ nombres du corps K linéairement indépendants. Nous avons démontré ainsi que, pour tout diviseur a, l'idéal $\bar{\mathfrak{a}}$ est un module complet du corps K. Il est clair que son anneau de stabilisateurs est l'ordre maximum du corps K. Réciproquement, si A est un module complet du corps K dont l'anneau de stabilisateurs est égal à l'ordre maximum $\mathfrak{D}$, alors A satisfait aux trois conditions de la définition d'un idéal (cf. § 6-4)). Ainsi l'ensemble de tous les idéaux $\bar{\mathfrak{a}}$ coïncide avec l'ensemble de tous les modules complets du corps K qui sont associés à l'ordre maximum $\mathfrak{D}$.

Au point 1) du § 6, chapitre II, nous avons introduit la notion de norme d'un module complet dans un corps de nombres algébriques. On peut donc parler de la norme de l'idéal $\bar{\mathfrak{a}}$. Montrons que la norme de tout diviseur est égale à la norme de l'idéal correspondant

$$N(a) = N(\ddot{U}). \qquad (7)$$

Pour les diviseurs entiers, cela résulte du théorème 1 de ce paragraphe et du théorème 1, § 6, chapitre II. Si le diviseur a est fractionnaire, on peut trouver $\gamma \in K^*$ tel que le diviseur $(\gamma^{-1})\mathfrak{a} = \mathfrak{b}$ soit entier. D'après le théorème 2, § 6, chapitre II, nous avons

$$N(a) = N(b)\,|N(\gamma)| = N(b)\,|N(\gamma)| = N(\gamma\bar{b}) = N(\gamma\bar{b}) = N(Ü)$$

ce qui démontre la formule (7) dans tous les cas.

Comme application très simple de la notion de norme, donnons une estimation précise du nombre $w(a)$ d'éléments non associés d'un ordre maximum dont la norme est égale à a en valeur absolue (la démonstration du théorème 5, § 2, chapitre II donnait l'estimation $w(a) \leqslant a^n$).

Désignons par $\psi(a)$ le nombre des diviseurs entiers de norme a. Puisque les nombres α et β sont associés si et seulement si les diviseurs principaux (α) et (β) sont égaux, nous avons, d'après la formule (1),

$$\omega(a) \leqslant \psi(a).$$

Cherchons donc une estimation du nombre $\psi(a)$. Supposons

$$a = p_1^{k_1} \dots p_s^{k_s},$$

pour des nombres premiers p_i distincts. Si $N(\mathfrak{a}) = a$, alors $\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_s$, où $\mathfrak{a}_i$ contient seulement des diviseurs premiers $\mathfrak{p}$ qui divisent p_i. D'après la formule (2) et la multiplicativité de la norme, nous avons $N(\mathfrak{a}_i) = p_i^{k_i}$, d'où $\psi(a) = \psi\left(p_1^{k_1}\right) \dots \psi\left(p_s^{k_s}\right)$; il suffit donc d'obtenir une estimation de $\psi(p^k)$. Soient $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ tous les diviseurs premiers qui divisent p et soient $f_1, \dots, f_m$ leurs degrés. D'après l'égalité

$$N\left(\mathfrak{p}_1^{x_1} \dots \mathfrak{p}_m^{x_m}\right) = p^{f_1 x_1 + \dots + f_m x_m},$$

on est ramené à trouver une estimation du nombre de solutions de l'équation

$$f_1 x_1 + \dots + f_m x_m = k,$$

telles que $x_i \geqslant 0$. Puisque $0 \leqslant x_i \leqslant k$, le nombre de ces solutions ne dépasse pas $(k+1)^m$. Mais $m \leqslant n = (K : Q)$ et par suite

$$\psi(a) \leqslant \left((k_1 + 1) \dots (k_s + 1)\right)^n.$$

Comme on le sait, l'expression contenue dans la parenthèse de droite est égale au nombre $\tau(a)$ de tous les diviseurs de a. Nous avons ainsi obtenu l'estimation

$$o(a) \leqslant \psi(a) \leqslant \left(\tau(a)\right)^n. \qquad (8)$$

Pour comparer l'estimation (8) à l'estimation précédente $\omega(a) \leqslant a^n$, remarquons que, pour tout $\varepsilon > 0$ aussi petit que l'on veut, le rapport $\frac{\tau(a)}{a^\varepsilon}$ tend vers 0 pour $a \to \infty$.

2) Classes de diviseurs

DÉFINITION. — ***Deux diviseurs*** $\mathfrak{a}$ ***et*** $\mathfrak{b}$ ***d'un corps*** K ***de nombres algébriques sont dits équivalents, et on note*** $a \sim b$, ***s'ils diffèrent entre eux par un diviseur principal :*** $a = b(a)$, $a \in K^*$. ***L'ensemble de tous les diviseurs du corps*** K ***qui sont équivalents à un diviseur donné a s'appelle une classe de diviseurs et se désigne par [a].***

En terme de théorie des groupes, l'équivalence $a \sim \mathfrak{b}$ indique que les diviseurs a et b appartiennent à la même classe quotient du groupe de tous les diviseurs par le sous-groupe des diviseurs principaux. L'égalité de deux classes [a] = [b] équivaut bien entendu à l'équivalence $a \sim \mathfrak{b}$.

Pour deux classes de diviseurs [a] et [b], posons

$$[a].\ [b] = [ab].$$

Il est facile de vérifier que le produit ci-dessus ne dépend pas du choix des représentants a et $\mathfrak{b}$ et que l'ensemble des classes forment ainsi un groupe (commutatif), appelé le groupe des classes de diviseurs du corps K. L'élément unité est la classe [e] constituée par tous les diviseurs principaux; l'inverse de la classe [a] est la classe [a-l].

En termes de théorie de groupe, le groupe des classes de diviseurs est le groupe quotient du groupe de tous les diviseurs par le sous-groupe de tous les diviseurs principaux. Le groupe des classes de diviseurs et en particulier son ordre, qui est le nombre de classes de diviseurs sont des importantes caractéristiques arithmétiques du corps de nombres algébriques K. Si le nombre des classes de diviseurs est égal à 1, cela signifie que tous les diviseurs sont principaux et cela équivaut à l'unicité de la décomposition en facteurs premiers dans l'anneau des nombres entiers du corps K (théorème 2 du § 3).

Ainsi, le problème de savoir si la décomposition des nombres entiers du corps K en facteurs premiers est unique, est un cas particulier du problème de la détermination du nombre des classes de diviseurs de ce corps. Démontrons que ce nombre est toujours fini.

THÉORÈME 2. — ***Le groupe des classes de diviseurs de tout corps de nombres algébriques est fini.***

DÉMONSTRATION. — Il résulte facilement de la définition de l'équivalence des diviseurs que les diviseurs a et $\mathfrak{b}$ sont équivalents si et seulement si les idéaux correspondants $\mathfrak{a}$ et b sont semblables (au sens de la similitude des modules, cf. 3), § 1, chap. II). A la répartition des diviseurs en classes de diviseurs équivalents correspond donc la répartition des idéaux du corps K (i. e. des modules complets du corps K dont l'anneau de stabilisateurs est l'ordre maximum du corps K) en classes d'idéaux semblables. Mais, d'après le théorème 3 du § 6, chapitre II, le nombre des classes de modules semblables associés à un ordre donné est fini; le théorème 2 est ainsi démontré.

Remarque 1. — Le théorème 2 a été obtenu très simplement comme corollaire du théorème 3, § 6, chapitre II et la démonstration de ce dernier reposait sur le lemme de Minkowski pour un corps convexe. Ainsi, finalement, la démonstration du théorème 2 repose sur le lemme de Minkowski.

Remarque 2. — L'examen de la démonstration du théorème 3, § 6, chapitre II permet d'obtenir un énoncé plus précis du théorème 2 : dans toute classe de diviseurs d'un corps K de nombres algébriques de degré $n = s + 2t$, il existe un diviseur entier de norme $\leqslant \frac{2^t}{0^\pi}\sqrt{|D|}$, D discriminant du corps (i. e. le discriminant de l'anneau de tous les nombres entiers du corps K). En effet, soit [b] une classe quelconque de diviseurs. Il existe un idéal $A = \mathfrak{a}\mathfrak{b}^{-1}$ semblable à l'idéal $\mathfrak{b}^{-1}$ tel que $A \supset \mathfrak{D}$ et $(A : \mathfrak{D}) \leqslant \frac{2^t}{0^\pi}\sqrt{|D|}$ (cf. démonstration du théorème 3, § 6, chap. II). Puisque l'idéal A contient $\mathfrak{D}$, le diviseur correspondant est l'inverse d'un diviseur entier : $A = \mathfrak{a}^{-1}$, a entier. De l'égalité a-' = $\mathfrak{b}^{-1}$ résulte que $a(a)$ = b, i. e. le diviseur entier a appartient à la classe [b]; par suite (exercice 2),

$$N(\mathfrak{a}) = \frac{N(e)}{N(\mathfrak{a}^{-1})} = (\mathfrak{a}^{-1} : e) = (A : \mathfrak{D}) \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|D|}.$$

THÉORÈME 3. — *Si le nombre de classes de diviseurs du corps* K *est égal à h, alors la* $h^{\text{ième}}$ *puissance de tout diviseur est un diviseur principal.*

DÉMONSTRATION. — Ce théorème est un simple corollaire d'un théorème Clémentaire de théorie des groupes : l'ordre de tout élément d'un groupe fini divise le nombre d'éléments de ce groupe. Soit a un diviseur quelconque. Puisque $[\mathfrak{a}]^h$ est l'élément unité du groupe des classes de diviseurs, alors $[\mathfrak{a}^h]$ = [e] et par suite le diviseur $\mathfrak{a}^h$ est principal.

COROLLAIRE. — *Si le nombre h des classes de diviseurs du corps* K *n'est pas divisible par un nombre premier l et si le diviseur* $\mathfrak{a}^l$ *est principal, alors* a *est aussi principal.*

En effet, d'après l'hypothèse, il existe des nombres entiers rationnels u et v tels que $lu + hv = 1$. Puisque les diviseurs $\mathfrak{a}^l$ et $\mathfrak{a}^h$ sont principaux (le

premier par hypothèse et le second d'après le théorème 3), alors $\mathfrak{a}^{lu}$ et $\mathfrak{a}^{hv}$ sont aussi principaux; leur produit $a^{lu+hv} = \mathfrak{a}$ est donc aussi principal.

D'après l'exercice 20, on peut plonger tout corps K de nombres algébriques dans un corps plus grand K tel que tout diviseur du corps K soit un diviseur principal du corps $\overline{K}$. Cependant, on ne peut pas affirmer que tous les diviseurs du corps $\overline{K}$ sont principaux; en effet, on a montré récemment (E. S. Golod et 1. R. Chafarevitch) il existe des corps de nombres algébriques (par exemple $K = \mathbf{Q}\sqrt{-3.5.7.11.13.17.19}$) qui n'admettent pas d'extension de degré fini pour laquelle $h = 1$. La question suivante est restée jusqu'à présent ouverte : existe-t-il une infinité de corps tels que $h = 1$? Les résultats connus montrent que ces corps semblent assez fréquents (cf. tables donnant les valeurs de h pour des corps quadratiques réels et des corps cubiques complètement réels).

On connaît très peu de résultats généraux sur le nombre h et le groupe des classes de diviseurs pour des corps quelconques (bien qu'on ait trouvé des formules pour certaines classes de corps, par exemple les corps quadratiques ou cycliques, cf. chap. V). Citons cependant le théorème de Siegel et Brauer qui affirme que pour tout les corps de degré fixé n, le nombre h des classes de diviseurs, le rtgulateur R et le discriminant D sont liés par la relation asymptotique suivante :

$$\frac{\text{Log } (hR)}{\text{Log } \sqrt{|D|}} \to 1 \quad \text{pour} \quad |D| \to \infty \qquad (*)$$

(R. Brauer, On the zeta-functions on algebraic number fields. *Amer. J. Math.*, 1947, 69, n° 2, 243-250). Puisque pour des corps quadratiques imaginaires, le régulateur est égal à 1, alors (*) entraîne que, pour ces corps, $h \to \infty$ pour $|D| \to \infty$. En particulier, nous obtenons qu'il existe seulement un nombre fini de corps quadratiques imaginaires tels que $h = 1$. Dans les limites des tables situées à la fin du volume, on a en évidence 9 corps quadratiques imaginaires tels que $h = 1$ (leurs discriminants sont égaux à -3, -4, -7, -8, -11, -19, -43, -67, -163). On a montré qu'en dehors de ces 9 corps, il existe au plus un autre corps quadratique imaginaire tel que $h = 1$, mais on ne sait pas s'il existe effectivement. Dans le cas général, la formule (*) ne nous permet pas des conclusions sur la grandeur de h puisqu'on ne connaît pas le comportement de R.

3) Application au théorème de Fermat

Les résultats qui précèdent nous permettent de démontrer le théorème 1 du § 1 pour une classe élargie d'exposants 1.

THÉORÈME 4. — *Soit l un nombre premier impair et ζ une racine primitive de degré l de* 1. *Si le nombre des classes de diviseurs du corps $\mathbf{Q}(\zeta)$ n'est pas*

divisible par l, alors le premier cas du théorème de Fermat est vrai pour l'exposant 1.

DÉMONSTRATION. — Supposons, en contradiction avec le théorème, qu'il existe des nombres entiers rationnels x, y, z non divisibles par l et tels que

$$x^l + y^l = z^l.$$

On peut supposer de plus que x, y, z sont premiers entre eux deux à deux. Dans l'anneau des nombres entiers du corps Q(C), cette égalité peut s'écrire

$$\prod_{k=0}^{l-1}(x + \zeta^k y) = z^l.$$

Puisque $x + y \equiv x^l + y^l = z^l \equiv z \pmod{l}$ et z non divisible par l, alors $x+y$ n'est pas non plus divisible par l. Mais alors, comme nous l'avons vu dans la démonstration du lemme 5, § 1, pour $m \not\equiv n \pmod{l}$, il existe des nombres ζ_0 et η_0 dans l'anneau $\mathbf{Z}[\zeta]$ tel que

$$(x + \zeta^n y)\xi_0 + (x + \zeta^m y)\eta_0 = 1.$$

Par suite, les diviseurs principaux $(x + \zeta^k y)$ (k = 0, 1, . . . , $l - 1$) sont premiers entre eux deux à deux. Puisque leur produit est une puissance $l^{\text{ième}}$ (du diviseur (z)), alors chacun de ces diviseurs pris séparément doit être une puissance $l^{\text{ième}}$. En particulier

$$(x + \zeta y) = a^l,$$

où a est un diviseur entier du corps Q(C). Par hypothèse, le nombre de classes de diviseurs du corps $\mathbf{Q}(\zeta)$ n'est pas divisible par l et par suite, d'après le corollaire du théorème 3, le diviseur a est principal, i. e. a = (a), a appartenant à l'ordre maximum $\mathfrak{D} = \mathbf{Z}[\zeta]$ du corps $\mathbf{Q}(\zeta)$. L'égalité

$$(x + \zeta y) = (\alpha^l)$$

entraîne que

$$x + \zeta y = \varepsilon\alpha^l$$

où ε est une unité de l'anneau $\mathfrak{D}$. De manière analogue, on obtient

$$x - \zeta z = \varepsilon_1\alpha_1^l$$

($\alpha_1 \in \mathfrak{D}$ et ε_1 est une unité dans $\mathfrak{D}$). Nous avons obtenu des égalités qui, comme nous l'avons montré dans le § 1, 3), sont incompatibles (dans cette partie de la démonstration du théorème 1, § 1, nous n'avons pas utilisé l'unicité de la décomposition). Le théorème 4 est ainsi démontré.

Les nombres premiers impairs l tels que le nombre de classes de diviseurs du corps $\mathbf{Q}(\zeta)$ n'est pas divisible par l sont dits ***réguliers*** et les autres ***irré-***

guliers. Kummer a obtenu un critère simple (exposé dans le chapitre V, § 6,4)) permettant de reconnaître si un nombre premier donné l est régulier ou pas. Avec ce critère, on peut montrer que parmi les nombres premiers inférieurs à 100, seuls les trois nombres 37, 59 et 67 sont irréguliers et tous les autres sont réguliers. Pour se rendre compte de l'amélioration obtenue en remplaçant le théorème 1 du § 1 par le théorème 4, remarquons que parmi les nombres premiers impairs < 100, seuls les sept premiers nombres 3, 5, 7, 11, 13, 17, 19 conduisent à un corps Q(T), $\zeta^l = 1$, pour lequel il y a unicité de la décomposition en facteurs premiers dans l'anneau $\mathfrak{D}$.

Dans son premier ouvrage, Kummer a émis la conjecture qu'il existait seulement un nombre fini de nombres premiers irréguliers. Dans un ouvrage beaucoup plus tardif, il est revenu sur cette conjecture et l'a remplacé par la suivante : les nombres réguliers sont en moyenne deux fois plus fréquents que les irréguliers (sur un intervalle assez grand). Récemment, on a vérifié avec des machines à calculer électroniques que parmi les 550 nombres premiers impairs $\leqslant 4001$, il en existe 216 irréguliers et 334 réguliers. La table de tous les nombres premiers irréguliers $\leqslant 4001$ est donnée à la fin de ce livre. Jensen (cf. chap. V, § 7, 2)) a montré qu'il existe une infinité de nombres premiers irréguliers mais, actuellement, on ne sait pas s'il existe une infinité de nombres premiers réguliers.

Le premier cas du théorème de Fermat pour un exposant l est aussi lié au nombre h_0 de classes de diviseurs du corps $\mathbf{Q}(\zeta + \zeta^{-1}) = \mathrm{Q}\left(\cos\frac{2\pi}{l}\right)$. Il est facile de voir que $\mathbf{Q}(\zeta + \zeta^{-1})$ est formé de tous les nombres réels du corps $\mathbf{Q}(\zeta)$. Vandiver a démontré que si le nombre h_0 de classes de diviseurs du corps $\mathbf{Q}(\zeta + \zeta^{-1})$, $\zeta^l = 1$, n'est pas divisible par le nombre premier l, alors le premier cas du théorème de Fermat est vrai (H. S. Vandiver, Fermat's last theorem and the second factor in the cyclotomic class number. *Bull. Amer. Math.* Soc., 1934, 40, n° 2, 118-126). Cependant, on ne sait pas s'il existe des nombres premiers l pour lesquels le nombre h_0 de classes de diviseurs du corps $\mathbf{Q}(\zeta + \zeta^{-1})$ soit divisible par l; on a seulement vérifié qu'il n'en existe pas parmi les nombres $\leqslant 4001$.

Signalons ici d'autres faits relatifs au premier cas du théorème de Fermat. Wieferich a démontré que le premier cas du théorème de Fermat est vrai pour tous les nombres premiers l tels que $2^{l-1} \not\equiv 1 \pmod{l^2}$ (A. Wieferich, Zum letzten Fermatschen Theorem. *J. für Math.*, 1909, 136, 293-302). Pour se rendre compte de l'importance de ce résultat, remarquons que parmi les nombres premiers $l \leqslant 200\,183$, il y en a seulement deux (1093 et 3511) qui satisfont à la congruence $2^{l-1} \equiv 1 \pmod{l^2}$ (Erna H. Pearson, Math. *Comp.*, 1963, 17, n° 82, 194-195). Cependant, on ne sait pas s'il existe ou non une infinité de tels l. D'autres auteurs ont établi le premier cas du théorème de Fermat pour tous les l tels que $q^{l-1} \not\equiv 1 \pmod{l^2}$, q nombre pre-

mier $\leqslant 43$ (D. Mirimanoff, H. S. Vandiver, G. Frobenius, F. Pollaczek, T. Morishima, J. B. Rosser). Cela permet de démontrer le premier cas du théorème de Fermat pour tous les nombres premiers $< 253\ 747\ 889$ (D. H. Lehmer, Emma Lehmer, On the first case of Fermat's last theorem, *Bull. Amer. Math. Soc.*, 1941, 47, n° 2, 139-142).

4) Questions d'effectivité

Jusqu'ici, nous n'avons pas étudié de méthodes de constructions effectives de diviseurs pour un corps donné de nombres algébriques. Puisque les diviseurs sont complètement définis par la connaissance des diviseurs premiers et que ces derniers, à leur tour, sont définis par des valuations du corps K, tout revient à construire effectivement tous les prolongements au corps K de la valuation ν_p du corps Q (pour tout p fixé). De plus, en dehors de la détermination des diviseurs premiers, il est important d'avoir un algorithme fini pour calculer le nombre h de classes de diviseurs du corps K.

Nous montrerons ici qu'on peut construire les prolongements de la valuation ν_p et calculer le nombre h par un nombre fini d'opérations.

Soit $\mathfrak{O}_p$ l'anneau de la valuation ν_p dans le corps Q (i. e. l'anneau des nombres rationnels p-entiers, cf. chap. 1, § 3-2)) et $\mathfrak{D}_p$ sa fermeture intégrale dans le corps K. Tout nombre $\xi \in \mathfrak{D}_p$ est racine d'un polynôme

$$t^k + a_1 t^{k-1} + \ldots + a_k$$

à coefficients a_i p-entiers. Si nous désignons par m le dénominateur commun des a_i, le nombre $m\xi = a$ sera une racine du polynôme

$$t^k + m a_1 t^{k-1} + \ldots + m^k a_k,$$

à coefficients dans $\mathbf{Z}$, i. e. appartiendra à l'anneau $\mathfrak{D}$ des nombres entiers du corps K (l'ordre maximum). Bien entendu, la réciproque est vraie : si $a \in \mathfrak{D}$ et si m est un entier rationnel non divisible par p, alors $\frac{\alpha}{m} \in \mathfrak{D}_p$. Ainsi, l'anneau $\mathfrak{D}_p$ est l'ensemble des nombres $\frac{\alpha}{m}$, $a \in \mathfrak{D}$ et m entier rationnel non divisible par p. Choisissons une base fondamentale $\omega_1, \ldots, \omega_n$ du corps K (i. e. une base de l'anneau $\mathfrak{D}$ sur $\mathbf{Z}$). Alors, d'après ce qu'on a vu, un nombre $\xi \in$ K, écrit sous la forme

$$\xi = a_1\omega_1 + \ldots + a_n\omega_n \qquad (a_j \in \mathbf{Q}),$$

appartient à l'anneau $\mathfrak{D}_p$ si et seulement si tous les a_i sont p-entiers.

D'après le théorème 7 du § 4, nous avons réduit notre premier problème (i. e. la construction des prolongements de la valuation ν_p) à la recherche d'un système complet d'éléments premiers deux à deux non associés

$\pi_1, \ldots, \pi_m$ de l'anneau $\mathfrak{D}_p$. En effet, si on a trouvé de tels éléments π_i, alors tout $\xi \in \mathfrak{D}_p^*$ admet la décomposition

$$\xi = \eta \pi_1^{k_1} \ldots \pi_m^{k_m} \tag{9}$$

où η est une unité de $\mathfrak{D}_p$. Il suffit pour cela de diviser ξ par chacun des π_i jusqu'à ce que le quotient de la division n'appartienne plus à l'anneau $\mathfrak{D}_p$; au bout d'un nombre fini de divisions, on obtient un nombre η qui n'est divisible par aucun des éléments premiers π et par suite c'est une unité dans $\mathfrak{D}_p$. Puisque tout élément de K est le quotient de deux éléments de $\mathfrak{D}_p$ (et de $\mathfrak{D}$) on obtient de la même manière une représentation de la forme (9) pour tout $\xi \in$ K*. Mais cela définit toutes les valuations $\nu_1, \ldots, \nu_m$ qui prolongent ν_p. Les indices de ramification $e_1, \ldots, e_m$ de ces valuations sont définis, comme nous le savons, par la décomposition $p = \varepsilon \pi_1^{e_1} \ldots \pi_m^{e_m}$ (ε unité dans $\mathfrak{D}_p$).

Soit π un élément premier quelconque de l'anneau $\mathfrak{D}_p$; puisque les entiers rationnels non divisibles par p sont des unités de $\mathfrak{D}_p$, on peut supposer que $\pi \in \mathfrak{D}$. Pour tout $\alpha \in \mathfrak{D}$, le nombre $\pi + p^2\alpha = \pi\left(+ \frac{p^2}{\pi}\alpha\right)$ sera associé à π puisque le facteur $1 + \frac{p^2}{\pi}\alpha \in \mathfrak{D}_p$ n'est divisible par aucun des éléments premiers $\pi_1, \ldots, \pi_m$. Ainsi nous pouvons choisir un système complet d'éléments premiers non associés deux à deux $\pi_1, \ldots, \pi_m$ parmi les nombres

$$x_1\omega_1 + \ldots + x_n\omega_n,$$

avec $0 \leqslant x_i < p^2$ ($i = 1, \ldots, n$). Puisque le nombre de tels éléments est fini, on peut trouver par un nombre fini d'opérations le système d'éléments premiers cherché; on définit par là même les valuations $\nu_1, \ldots, \nu_n$.

Pour trouver les degrés $f_1, \ldots, f_m$ des diviseurs premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ correspondant aux valuations trouvées $\nu_1, \ldots, \nu_m$, on peut utiliser le théorème 5, § 5. D'après ce résultat, pour tout élément premier $\pi_i \in \mathfrak{D}$ de l'anneau $\mathfrak{D}_p$, nous avons

$$N(\pi_i) = p^{f_i}a,$$

où a est un entier rationnel non divisible p; ainsi, $f_i = \nu_p(N(\pi_i))$.

Passons à notre second problème, i. e. le calcul effectif du nombre h des classes de diviseurs.

Dans la remarque 2 qui suit le théorème 2, on a vu que dans toute classe de diviseurs il existe un diviseur entier a tel que

$$N(a) \leqslant \frac{2}{0\pi}\sqrt[t]{|D|}. \tag{10}$$

(cf. exercice 9). Soient

$$\mathfrak{a}_1, \ldots . \mathfrak{a}_N \tag{11}$$

tous les diviseurs entiers du corps K qui satisfont à la condition (10). Le nombre de ces diviseurs est fini puisqu'il existe dans K seulement un nombre fini de diviseurs entiers de norme donnée (pour a fixé, l'égalité

$$N\left(\mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_r^{k_r}\right) = a$$

entraîne la finitude de la quantité des nombres premiers p divisibles par $\mathfrak{p}$ et des exposants positifs k_i). Pour calculer le nombre des classes de diviseurs, il faut extraire du système (11) un sous-système maximal de diviseurs deux à deux non équivalents. Pour ce faire, il faut savoir reconnaître si deux diviseurs donnés sont équivalents ou pas. Soient a et $\mathfrak{b}$ deux diviseurs entiers. Choisissons dans K un nombre $\beta \neq 0$ divisible par $\mathfrak{b}$ et considérons le diviseur $\mathfrak{a}\mathfrak{b}^{-1}(\beta)$. Les diviseurs a et $\mathfrak{b}$ sont équivalents si et seulement si le diviseur entier $\mathfrak{a}\mathfrak{b}^{-1}(\beta)$ est ***principal.*** Ainsi, il faut savoir reconnaître si un diviseur entier donné est principal.

Désignons par a la norme du diviseur entier a. Dans le chapitre II, § 5, 4), on a montre qu'on peut, par un nombre fini d'opérations, trouver dans l'ordre maximum $\mathfrak{D}$ des éléments

$$\alpha_1, \ldots, \alpha_r \tag{12}$$

de norme $\pm a$ et tels que tout $\alpha \in \mathfrak{D}$ de norme $\pm$ a soit associé à l'un d'entre eux. Si le diviseur a est principal, i. e. a = (a) ($a \in \mathfrak{D}^*$), alors $|N(a)| = a$ et par suite, pour un certain i, on aura a = (α_i). Ainsi, si on a déterminé le système (12), pour savoir si a est principal il suffit de le comparer aux diviseurs principaux $(\alpha_1), \ldots, (\alpha_r)$.

Ainsi, pour un corps donné K, on peut calculer le nombre h par un nombre fini d'opérations.

Soit maintenant θ un nombre entier primitif d'un corps K de nombres algébriques, de degré n. L'indice de l'ordre $\mathfrak{D}' = \{1, \theta, \ldots, \theta^{n-1}\}$ dans l'ordre maximum $\mathfrak{D}$ est appelé ***l'indice*** de θ.

LEMME. — ***Si le diviseur premier $\mathfrak{p}$ ne divise pas l'indice k du nombre θ, alors tout nombre entier $a \in K$ est congru modulo $\mathfrak{p}$ à un nombre de l'ordre***

$$\mathfrak{D}' = \{1, \theta, \ldots, \theta^{n-1}\}.$$

En effet, puisque $\mathfrak{p} \nmid k$, alors il existe un entier x tel que $kx \equiv 1 \pmod{p}$. Posons $y = kxa$. Puisque $ka \in \mathfrak{D}$, alors y appartient aussi à $\mathfrak{D}'$ et $a \equiv y \pmod{\mathfrak{p}}$.

COROLLAIRE. — ***Si $\mathfrak{p}$ ne divise pas le discriminant*** $D' = D(1, \theta, \ldots, \theta^{n-1})$, ***alors tout entier $a \in K$ est congru modulo $\mathfrak{p}$ à un nombre de l'ordre***

$$\mathfrak{D}' = \{1, \theta, \ldots, \theta^{n-1}\}.$$

Si $\mathfrak{p}$ ne divise pas D', alors $\mathfrak{p}$ ne divise pas non plus l'indice k du nombre θ (cela résulte de la formule $D' = Dk^2$, où D est le discriminant du corps K; cf. lemme 1, § 6, chap. II et égalité (12) du § 2 de l'appendice).

Supposons maintenant que le nombre premier rationnel p ne figure pas dans l'indice du nombre $\theta \in K$. Soient $\mathfrak{p}$ un diviseur premier de degré f qui divise p et $\bar{\theta}$ la classe résiduelle de θ modulo $\mathfrak{p}$. D'après le lemme, le corps résiduel $\mathfrak{D}/\mathfrak{p}$ est engendré par la classe résiduelleë de représentant θ. Par suite, si $x_1, \ldots, x_f$ parcourent indépendamment l'un de l'autre un système complet de résidus modulo p (dans l'anneau Z), alors, parmi les nombres

$$\gamma = x_1 + x_2\theta + \ldots + x_f\theta^{f-1} + \theta^f,$$

il en existe un et un seul qui soit divisible par p. Après avoir calculé les normes N(y), nous pouvons facilement en déduire ceux de ces nombres y qui sont divisibles par des diviseurs premiers figurant dans p. Si par exemple pourf = 1 nous avons trouvé s nombres y dont la norme est divisible par p seulement au premier degré, nous avons déterminé s diviseurs premiers figurant au premier degré dans p. Supposons que ces diviseurs premiers de degré 1 qui figurent dans p ont été trouvés (par la détermination des nombres $\beta_1, \ldots, \beta_u$ de normes pa_i, $p \nmid a_i$). Prenant maintenant $f = 2$, isolons les nombres y dont la norme est divisible par p^2; nous pouvons libérer ces nombres y des diviseurs premiers de degré 1 en les divisant par les β^i trouvés précédemment et si, après cela, $N(y) = p^2\frac{b}{c}$ ((bc, p) = 1), alors y contient un diviseur premier de degré 2. Ce moyen nous permet donc de trouver tous les diviseurs premiers de degré 2 figurant dans p ; nous choisirons alors f = 3, etc. Bien entendu, les calculs sont assez longs. Des précisions complémentaires sont données dans les exercices 25-27.

Exemple 1. — Déterminons les décompositions des nombres 2, 3, 5, 7 comme produits de diviseurs premiers dans le corps de degré 5 : Q(O), $\theta^5 = 2$. Le discriminant $D(1, \theta, \theta^2, \theta^3, \theta^4)$ est égal à 2^45^5 ; par suite, seuls les nombres premiers 2 et 5 peuvent figurer dans l'indice du nombre 8. Mais le nombre 2 ne figure pas dans cet indice d'après l'exercice 15. Puisque $\theta^5 = 2$, alors $\mathfrak{p}_2 = (\theta)$ est un diviseur premier de degré 1 et nous avons la décomposition

$$2 = \mathfrak{p}_2^5.$$

Les égalités

$$N(8) = 2, \qquad N(\theta + 1) = 3, \qquad N(\theta - 1) = 1 \tag{13}$$

entraînent que dans la décomposition du nombre 3 figure seulement un diviseur premier de degré 1, $\mathfrak{p}_3 = (\theta + 1)$; par suite $\mathfrak{p}_3^2 \nmid 3$, d'après le théorème 8 du § 5. De plus,

$$N(\theta + 2) = 2.17, \qquad N(\theta - 2) = -2.3.5. \tag{14}$$

La deuxième de ces égalités affirme que le nombre 5 admet un diviseur premier $\mathfrak{p}_5$ de degré 1; d'après la divisibilité de $\theta - 2 = \theta + 1 - 3$ par $\mathfrak{p}_3$, nous avons la décomposition $(\theta - 2) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$. Le nombre $\theta - 2$ satisfait à l'équation

$$(\theta - 2)^5 + 10(\theta - 2)^4 + 40(\theta - 2)^3 + 80(\theta - 2)^2 + 80(\theta - 2) + 30 = 0.$$

D'après l'exercice 9 du § 5, le nombre 5 admet alors la décomposition

$$5 = \mathfrak{p}_5^5.$$

Le résultat de l'exercice 15 montre aussi que 5 ne figure pas dans l'indice du nombre θ; cela signifie que l'anneau des nombres entiers du corps Q(0) coïncide avec l'ordre $\{1, \theta, \theta^2, \theta^3, \theta^4\}$.

La réunion des égalités (13) et (14) donne

$$N(\theta + 3) = 5.72, \qquad N(\theta - 3) = -241.$$

On ne peut pas en déduire directement la décomposition de 7 en facteurs premiers : le nombre $\theta + 3$ est divisible soit par le carré d'un diviseur premier de degré 1, soit par un diviseur premier de degré 2. Mais pour le nombre $\theta - 4 = (\theta + 3) - 7$, nous avons $N(\theta - 4) = -2.7.73$; par suite il existe un diviseur premier et un seul de degré 1, $\mathfrak{p}_7$, qui divise 7, $\mathfrak{p}_7^2 \nmid 7$.

Pour trouver les diviseurs premiers de degré 2 qui figurent dans 3 ou 7, considérons les normes des nombres $\theta^2 + \theta x + y$. Nous avons

$$N(\theta^2 + x\theta + y) = 2x^5 + y^5 - 10x^3y + 10xy^2 + 4. \qquad (15)$$

Donnant à x et y les valeurs 0, 1, -1, nous obtenons 9 nombres dont aucun n'est divisible par 9. Cela signifie qu'il n'y a aucun diviseur premier de degré 2 de 3. La formule (3) donne maintenant une seule possibilité pour la décomposition du nombre 3 :

$$3 = \mathfrak{p}_3\mathfrak{p}_3',$$

où $\mathfrak{p}_3'$ est un diviseur premier de degré 4. Si nous prenons pour x et y dans (15) les valeurs 0, ± 1, ± 2, ± 3, un seul des 49 nombres obtenus est divisible par 7^2 :

$$N(\theta^2 + 2\theta - 3) = 5.7^2.$$

Mais $\theta^2 + 2\theta - 3 = (\theta + 3)(\theta - 1)$ et nous obtenons ici le carré du diviseur $\mathfrak{p}_7$; nous pouvons donc écrire la décomposition suivante du nombre 7 :

$$7 = \mathfrak{p}_7\mathfrak{p}_7'$$

où $\mathfrak{p}_7'$ est un diviseur premier de degré 4.

Exemple 2. — Considérons le corps cubique Q(0), $\theta^3 - 9\theta - 6 = 0$. Puisque $D(1, \theta, \theta^2) = 3^5 . 2^3$, alors, d'après l'exercice 15, seul 2 peut figurer dans l'indice de θ (en fait, on peut montrer que l'ordre $\{ 1, \theta, \theta^2 \}$ est maximum, mais nous n'utiliserons pas ce fait). D'après l'exercice 9, § 5, le nombre 3 admet la décomposition

$$3 = \mathfrak{p}_3^3.$$

Des égalités

$$N(0) = 6, \qquad N(\theta + 1) = -4, \qquad N(\theta - 1) = 14 \tag{16}$$

résulte alors que dans le nombre 2 figurent au moins deux diviseurs premiers de degré 1 distincts, $\mathfrak{p}_2$ et $\mathfrak{p}_2'$:

$$(\theta) = \mathfrak{p}_2\mathfrak{p}_3, \qquad (\theta - 1) = \mathfrak{p}_2'\mathfrak{p}_7 \tag{17}$$

Mais, d'après l'égalité

$$(\theta - 1)^3 + 3(\theta - 1)^2 - 6(\theta - 1) - 14 = 0,$$

le nombre 2 est divisible par $\mathfrak{p}_2'^2$; par suite

$$2 = \mathfrak{p}_2\mathfrak{p}_2'^2, \qquad \theta + 1 = \mathfrak{p}_2'^2. \tag{18}$$

Les normes (16) et aussi

$$N(\theta + 2) = -4, \qquad N(\theta - 2) = 16 \tag{19}$$

ne sont pas toutes divisibles par 5. Cela signifie que dans 5 il n'y a pas de diviseurs premiers de degré 1. Dans le cas présent, cela entraîne que le diviseur principal 5 est premier. Pour trouver la décomposition du nombre 7, il faut, en même temps que (16) et (19), considérer aussi les normes

$$N(\theta + 3) = 6, \qquad N(\theta - 3) = 6.$$

Puisque parmi ces 7 valeurs il y en a seulement une qui est divisible par 7, alors 7 contient exactement un diviseur premier de degré 1. Remarquant que $\mathfrak{p}_7^2 \nmid 7$, on peut écrire la décomposition $7 = \mathfrak{p}_7\mathfrak{p}_7'$ où $\mathfrak{p}_7'$ est un diviseur premier de degré deux.

La méthode utilisée, qui repose sur l'examen des valeurs des normes de nombres entiers, donne une série d'équivalences entre diviseurs premiers. Ces équivalences permettent de diminuer le nombre de diviseurs considérés dans le système (11) d'où l'on peut extraire un sous-système maximal de diviseurs deux à deux non équivalents (pour le calcul du nombre h); parfois, on obtient ainsi ce sous-système maximal. Ainsi, dans l'exemple 2, en

liaison avec le résultat de l'exercice 9, le système (11) est formé des diviseurs entiers de normes $\leqslant \frac{3!}{3^2}\sqrt{3^5 2^3} < 10$, i. e. des diviseurs :

$$1,\ \mathfrak{p}_2,\ \mathfrak{p}_2',\ \mathfrak{p}_3,\mathfrak{p}_2^2,\ \mathfrak{p}_2'^2,\ \mathfrak{p}_2\mathfrak{p}_2',\ \mathfrak{p}_2\mathfrak{p}_3,\mathfrak{p}_2'\mathfrak{p}_3,\ \mathfrak{p}_7,\ \mathfrak{p}_2^3,\ \mathfrak{p}_2^2\mathfrak{p}_2',\ 2,\mathfrak{p}_2'^3,\ \mathfrak{p}_3^2. \qquad (20)$$

Mais il résulte de (18) que $\mathfrak{p}_2'^2 \sim 1$ et $\mathfrak{p}_2 \sim 1$ (1 est le diviseur unité). Par suite, d'après (17) et l'égalité $(\theta + 3) = \mathfrak{p}_2'\mathfrak{p}_3$, on a également $\mathfrak{p}_3 \sim 1$, $\mathfrak{p}_2 \sim 1$ et $\mathfrak{p}_7 \sim 1$. Ainsi, tous les diviseurs du système (20) sont principaux et par suite pour le corps Q(O), $\theta^3 - 9\theta - 6 = 0$, le nombre h est égal à 1.

Parfois (pour des discriminants petits), le système de diviseurs (11) se réduit à un seul diviseur. Dans ces cas, nous obtenons sans calcul $h = 1$. Ainsi, par exemple, pour le corps Q(O), $\theta^3 - \theta - 1 = 0$, le discriminant de la base 1, θ, θ^2 est égal à -23; par suite, d'après l'exercice 8, § 2, chapitre II, cette base est fondamentale et -23 est le discriminant du corps. D'après l'exercice 9, dans toute classe de diviseurs du corps $\mathbf{Q}(\theta)$, il existe un diviseur entier de norme

$$\leqslant \frac{4}{\pi}\frac{3!}{3^2}\sqrt{23} < 2,$$

et par suite tous les diviseurs du corps Q(0) sont principaux.

Dans le cas des corps quadratiques, le nombre des classes de diviseurs peut aussi être calculé en utilisant la méthode de réduction exposée dans les exercices 12 à 15 et 27 du § 7, chapitre II.

EXERCICES

1. Montrer que dans tout corps de nombres algébriques de degré n, le nombre $\psi(a)$ des diviseurs entiers de norme donnée a est inférieur ou égal au nombre $\tau_n(a)$ de solutions de l'équation $x_1x_2 \ldots x_n = a$ ($x_1, \ldots, x_n$ parcourent indépendamment l'un de l'autre les entiers naturels).

2. Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux diviseurs d'un corps de nombres algébriques (entiers ou fractionnaires) et $\bar{\mathfrak{a}}$ et $\bar{\mathfrak{b}}$ les idéaux qui leur correspondent. Démontrer que si a est divisible par $\mathfrak{b}$, alors

$$(\bar{\mathfrak{b}} : \bar{\mathfrak{a}}) = N(a\mathfrak{b}^{-1}).$$

3. Démontrer que deux classes de diviseurs distinctes contiennent respectivement des diviseurs premiers entre eux.

4. Pour tout diviseur entier a d'un corps de nombres algébriques, désignons par $\varphi(\mathfrak{a})$ le nombre de classes résiduelles modulo a constituées de nombres premiers avec a (généralisation de la fonction d'Euler). Démontrer que si deux diviseurs entiers a et $\mathfrak{b}$ sont premiers alors

$$\varphi(a\mathfrak{b}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b}).$$

5. Démontrer la formule

$$\varphi(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}) \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right),$$

dans laquelle $\mathfrak{p}$ parcourt tous les diviseurs premiers qui divisent le diviseur entier a.

6. Démontrer que pour tout nombre entier α premier avec un diviseur entier $\mathfrak{a}$ on a la congruence

$$\alpha^{\varphi(\mathfrak{a})} \equiv 1 \pmod{a}$$

(généralisation du théorème d'Euler). Démontrer que pour tout entier α et pour tout diviseur premier $\mathfrak{p}$ d'un corps de nombres algébriques, on a la congruence

$$\alpha^{\mathrm{N}(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}},$$

(généralisation du petit théorème de Fermat).

7. Démontrer la formule

$$\sum_{\mathfrak{c}} \varphi(\mathfrak{c}) = \mathrm{N}(\mathfrak{a}),$$

où c parcourt tous les diviseurs qui divisent le diviseur a (y compris e et a).

8. Soit $\xi_1, \ldots, \xi_s$ ($s = \mathrm{N}(\mathfrak{p}) - 1$) un système de résidus modulo $\mathfrak{p}$ premier non divisibles par $\mathfrak{p}$. Démontrer qu'alors

$$\xi_1 \ldots \xi_s \equiv -1 \pmod{\mathfrak{p}}$$

(analogue du théorème de Wilson).

9. Utilisant l'exercice 2 du chapitre II, § 6, démontrer que toute classe de diviseurs d'un corps K de nombres algébriques de degré $n = s + 2t$ et de discriminant D contient un diviseur entier a tel que

$$\mathrm{N}(\mathfrak{a}) \leqslant \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|D|}.$$

10. Montrer que pour les corps quadratiques de discriminants 5, 8, 12, 13, -3, -4, -7, -11 le nombre des classes de diviseurs est égal à 1.

11. Montrer que le nombre des classes de diviseurs du corps $\mathbf{Q}(\sqrt{-19})$ est égal à 1.

12. Montrer que dans le corps $\mathbf{Q}(\zeta)$, où ζ est une racine primitive d'ordre 5 de 1, la décomposition des nombres entiers en facteurs premiers est définie de manière unique.

13. Montrer que le nombre des classes de diviseurs du corps $\mathbf{Q}(\sqrt{-23})$ est égal à 3.

14. Soient K_1, K_2 et K_3 les corps cubiques étudiés dans l'exercice 21, chapitre II, § 2. Montrer que le nombre 5 est premier dans les corps K_1 et K_2 et se décompose dans le corps K_3 en un produit $5 = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ de trois diviseurs premiers distincts de degré 1. Montrer de plus que le nombre 11 se décompose en un produit $11 = \mathfrak{q}\mathfrak{q}'\mathfrak{q}''$ de trois diviseurs premiers distincts dans le corps K_1 et reste premier dans le corps K_2 (Il en résulte que K_1, K_2 et K_3 sont distincts).

15. Supposons qu'un nombre entier primitif $\theta \in K$ est racine d'un polynôme d'Eisenstein relatif au nombre premier p. Utilisant le résultat de l'exercice 9 du § 5, montrer que p ne figure pas dans l'indice du nombre θ.

16. Soit p un nombre premier inférieur au degré n d'un corps K de nombres algébriques. Démontrer que s'il existe dans K un nombre entier primitif dont l'indice n'est pas divisible par p, alors le nombre p ne peut pas être décomposé dans le corps K en un produit de n diviseurs premiers distincts de degré 1.

17. Utilisant les exercices 18 et 19 du § 5, démontrer qu'un nombre premier rationnel est ramifié dans un corps K de nombres algébriques (i. e. est divisible par le carré d'un diviseur premier) si et seulement s'il figure dans le discriminant du corps K.

18. Soit $\mathfrak{p}$ un diviseur premier ne divisant ni le nombre 2 ni le déterminant δ d'une forme quadratique $f(x_1, \ldots, x_n)$ à coefficients entiers d'un corps K de nombres algébriques. Pour tout entier $\alpha \in K$ non divisible par $\mathfrak{p}$, posons $\left(\frac{\alpha}{\mathfrak{p}}\right) = +1$ si la congruence $\xi^2 \equiv \alpha \pmod{\mathfrak{p}}$ est résoluble dans l'anneau des nombres entiers du corps K et $\left(\frac{\alpha}{\mathfrak{p}}\right) = -1$ dans le cas contraire. Démontrer que le nombre N de solutions de la congruence

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}}$$

est donné par les formules :

$$N = N(\mathfrak{p})^{n-1}, \quad \text{si } n \text{ est impair ;}$$

$$N = N(\mathfrak{p})^{n-1} + \left(\frac{(-1)^{\frac{n}{2}}\delta}{\mathfrak{p}}\right) N(\mathfrak{p})^{\frac{n-2}{2}} (N(\mathfrak{p}) - 1), \quad \text{si } n \text{ est pair.}$$

19. Soit $\mathfrak{a}$ un diviseur d'un corps K de nombres algébriques et supposons que $\mathfrak{a}^m = (a)$ est principal. Démontrer que dans le corps $K(\sqrt[m]{a})$ le diviseur $\mathfrak{a}$ devient principal.

20. Démontrer que tout corps K de nombres algébriques admet une extension finie $\bar{K}/K$ telle que tout diviseur $\mathfrak{a}$ du corps K soit un diviseur principal du corps $\bar{K}$.

21. Supposons que dans un corps cubique K un nombre premier p se décompose en un produit $p = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ de trois diviseurs premiers distincts et soit α un nombre entier de K. Démontrer que si $\mathrm{Tr}\,\alpha = 0$ et $\mathfrak{p}\mathfrak{p}' | \alpha$, alors $\mathfrak{p}'' | \alpha$ et par suite $p | \alpha$.

22. Démontrer que le nombre de classes de diviseurs du corps $Q(\theta)$, $\theta^3 = 6$, est égal à 1 (d'après l'exercice 24 du chapitre II, § 2, les nombres 1, θ, θ^2 forment une base fondamentale du corps $Q(\theta)$).

23. Démontrer que dans le corps cubique $K = Q(\theta)$, $\theta^3 = 6$, il n'existe pas de nombre $\alpha \neq 0$ de la forme $x + y\theta$ pour des entiers x et y entiers rationnels tels que $N(\alpha) = 10z^3$ (z est un entier rationnel). En déduire que l'équation

$$x^3 + 6y^3 = 10z^3$$

(et par suite également l'équation $3x^2 + 4y^3 + 5z^3 = 0$) n'a pas de solution non triviale dans les nombres entiers rationnels.

Indication. — Supposons qu'un tel nombre a existe, montrer qu'il est nécessairement de la forme $\alpha = \alpha_0 \xi^3$ où ξ est un nombre entier du corps K et α_0 un des six nombres suivants :

$$\lambda\mu; \quad \lambda\mu\varepsilon; \quad \lambda\mu\varepsilon^2; \quad \lambda\nu; \quad \lambda\nu\varepsilon; \quad \lambda\nu\varepsilon^2.$$

Ici $\lambda = 2 - \theta$ $(N(\lambda) = 2)$; $\mu = \theta - 1$ $(N(\mu) = 5)$; $\gamma(\theta^2 + \theta + 1)^2 = 13 + 8\theta + 3\theta^2$ $(N(\nu) = 5.53)$; $\varepsilon = 1 - 69 + 38$ est une unité fondamentale du corps K (exer-

cice 4 du chapitre II, § 5). Pour la démonstration, utiliser l'exercice 21 en l'appliquant au nombre $\alpha\theta$, les exercices 17 et 22 et utiliser aussi la décomposition des nombres 2, 3 et 5 en facteurs premiers dans le corps K. Posant alors $\xi = u + v\theta + w\theta^2$, écrire

$$\alpha = \alpha_0 \xi^3 = \Phi + \Psi\theta + \Omega\theta^2,$$

où Φ, Y et Ω sont des formes cubiques des variables u, v, w, à coefficients entiers. Montrer que pour chacune des six valeurs ci-dessus de α_0 l'équation $\Omega(u, v, w) = 0$ admet seulement la solution triviale dans les nombres rationnels (et 3-adiques).

24. Soient a et b des entiers naturels, sans carrés, premiers entre eux et supposons $d = ab^2 > 1$. Montrer que dans le corps $\mathbf{Q}(\sqrt[3]{d})$ la décomposition du nombre 3 comme produit de diviseurs premiers s'écrit

$$3 = \mathfrak{p}^3, \qquad \text{si} \qquad d \not\equiv \pm 1 \pmod 9;$$

$$3 = \mathfrak{p}^2\mathfrak{q} \ (\mathfrak{p} \neq \mathfrak{q}), \qquad \text{si} \qquad d \equiv \pm 1 \pmod 9.$$

Indication. — Dans le cas $d \equiv \pm 1 \pmod 9$, considérer les normes $N(\omega - 1)$, $N(\omega)$, $N(\omega + 1)$ pour

$$\omega = \frac{1}{3}(1 + \sigma\sqrt[3]{ab^2} + \tau\sqrt[3]{a^2b}),$$

$$\sigma = \pm 1, \qquad \tau = \pm 1, \qquad \sigma a \equiv \tau b \equiv 1 \pmod 3.$$

25. Soient θ un nombre entier primitif d'un corps K de nombres algébriques, $\varphi(t)$ son polynôme minimal et p un nombre premier rationnel ne figurant pas dans l'indice du nombre θ. Supposons que l'on ait, modulo p, la décomposition

$$\varphi(t) \equiv \varphi_1(t)^{e_1} \ldots \varphi_m(t)^{e_m} \pmod p$$

où $\varphi_1, \ldots, \varphi_m$ sont des polynômes à coefficients entiers modulo p, irréductibles et deux à deux distincts, de degrés $f_1, \ldots, f_m$ respectivement. Démontrer que la décomposition du nombre p en un produit de diviseurs premiers du corps K s'écrit

$$p = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_m^{e_m}$$

où les diviseurs premiers distincts $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sont de degrés respectifs $f_1, \ldots, f_m$ et $\varphi_i(\theta) \equiv 0 \pmod{\mathfrak{p}_i}$, $i = 1, \ldots, m$.

Indication. — Utiliser le fait que tout nombre entier de K est congru modulo $\mathfrak{p}_i$ à une combinaison linéaire à coefficients entiers des puissances θ^s $(s \geqslant 0)$.

26. Soit p un nombre premier rationnel ne figurant pas dans l'indice d'un nombre entier primitif θ d'un corps K. Démontrer que pour aucun entier rationnel x, le nombre $\theta + x$ n'est divisible dans le corps K par un diviseur premier figurant dans p avec un degré supérieur à 1.

27. Généralisant l'exercice précédent, démontrer (sous les mêmes hypothèses) que pour aucun système d'entiers rationnels $x_0, \ldots, x_{r-1}$ le nombre

$$\theta r + x_{r-1}\theta^{r-1} + \ldots + x_0$$

n'est divisible par un produit $\mathfrak{p}_1 \ldots \mathfrak{p}_s$ de diviseurs premiers distincts figurant danspavecdesdegrésf,, . . ., f_s tels que $f_1 + \ldots + f_s > r$.

§ 8. — CORPS QUADRATIQUES

Nous étudierons ici de manière plus détaillée la théorie des diviseurs pour un **corps** quadratique. Commençons par décrire les diviseurs premiers.

1) Diviseurs premiers

Puisque tout diviseur premier divise un nombre premier et un seul, alors, pour décrire tous les diviseurs premiers, il suffit quel que soit le corps de nombres algébriques, d'étudier comment un nombre premier rationnel p quelconque se décompose en produit de diviseurs premiers. D'après l'égalité (3) du § 7, dans le cas d'un corps quadratique (i. e. $n = 2$), les nombres m, f_i et e_i peuvent seulement prendre les valeurs suivantes :

1°	$m = 2,$	$f_1 = f_2 = 1,$	$e_1 = e_2 = 1;$
2°	$m = 1,$	$f = 2,$	$e = 1;$
3°	$m = 1,$	$f = 1,$	$e = 2.$

Par suite, nous obtenons dans un corps quadratique trois types de décompositions :

1°	$p = \mathfrak{p}\mathfrak{p}',$	$N(\mathfrak{p}) = N(\mathfrak{p}') = p,$	$\mathfrak{p} \neq \mathfrak{p}';$
2°	$p = \mathfrak{p}$	$N(\mathfrak{p}) = p^2;$	
3°	$p = \mathfrak{p}^2,$	$N(\mathfrak{p}) = p.$	

Le théorème 8, § 5 nous permet facilement de reconnaître le type de la décomposition d'un nombre p donné.

Dans le chapitre II, § 7-1), on a montré que tout corps quadratique est de la forme $Q(\sqrt{d})$, où d est un nombre entier rationnel sans carrés.

Considérons tout d'abord un nombre premier p impair. Si p ne divise pas d, alors il ne divise pas non plus le discriminant du polynôme $x^2 - d$ dont chaque racine engendre le corps. Par suite, d'après le théorème 8 du § 5, p admet une décomposition du 1er ou du 2e type suivant que le polynôme $x^2 - d$ est réductible modulo p ou pas. Cela dépend à son tour du fait que d est un résidu quadratique modulo p ou pas.

Si $p|d$, alors $d = pd_1$ où d_1 n'est pas divisible par p puisque d est sans carrés. L'égalité

$$pd_1 = (\sqrt{d})^2, \quad (d_1, p) = 1.$$

montre que tous les diviseurs premiers qui figurent dans p y figurent avec un degré pair; par suite, p admet une décomposition du 3e type. Ainsi.

pour p impair, nous aurons le 1er, 2e ou 3e type de décomposition respectivement dans les cas suivants

1° $\quad p \nmid d, \qquad \left(\frac{d}{p}\right) = 1 ;$

2° $\quad p \nmid d, \qquad \frac{d}{0p} = -1 ;$

3° $\quad p \mid d.$

Remarquons que, puisque le discriminant D du corps $\mathbf{Q}(\sqrt{d})$ est égal à d ou à $4d$ (théorème 1 du chapitre II, § 7), on peut, pour toutes ces conditions, remplacer d par D.

Il reste à considérer le cas $p = 2$. Supposons tout d'abord que $2 \nmid d$; d'après le théorème 1 du chapitre II, § 7, cela a lieu pour $D = d \equiv 1 \pmod 4$. Il est clair que $\mathbf{Q}(\sqrt{d}) = Q(w)$ où $\omega = \frac{-1+\sqrt{D}}{2}$. Le polynôme minimal de ω est le polynôme

$$x^2 + x + \frac{1 - D}{4}. \tag{1}$$

Puisque le discriminant de la base 1, ω est impair, on obtient, en appliquant le théorème 8 du § 5, que 2 admet une décomposition du premier ou deuxième type selon que le polynôme (1) est *réduit* modulo 2 ou pas. Il est évident que le polynôme $x^2 + x +$ a est réductible modulo 2 si et seulement si 2 divise a. Ainsi, si $2 \nmid D$, 2 admet la première ou la deuxième décomposition suivant que $D \equiv 1 \pmod 8$ ou $D \equiv 5 \pmod 8$.

Montrons maintenant que si $2|D$, alors, de même que pour $p \neq 2$, on a le troisième type de décomposition. En effet, si $2|d$ alors $d = 2d'$, $2 \nmid d'$, et de l'égalité

$$2d' = (\sqrt{d})^2, \qquad 2 \nmid d',$$

résulte, comme dans le cas impair, que 2 a une décomposition du troisième type. Si maintenant $2 \nmid d$, alors $d \equiv 3 \pmod 4$ (théorème 1 du chapitre II, § 7). Dans l'égalité

$$(1 + \sqrt{d})^2 = 2\alpha$$

le nombre entier $\alpha = \frac{1+d}{2} + \sqrt{d}$ est premier avec 2 puisque sa norme

$$N(\alpha) = \frac{(1+d)^2}{4} - d = \frac{(1-d)^2}{4}$$

n'est pas divisible par 2. Par suite 2 admet encore dans ce cas une décomposition du troisième type.

Formulons les résultats obtenus.

THÉORÈME 1. — *Dans un corps quadratique de discriminant* D, *un nombre premier p admet une décomposition du type*

$$p = \mathfrak{p}^2, \qquad N(\mathfrak{p}) = p,$$

si et seulement sip divise D.

Si p impair ne divise pas D, *alors*

$$p = \mathfrak{p}\mathfrak{p}', \ \mathfrak{p} \neq \mathfrak{p}', \quad N(\mathfrak{p}) = N(\mathfrak{p}') = p \quad si \quad \left(\frac{D}{p}\right) = 1 ;$$

$$p = \mathfrak{p}, \quad N(\mathfrak{p}) = p^2, \quad si \quad \left(\frac{D}{p}\right) = -1.$$

Si le nombre 2 ne divise pas D *(cela signifie* $D \equiv 1 \pmod 4$*), alors*

$$2 = \mathfrak{p}\mathfrak{p}', \ \mathfrak{p} \neq \mathfrak{p}', \quad N(\mathfrak{p}) = N(\mathfrak{p}') = 2 \ si \ D \equiv 1 \pmod 8;$$
$$2 = \mathfrak{p}, \quad N(\mathfrak{p}) = 4 \qquad \text{si} \quad D \equiv 5 \pmod 8.$$

2) Loi de décomposition

D'après le théorème 1, le type de décomposition d'un nombre premier impair est défini par le résidu de D (ou *d)* modulo *p* ou plus exactement par la valeur du symbole de Legendre $\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right)$. En liaison avec ce fait, cherchons s'il est possible de formuler le théorème 1 de telle sorte que le type de dtcomposition soit défini par le résidu de *p* modulo une constante (dépendant seulement du corps). Nous utiliserons la loi de réciprocité pour le symbole de Jacobi.

Le symbole de Jacobi $\left(\frac{c}{b}\right)$ est défini, comme on le sait, pour c impair et *b* impair positif premier avec c. La loi de réciprocité pour ce symbole affirme que

$$\left(\frac{c}{b}\right) = (-1)^{\frac{b-1}{2}\cdot\frac{c-1}{2}} \left(\frac{b}{|c|}\right)$$

(la démonstration, pour $c < 0$, se ramène au cas d'un numérateur positif).

Soit *p* un nombre impair premier quelconque. Si $d = D \equiv 1 \pmod 4$, alors

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{d-1}{2}} \left(\frac{p}{|d|}\right) = \left(\frac{p}{|D|}\right), \tag{2}$$

puisque $d - 1$ est pair. Si maintenant $d \equiv 3 \pmod 4$, alors

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{d-1}{2}} \left(\frac{1}{|d|}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{|d|}\right) \tag{3}$$

puisque $\frac{d-1}{2}$ est impair. Enfin, pour $d = 2d', 2 \nmid d'$, nous avons

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{d'}{p}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}\cdot\frac{d'-1}{2}} \left(\frac{p}{|d'|}\right). \quad (4)$$

La valeur du symbole de Jacobi $\left(\frac{p}{|d|}\right)$ ou $\left(\frac{p}{|d'|}\right)$ dépend du résidu de p modulo $|d|$ ou $|d'|$. Si $d \equiv 1 \pmod 4$, c'est-à-dire dans le cas où le discriminant D du corps $Q(\sqrt{d})$ est égal à d, alors $\left(\frac{D}{p}\right)$ dépend seulement du résidu de p modulo $|d| = |D|$. Si $d \equiv 3 \pmod 4$ et par suite $D = 4d$, alors $\left(\frac{D}{p}\right)$ dépend du résidu dep modulo $|d|$ mais aussi du nombre $(-1)^{\frac{p-1}{2}}$ i. e. du résidu de p modulo 4; ainsi, $\left(\frac{D}{p}\right)$ dépend finalement du résidu de p modulo $4|d| = D$. Enfin, si $d = 2d'$, $D = 4d = 8d'$, alors $\left(\frac{p}{|d'|}\right)$ dépend du résidu de p modulo $|d'|$ de $(-1)^{\frac{p-1}{2}}$ (i. e. du résidu de p modulo 4) et de $(-1)^{\frac{p^2-1}{8}}$ (i. e. du résidu de p modulo 8). Par suite, dans ce cas, $\left(\frac{D}{p}\right)$ dépend du résidu dep modulo $8|d'| = |D|$. Nous avons donc montré que, dans tous les cas, le type de décomposition d'un nombre premier impair p est défini par son résidu modulo $|D|$ puisque tous les nombres premiers qui ont le même résidu, i. e. qui appartiennent à une progression arithmétique du type $a + |D|x$, ont le même type de décomposition. Cela n'est pas évident ***a priori*** et est une importante loi de décomposition des nombres premiers dans un corps quadratique.

Pour formuler cette loi plus clairement, considérons, pour les nombres entiers x premiers avec le discriminant D, la fonction $\chi(x)$ définie par

$$\chi(x) = \begin{cases} \left(\frac{x}{|d|}\right) & \text{pour} \quad d \equiv 1 \pmod 4 \\ (-1)^{\frac{x-1}{2}}\left(\frac{x}{|d|}\right) & \text{pour} \quad d \equiv 3 \pmod 4 \\ (-1)^{\frac{x^2-1}{8} + \frac{x-1}{8}\cdot\frac{d'-1}{2}}\left(\frac{x}{|d'|}\right) & \text{pour} \quad d = 2d' \end{cases} \quad (5)$$

(dans le cas $d \equiv 2, 3 \pmod 4$, les expressions $(-1)^{\frac{x-1}{2}}$ et $(-1)^{\frac{x^2-1}{8}}$ ont un sens, puisque, d'après la parité du discriminant $D = 4d$, le nombre x est impair).

Dans le raisonnement ci-dessus qui montre que, pour p impair, la valeur $\frac{D}{0p}$ dépend seulement du résidu de p modulo $|D|$, nous n'avons nulle part utilisé le fait que p est premier. Nous obtenons donc que $\chi(x)$ dépend seulement du résidu de x modulo $|D|$. De plus, on vérifie facilement que si (x, D) = 1 et (x', D) = 1, alors $\chi(xx') = x(x)x(x')$. Tout cela montre que la fonction χ est un homomorphisme du groupe multiplicatif des classes résiduelles modulo $|D|$ des éléments premiers avec D dans le groupe d'ordre 2 formé des éléments + 1 et — 1. De telle fonctions définies sur les nombres premiers avec D et ne s'annulant pas sont appelées des caractères *(quadratiques)* .

DÉFINITION. *-Le caractère modulaire χ modulo $|D|$ dont les valeurs $\chi(x)$ pour x premier avec* **D** *sont définies par les égalités (5) s'appelle un caractère quadratique du corps* $\mathbf{Q}(\sqrt{d})$.

Revenant aux égalités (2), (3) et (4), nous voyons que p premier impair ne divisant pas D admet une décomposition du premier ou deuxième type selon que $\chi(p) = +1$ ou 1. Ce résultat est aussi vrai pour $p = 2$; en effet, si $2 \nmid D$, alors $D \equiv 1 \pmod 4$ et par suite $\chi(2) = \left(\frac{2}{|D|}\right)$ qui est égal à + 1 pour $D \equiv 1 \pmod 8$ et à — 1 pour $D \equiv 5 \pmod 8$.

THÉORÈME 2. — *En termes du caractère χ d'un corps quadratique* $\mathbf{Q}(\sqrt{d})$, *la décomposition d'un nombre premier p en produit de diviseurs premiers est définie par les conditions suivantes* :

$$\begin{aligned} p = \mathfrak{p}\mathfrak{p}', \quad & 4 \neq \mathfrak{p}', \quad N(p) = N(\mathfrak{p}') = p \quad && si\ \chi(p) = 1; \\ & p = \mathfrak{p} \quad && N(\mathfrak{p}) = p^2 \quad && si\ \chi(p) = -1; \\ & p = \mathfrak{p}^2, \quad && N(\mathfrak{p}) = p \quad && si\ \chi(p) = 0. \end{aligned}$$

Tous les nombres entiers rationnels sont donc divisés en trois groupes suivant la valeur prise par le caractère χ; chacun de ces groupes est une réunion de classes résiduelles modulo $|D|$.

Une telle loi de décomposition, où le type de la décomposition est défini seulement par le résidu du nombre premier modulo une constante, existe pour d'autres corps que les corps quadratiques, par exemple pour les corps cyclotomiques (cf. chap. V, § 2-2)). Pourtant, tous les corps de nombres algébriques ne possèdent pas une telle loi.

La connaissance des lois de décomposition dans les corps de nombres algébriques permet de résoudre de nombreux problèmes de théorie des nombres (cf. par exemple le chapitre V, § 2); il serait donc intéressant de savoir quels sont les corps qui admettent une loi de décomposition du type

ci-dessus. La réponse a cette question constitue la théorie du corps de classes; on montre que ces corps sont les extensions normales du corps des nombres rationnels dont le groupe de Galois est abélien. Tous les corps quadratiques ont pour groupe de Galois un groupe cyclique d'ordre 2. Un exemple très simple de corps non abélien est un corps cubique dont le discriminant n'est pas un carré parfait, par exemple le corps $\mathbf{Q}(\theta)$,

$$\theta^3 - \theta - 1 = 0.$$

Pour ce corps, il est impossible de trouver un nombre N tel que le type de décomposition d'un nombre premier p comme produit de diviseurs premiers dépende seulement du résidu de p modulo N.

La théorie du corps de classes résout d'ailleurs une question beaucoup plus générale que celle qui précède. Elle décrit la loi de décomposition des diviseurs premiers d'un corps quelconque k de nombres algébriques en facteurs dans une extension K/k si le groupe de Galois de cette décomposition est abélien (nous avons cité ci-dessus le cas où k = Q). Cette théorie admet de nombreuses applications en théorie des nombres. Ainsi, elle permet d'étendre les théorèmes démontrés au chapitre premier (relatifs aux formes quadratiques à coefficients rationnels) aux formes quadratiques à coefficients dans un corps quelconque k de nombres algébriques, d'interpréter de manière plus profonde la théorie des genres que nous avons étudiée au point 4), de démontrer le théorème d'existence de diviseurs premiers dans une classe donnée de diviseurs, etc... On pourra se référer aux livres suivants :

H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. *Juhresbericht d. Deutschen Mathematiker Vereinigung*. Teil 1 (Klassenkorpertheorie), 1926, 35, 1-55; Teil Ia (Beweise zu Teil 1), 1927, 36, 233-311; Teil II (Reziprozitatsgesetz), 1930, Erganzungsband 6, l-204.

C. Chevalley, Sur la théorie du corps de classes dans les corps finis et les corps locaux. *J. Fac. Sci. Imp. Univ. Tokyo, 1933,* 2, n° 9, 366-476.

E. Artin et J. Tate, Class field theory, Princeton, 1961.

On connaît très peu de résultats sur les lois de décomposition des nombres premiers dans les corps dont le groupe de Galois est non abélien.

3

3) Représentation des nombres par des formes quadratiques binaires

Dans le chapitre II, § 7-5), nous avons vu qu'il existe une correspondance biunivoque entre les classes de formes quadratiques binaires strictement équivalentes et les classes de modules semblables (au sens strict) d'un corps

quadratique (dans le cas $D < 0$, on considère seulement les formes définies positives). D'autre part, d'après le théorème 6 du § 6, les modules complets associés à l'ordre maximum (i. e. les idéaux du corps) correspondent biunivoquement aux diviseurs. On s'attend donc à des liens étroits entre la théorie des diviseurs d'un corps quadratique et la théorie des formes primitives dont le discriminant coïncide avec le discriminant du corps.

Il faut étendre aux diviseurs la correspondance entre les classes de formes et les classes de modules et changer la notion d'équivalence des diviseurs.

DÉFINITION. — *Deux diviseurs a et $\mathfrak{b}$ d'un corps quadratique $\mathbf{Q}(\sqrt{d})$ sont dits équivalents au sens strict s'il existe un nombre $a \neq 0$ dans le corps $Q(\sqrt{d})$ tel que $N(a) > 0$ et* $a = b(a)$.

Puisque pour les corps quadratiques imaginaires, la norme de tout élément non nul est positive, alors, dans ce cas, l'équivalence des diviseurs au sens strict coïncide avec la notion habituelle d'équivalence (définition, § 7-2)). Les mêmes raisonnements que pour les modules (cf. chap. II, § 7-5)) montrent que, dans un corps réel $\mathbf{Q}(\sqrt{d})$, la nouvelle notion d'équivalence des diviseurs coïncide avec l'ancienne si et seulement si la norme d'une unité fondamentale ε du corps $Q(\sqrt{d})$ est égale à -1. Si maintenant $N(E) = +1$, alors toute classe de diviseurs pour l'équivalence ordinaire se décompose exactement en deux classes de diviseurs équivalents au sens strict. Alors le nombre $\bar{h}$ de classes de diviseurs au sens strict est fini et lié au nombre h de classes de diviseurs (au sens usuel) par la relation :

$$\bar{h} = h \quad \text{pour} \quad d < 0 ;$$
$$\bar{h} = h \quad \text{pour} \quad d > 0, \qquad N(E) = +1 ;$$
$$\bar{h} = 2h \quad \text{pour} \quad d > 0, \qquad N(E) = -1.$$

Le théorème 4 du chapitre II, § 7, appliqué aux modules associés à l'ordre maximum du corps $\mathbf{Q}(\sqrt{d})$ de discriminant D peut être reformulé de la manière suivante : les classes de diviseurs (au sens strict) d'un corps quadratique $\mathbf{Q}(\sqrt{d})$ sont en correspondance biunivoque avec les classes de formes quadratiques binaires primitives de discriminant D strictement équivalentes (définies positives pour $D < 0$).

Essayons d'appliquer les résultats des points 1) et 2) à la représentation des nombres par des formes binaires.

D'après le théorème 6 du chapitre II, § 7, le nombre entier naturel a est représentable par une certaine forme de discriminant D si et seulement s'il existe dans le corps $\mathbf{Q}(\sqrt{d})$ un diviseur entier de norme a (nous savons que la norme d'un diviseur est égale à la norme du module correspondant). Mais les normes de tous les diviseurs entiers sont caractérisées par le théo-

rème 2. En effet, la norme N(p) d'un diviseur premier $\mathfrak{p}$ est égale au nombre p si $\chi(p) = 0$ ou $x(p) = 1$ et au carré du nombre premier p si $x(p) = -1$. Par suite, le nombre a est la norme $N(\mathfrak{a})$ d'un diviseur entier $a = \prod_p p^{\alpha(p)}$ du corps $\mathbf{Q}(\sqrt{d})$ si et seulement si tous les nombres premiers p tels que $x(p) = -1$ figurent dans a avec des exposants pairs.

Nous pouvons donner d'autres formes de cette condition en utilisant le symbole de Hilbert que nous avons défini au chapitre premier, § 6-3). Calculons $\left(\frac{a, D}{p}\right)$ pour tous les nombres premiers p qui ne divisent pas D. Soit $a = p^k b$ où b n'est pas divisible par p; d'après les propriétés du symbole de Hilbert, nous avons

$$\left(\frac{a, D}{p}\right) = \left(\frac{b, D}{p}\right)\left(\frac{D}{p}\right)^k = \left(\frac{D}{p}\right)^k = \chi(p)^k \qquad \text{pour } p \neq 2,\ p \nmid D;$$

$$\left(\frac{a, D}{2}\right) = (-1)^{\frac{b-1}{2}\cdot\frac{D-1}{2} + k\frac{D^2-1}{8}} = (-1)^{k\frac{D^2-1}{8}} = \chi(2)^k \quad \text{pour } p = 2,\ 2 \nmid D$$

(dans le cas $p = 2, 2 \nmid D$, le calcul résulte de la congruence $D \equiv 1 \pmod 4$). Les formules obtenues démontrent la deuxième partie du théorème suivant.

THÉORÈME *3.* — ***Pour qu'un nombre naturel a soit représentable par au moins une forme binaire de discriminant*** D, ***il faut et il suffit qu'il ne contienne pas de nombres premiers p, tels que*** $x(p) = -1$, ***avec un exposant impair. Pour cela, il faut et il suffit que***

$$\left(\frac{a, D}{p}\right) = +1 \qquad \textit{pour tout } p \nmid D.$$

Puisque les nombres entiers a et ab^2 sont simultanément représentables ou pas par les formes de discriminant D, nous pouvons nous limiter à l'étude des nombres a sans carré.

Si $p \neq 2$, $p \nmid D$ et $p \nmid a$, alors, comme nous le savons, $\left(\frac{a, D}{p}\right) = +1$; par suite le théorème 3 impose seulement un nombre fini de conditions au nombre a, portant sur les résidus des diviseurs premiers du nombre a (sans carré) modulo $|D|$.

On peut obtenir facilement le théorème 3 à partir du théorème 7 du chapitre II, § 7. La démonstration donnée, qui repose sur le théorème 2, met en évidence le lien qui existe entre la représentation des nombres par des formes de discriminant D et la décomposition en facteurs dans le corps quadratique correspondant.

Ce résultat ne nous satisfait cependant pas entièrement. En effet, nous

aurions aimé avoir un critère de représentabilité du nombre a par les formes d'une classe donnée de formes strictement équivalentes, alors que le théorème 3 donne une condition de représentabilité de a par une forme d'une classe beaucoup plus vaste. Posons donc le problème suivant : est-il possible de diviser les classes de formes en ensembles disjoints de telle sorte que, pour tout a, toutes les formes qui représentent ce nombre a (s'il en existe) appartiennent à un des ensembles ci-dessus ? Une telle répartition des classes de formes a été trouvée par Gauss; ce problème est lié à l'étude de l'équivalence rationnelle des formes quadratiques.

DÉFINITION. — ***On dit que deux formes quadratiques binaires primitives de discriminant*** D ***appartiennent au même genre si elles sont rationnellement équivalentes.***

Puisque des formes équivalentes sur $\mathbf{Z}$ le sont aussi rationnellement, toutes les formes d'une même classe appartiennent au même genre. Ainsi, tout genre est une réunion de classes de formes; il en résulte en particulier que le nombre des genres de formes (de discriminant D donné) est fini.

Dans le chapitre premier, § 7-5), on a introduit, pour toute forme binaire rationnelle non singulière, des invariants $e_p(f)$ (p nombre premier ou le symbole ∞). Dans le cas considéré ici des formes primitives f de discriminant D, leur déterminant est égal à $-\frac{D}{4}$ et par suite

$$e_p(f) = \left(\frac{a, D}{p}\right),$$

où $a \neq 0$ est un nombre quelconque représentable rationnellement par la forme f.

Soit G un genre de formes. Puisque toutes les formes de G ont les mêmes invariants, nous pouvons poser

$$e_p(G) = e_p(f),$$

où f est une forme quelconque du genre G.

Soit a un nombre $\neq 0$ représentable par la forme f. D'après le deuxième argument du théorème 3, nous aurons $e_p(f) = \left(\frac{a, D}{p}\right) = 1$ pour tout p premier ne figurant pas dans D. De plus, $e_p(f) = 1$ puisque dans le cas $D < 0$ nous considérons seulement des formes définies positives. Par suite, pour tout genre G de formes de discriminant D, nous avons

$$e_p(G) = 1 \quad \text{pour} \quad p \nmid D \quad \text{et} \quad p = \infty. \tag{6}$$

Tout genre G est donc défini de manière unique par les invariants $e_p(G)$ où p parcourt tous les diviseurs premiers du discriminant D.

La condition de représentabilité des nombres par les formes d'un genre fixé G peut s'énoncer ainsi :

THÉORÈME *4.* — ***Pour qu'un nombre entier positif a soit représentable dans Z par une forme d'un genre G, il faut et il suffit que l'on ait pour tout p l'égalité***

$$\left(\frac{a, D}{p}\right) = e_p(G)$$

DÉMONSTRATION. — La nécessité de la condition est évidente. Si pour un certain a nous avons $\left(\frac{a, D}{p}\right) = e_p(G)$ pour tout p, alors, d'après (6), $\left(\frac{a, D}{p}\right) = 1$ pour tout $p \nmid D$. Mais alors, dans ce cas, d'après le théorème 3, le nombre a est représenté par une certaine forme f de discriminant D et puisque

$$e_p(f) = \left(\frac{a, D}{p}\right) = e_p(G),$$

f appartient au genre G. Le théorème 4 est démontré.

L'intérêt du théorème 4 est qu'il caractérise la représentabilité du nombre a par une certaine forme d'un genre G au moyen du résidu du nombre a modulo $|D|$ (à condition que a soit représentable par au moins une forme de discriminant D, i. e. à condition que $\left(\frac{a, D}{p}\right) = 1$ pour tout $p \nmid D$).

En effet, toutes les valeurs $\left(\frac{a, D}{P}\right)$, pour p divisant D, dépendent seulement du résidu de a modulo $|D|$. Dans le cas où la décomposition des formes en genres coïncide avec la décomposition en classes (i. e. lorsque tout genre est formé d'une seule classe) le théorème 4 donne la solution « idéale » du problème de la représentation des nombres par les formes binaires.

Dans le cas général, on ne peut pas améliorer le résultat. Cela signifie : considérons un ensemble de classes de formes de discriminant D (d'un ordre maximum) qui ne soit pas une réunion de genres; il n'existe pas de nombre m tel que la représentabilité d'un nombre par au moins une forme de notre ensemble dépende seulement du résidu de ce nombre modulo m. En particulier, si un genre contient plus d'une classe, on ne peut pas caractériser les nombres représentables par une classe en termes de leurs résidus modulo un certain nombre. La démonstration de ces résultats est une conséquence de la théorie du corps de classes en utilisant le fait suivant (en se limitant à des nombres premiers) : on peut interpréter la représentabilité d'un nombre premier par les formes d'un certain ensemble de classes en termes du type de décomposition de ce nombre premier dans un certain corps L. Ce corps L aura un groupe de Galois abélien sur le corps des nombres rationnels quand l'ensemble des classes de formes considéré

est une réunion de genres (cf. H. Hasse, Zur Geschlechtertheorie in quadratischen Zahlkorpern. *J. Math. Soc. Japan,* 1951, 3, n° 1, 45-51).

Recherchons maintenant le nombre de genres. Soient $p_1, \ldots, p_t$ tous les diviseurs premiers, deux à deux distincts, du discriminant D. D'après (6), tout genre G est défini par la donnée des invariants $e_i = e_{,}(G)$. Ces invariants ne sont pas quelconques puisque si f est une forme de G et $a \neq 0$ un nombre représentable par f, nous avons (formule (17), chap. Ier, § 7)

$$e_1 \ldots e_t = \prod_p e_p(G) = \prod_p \left(\frac{a, D}{p}\right) = 1$$

(dans les produits, p parcourt tous les nombres premiers et le symbole ∞). Montrons que la relation ainsi obtenue

$$e_1 \ldots e_t = 1 \tag{7}$$

pour des nombres $e_i = \pm 1$ est non seulement nécessaire mais aussi suffisante pour que ces nombres soient les invariants d'un certain genre G.

Désignons par k_i l'exposant avec lequel p_i figure dans D ($k_i = 1$ pour $p_i \neq 2$ et égal à 2 ou 3 pour $p_i = 2$). Pour tout $i = 1, \ldots, t$, soit a_i un entier non divisible par p_i et tel que $\left(\frac{a_i, D}{p_i}\right) = e_i$ et soit a un entier défini par les congruences

$$a \equiv a, \pmod{p_i^{k_i}} \qquad (1 \leqslant i \leqslant t).$$

Pour tout a satisfaisant à ces congruences, nous avons (d'après les propriétés du symbole de Hilbert)

$$\left(\frac{a, D}{p_i}\right) = \left(\frac{a_i, D}{p_i}\right) = e_i.$$

*Il faut montrer qu'on peut trouver a satisfaisant à la condition supplémentaire $\left(\frac{a., D}{p}\right) = 1$ pour tout $p \nmid D$. Nous utiliserons le théorème de Dirichlet sur les nombres premiers dans une progression arithmétique (cf. chap. V, § 3). Puisque toutes les valeurs possibles de a sont premières avec D et constituent une classe résiduelle modulo $D = \Pi p_i^{k_i}$, alors, d'après le théorème de Dirichlet, il existe parmi celles-ci un nombre premier impair q. Nous aurons

$$\left(\frac{q, D}{p}\right) = \left(\frac{a, D}{p_i}\right) = e \ ;$$

$$\left(\frac{q, D}{p}\right) = 1 \quad \text{pour} \quad p \nmid D, \quad p \neq 2 \quad \text{et} \quad p \neq q \ ;$$

$$\left(\frac{q, D}{2}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{D-1}{2}} = 1 \quad \text{pour} \quad 2 \nmid D.$$

La relation $\prod_p \left(\frac{q, D}{p}\right) = 1$ nous donne alors $e_1 \ldots e_t \left(\frac{q, D}{q}\right) = 1$; par suite, d'après (7), $\left(\frac{q, D}{q}\right) = 1$.

Ainsi, il existe un entier naturel a (et même premier) tel que

$$\left(\frac{a, D}{p_i}\right) = e_i \ (1 \leqslant i \leqslant t) \text{ et } \left(\frac{a, D}{p}\right) = 1 \quad \text{pour} \quad p \nmid D.$$

D'après le théorème 3, a est représenté par une certaine forme f de discriminant D; si on désigne par G le genre qui contient cette forme, alors

$$e_{p_i}(G) = \left(\frac{a, D}{p_i}\right) = e_i \quad (1 \leqslant i \leqslant t).$$

Ceci démontre l'existence d'un genre admettant des invariants donnés à l'avance (qui satisfont à la relation (7)). Puisque le nombre de tous les systèmes possibles de valeurs $e_i = \pm 1$ satisfaisant à la condition (7) est égal à 2^{t-1}, il existe 2^{t-1} genres de formes de discriminant D. Formulons le résultat obtenu.

THÉORÈME 5. — ***Soient*** $p_1, \ldots, p_t$ ***tous les diviseurs premiers*** (deux à deux distincts) ***du discriminant*** D ***du corps quadratique*** $\mathbf{Q}(\sqrt{d})$. ***Pour tout système de valeurs*** $e_i = \pm 1$ $(1 \leqslant i \leqslant t)$ ***satisfaisant à la condition*** $e_1 \ldots e_t = 1$, ***il existe un genre G de formes de discriminant*** D ***tel que*** $e_{p_i}(G) = e_i$. ***Le nombre de tous les genres de formes de discriminant*** D ***est égal à*** 2^{t-1}.

Remarque 1. — La théorie des genres étudiée ici pour les formes dont le discriminant est égal au discriminant D de l'ordre maximum d'un corps quadratique peut aussi être faite pour les formes de discriminant $D f^2$.

Remarque 2. — Si tout genre de formes de discriminant $D f^2 < 0$ est formé seulement d'une classe, alors on peut calculer simplement le nombre de représentations des nombres entiers premiers avec f par une forme donnée de discriminant $D f^2$ (cf. exercice 18). La table des valeurs des discriminants $D f^2 < 0$ dont les genres sont constitués chacun d'une seule classe est donnée à la fin du livre. On ne sait pas actuellement si cette table épuise toutes les valeurs des discriminants négatifs pour lesquels chaque genre de formes est composé d'une seule classe; on a seulement démontré qu'il n'existe qu'un nombre fini de tels discriminants. Pour $D f^2$ pair, les nombres $-\frac{Df}{4}$ ont été déterminés par Euler et sont appelés ***nombres « convenables » d'Euler***; ils ont été utilisés par lui pour trouver de grands nombres premiers, grâce à la propriété suivante : si le produit ab de deux nombres naturels a et b premiers entre eux est égal à l'un de ces nombres et si la forme $ax^2 + by^2$ représente le nombre q d'une seule manière (pour x et y

premiers entre eux), alors ce nombre q est premier (cf. exercice 19). Par exemple, la différence $3\,049 - 120\,y^2$ est un carré seulement pour y = 5; cela signifie que le nombre 3 049 est représenté de manière unique par la forme $x^2 + 120\,y^2$:

$$3\,049 = 7^2 + 120.\ 5^2$$

et par suite est premier. Par cette méthode, Euler a pu établir que de nombreux nombres étaient premiers.

4) Genres de diviseurs

Les résultats obtenus au point 3) sur les genres de formes donnent des indications sur la structure du groupe des classes (au sens strict) de diviseurs d'un corps quadratique. Définissons pour cela les genres de diviseurs.

D'après le théorème 6 du § 6, à tout diviseur a (entier ou fractionnaire) correspond biunivoquement l'idéal $\bar{a}$ des nombres du corps qui sont divisibles par a. Dans le cas d'un corps quadratique, à toute base $\{\alpha, \beta\}$ du module $\bar{a}$ satisfaisant à la condition (10), chapitre II, § 7, correspond une forme primitive

$$f(x, y) = \frac{N(\alpha x + \beta y)}{N(a)} \tag{8}$$

Par passage à une autre base du module $\bar{a}$ (avec la même condition (10) du chapitre II, § 7), la forme f est remplacée par une forme strictement équivalente. L'égalité (8) associe donc au diviseur a une classe de formes strictement équivalentes. Cette application établit une correspondance biunivoque entre les classes de diviseurs (au sens strict) et les classes de formes de discriminant D strictement équivalentes.

DÉFINITION. — ***Deux diviseurs d'un corps quadratique appartiennent au même genre si les classes de formes correspondantes appartiennent au même genre de formes*** (i. e. sont rationnellement équivalentes).

Puisque à des diviseurs équivalents au sens strict correspond la même classe de formes, chaque genre de diviseurs est une réunion de plusieurs classes de diviseurs (au sens strict).

Nous désignerons encore par la lettre G le genre de diviseurs qui correspond au genre de formes G. Les invariants $e_p(G)$ désigneront les invariants analogues du genre de formes correspondant; nous avons les formules

$$e_p(G) = \left(\frac{N(a), D}{p}\right), \tag{9}$$

où a est un diviseur quelconque du genre G. En effet, d'après la définition des invariants, $e_p(G) = \left(\frac{a, D}{p}\right)$ où a est un nombre rationnel $\neq 0$ représentable par la forme $f(x, y)$ du type (8) correspondant au diviseur a. Mais la forme $N(ax + \beta y)$ représente tous les carrés des nombres rationnels, en particulier $N(a)^2$. Par suite, $f(x, y)$ représente N(a) et cela démontre la formule (9).

Le genre de diviseurs G_0 dont tous les invariants sont égaux à 1 est appelé le genre principal. Tous les diviseurs a du genre principal sont caractérisés par les conditions $\left(\frac{N(a), D}{p}\right) = 1$ pour tout p. Il en résulte que le genre principal est un groupe pour la multiplication des diviseurs; c'est un sous-groupe du groupe de tous les diviseurs. Il est clair qu'un genre quelconque G est une classe résiduelle aG_0 selon le sous-groupe G_0 (a est un diviseur quelconque du genre G). Mais l'ensemble de toutes les classes résiduelles selon le sous-groupe G_0 est le groupe quotient du groupe de tous les diviseurs par le sous-groupe G_0. L'ensemble de tous les genres est donc muni d'une structure de groupe ; on l'appelle le groupe des genres. D'après le théorème 5, l'ordre du groupe des genres est égal à 2^{t-1}, où t est le nombre de diviseurs premiers distincts du diviseur D.

Donnons une caractérisation directe des genres de diviseurs (ne faisant pas appel aux formes correspondantes).

THÉORÈME *6.* — ***Deux diviseurs*** a ***et*** a, ***d'un corps quadratique appartiennent au même genre si et seulement s'il existe un nombre y du corps, de norme*** > 0, ***tel que***

$$N(a_1) = N(a)N(\gamma).$$

DÉMONSTRATION. — Choisissons dans les idéaux $\bar{a}$ et $\bar{a}_1$ des bases $\{a, \beta\}$ et $\{a_1, \beta_1\}$ satisfaisant à la condition 10 du chapitre II, § 7. Aux diviseurs a et a_1 correspondent les formes

$$f(x, y) = \frac{N(\alpha x + \beta y)}{N(a)}, \qquad f_1(x, y) = \frac{N(\alpha_1 x + \beta_1 y)}{N(a_1)}.$$

D'après le théorème 11 du § 1 de l'appendice, les formes f et f_1 sont rationnellement équivalentes si et seulement s'il existe au moins un nombre rationnel $\neq 0$ représentable simultanément par ces formes, i. e. lorsque

$$\frac{N(\xi)}{N(a)} = \frac{N(\xi_1)}{N(a_1)} \qquad (\xi, \xi_1 \neq 0).$$

Le théorème en résulte.

Pour les diviseurs du genre principal, nous avons l'importante caractérisation suivante.

THÉORÈME 7. — ***Un diviseur a appartient au genre principal si et seulement s'il est équivalent au sens strict au carré d'un diviseur.***

DÉMONSTRATION. — Soit a un diviseur appartenant au genre principal. Puisque le diviseur unité appartient au genre principal, alors, d'après le théorème 6, il existe un nombre y tel que N(a) = N(y). Remplaçant a par le diviseur équivalent $\mathfrak{a}(\gamma^{-1})$, nous pouvons supposer que N(a) = 1. Décomposons le diviseur a en un produit de diviseurs premiers; nous séparerons les diviseurs premiers $\mathfrak{p}_i$ pour lesquels il existe un autre diviseur premier $\mathfrak{p}'_i$ de même norme (décomposition du 1er type, en utilisant la terminologie du point 1)) des diviseurs restants $\mathfrak{q}_j$:

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i} \mathfrak{p}'^{b_i} \prod_j \mathfrak{q}_j^{c_j}.$$

Puisque $N(\mathfrak{p}_i) = N(\mathfrak{p}'_i) = p_i$ et $N(\mathfrak{q}_j) = q_j^{r_j}$ (où $r_j = 1$ ou 2), la condition N(a) = 1 nous donne

$$\prod_i p_i^{a_i+b_i} \prod_j q_j^{r_j c_j} = 1.$$

Les nombres premiers p_i et q_j sont distincts deux à deux et par suite $b_i = -a_i$ et $c_j = 0$, ce qui signifie :

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i} \mathfrak{p}'^{-a_i}_i.$$

Mais $\mathfrak{p}_i \mathfrak{p}'_i = p_i$ et par suite $\mathfrak{p}_i'^{-1} \sim \mathfrak{p}_i$; il en résulte que

$$\mathfrak{a} \sim \left(\prod_i \mathfrak{p}_i^{a_i} \right)^2$$

(le signe $\sim$ désigne l'équivalence des diviseurs au sens strict).

Inversement, si $\mathfrak{a} \sim \mathfrak{b}^2$, i. e. $\mathfrak{a} = \mathfrak{b}^2(\alpha)$, N(a) > 0, alors N(a) = N(P) où $\beta = N(\mathfrak{b})\alpha$, i. e., d'après le théorème 6, a appartient au genre principal.

Le théorème 7 est démontré.

Considérons maintenant le groupe $\mathfrak{C}$ des classes de diviseurs au sens strict. Si à toute classe $C \in \mathfrak{C}$ nous faisons correspondre le genre G qui contient cette classe, nous avons défini un homomorphisme du groupe des classes $\mathfrak{C}$ sur le groupe des genres. Son noyau est l'ensemble des classes qui sont contenues dans le genre principal G_0. D'après le théorème 7, la classe C' est contenue dans le genre principal si et seulement si c'est le carré d'une certaine classe de $\mathfrak{C}$. Ainsi le noyau de l'homomorphisme du groupe $\mathfrak{C}$ sur le

groupe des genres est le sous-groupe $\mathfrak{C}^2$ formé des carrés C^2 des classes $C \in \mathfrak{C}$. Appliquant le théorème des noyaux (de la théorie des groupes) et rappelant que le groupe des genres est d'ordre 2^{t-1}, nous obtenons le résultat suivant :

THÉORÈME *8. -Le groupe quotient $\mathfrak{C}/\mathfrak{C}^2$ du groupe $\mathfrak{C}$ des classes de diviseurs au sens strict par le sous-groupe des carrés est d'ordre 2^{t-1}, où t est le nombre de diviseurs premiers distincts du discriminant* D *du corps quadratique.*

Le théorème 8 donne d'intéressantes informations sur la structure du groupe $\mathfrak{C}$. D'après le théorème 1 du § 5 de l'appendice, le groupe $\mathfrak{C}$ est décomposable en un produit direct de sous-groupes cycliques. Du théorème 8 résulte alors facilement que parmi ces sous-groupes, $t - 1$ d'entre eux sont d'ordre pair. Nous obtenons en particulier le résultat suivant :

COROLLAIRE. *-Le nombre des classes de diviseurs* (au sens strict) *est impair si et seulement si son discriminant contient seulement un nombre premier.*

De tels corps sont $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{p})$ avec p premier de la forme $4n + 1$ et $\mathbf{Q}(\sqrt{-q})$ avec q premier de la forme $4n + 3$.

Les faits ci-dessus font partie du très petit nombre de résultats connus sur la structure du groupe des diviseurs.

EXERCICES

1. Démontrer que le caractère χ d'un corps quadratique de discriminant D s'exprime, en termes de symbole de Hilbert, par la formule

$$\chi(a) = \prod_{p \mid D} \left(\frac{a, D}{p}\right), \qquad (a, D) = 1.$$

2. Démontrer que pour tout entier y et un corps quadratique, premier avec le discriminant D, la congruence

$$x^2 \equiv N(y) \pmod{|D|}$$

est toujours résoluble.

3. Les classes modulo $|D|$ des nombres congrus aux normes des nombres entiers d'un corps quadratique qui sont premiers avec le discriminant D forment un sous-groupe H du groupe G des classes modulo $|D|$ des nombres premiers avec $|D|$. Démontrer que l'indice (G : H) est égal à $2t$ en désignant par t le nombre de diviseurs premiers distincts du discriminant D.

4. Soit H* le groupe des classes résiduelles modulo $|D|$ des nombres congrus aux normes des diviseurs entiers d'un corps quadratique qui sont premiers avec D. Démontrer que (G : H*) = 2.

5. Démontrer que pour tout nombre y de norme positive d'un corps quadratique de discriminant D on a, pour tout p,

$$\left(\frac{N(\gamma), D}{p}\right) = 1.$$

6. Démontrer que des idéaux entiers a et $\mathfrak{b}$ premiers avec D appartiennent à un même genre si et seulement s'il existe un entier y tel que

$$N(\mathfrak{a}) = N(\gamma)N(\mathfrak{b}) \pmod{|D|}.$$

7. Montrer que dans un corps quadratique réel dont le discriminant contient seulement un nombre premier, la norme d'une unité fondamentale est égale a- 1.

8. Démontrer que tout automorphisme différent de l'identité $\sigma : \alpha \to \alpha^\sigma$ d'un corps quadratique $\mathbf{Q}(\sqrt{d})$ définit de manière unique un automorphisme σ. $\mathfrak{a} \to \mathfrak{a}^\sigma$ du groupe des diviseurs tel que $(\alpha^\sigma) = (\alpha)^\sigma$ pour tout $\alpha \neq 0$. Expliquer comment opère l'automorphisme a sur les diviseurs premiers.

9. L'automorphisme σ du groupe des diviseurs défini dans l'exercice 8, induit de manière naturelle un automorphisme a : $C \to C^\sigma$ du groupe $\mathfrak{C}$ des classes de diviseurs (au sens strict). Si a $\in$ C, alors C^σ est la classe qui contient $\mathfrak{a}^\sigma$. Une classe C est dite invariante si $C^\sigma = C$. Démontrer qu'une classe C est invariante si et seulement si C^2 est une classe principale.

10. Démontrer que le sous-groupe du groupe $\mathfrak{C}$ des classes de diviseurs (au sens strict) formé des classes invariantes est d'ordre 2^{t+1} (t est le nombre de diviseurs premiers distincts du discriminant).

11. Démontrer que si, dans un corps quadratique, $N(\beta) = 1$, alors il existe α tel que

$$N(\alpha) > 0, \qquad \beta = \pm \frac{\alpha^\sigma}{\alpha}$$

12. Montrer que dans toute classe invariante C, il existe un diviseur a tel que $\mathfrak{a}^\sigma = \mathfrak{a}$.

13. Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ tous les diviseurs premiers deux à deux distincts qui divisent le discriminant D. Montrer que dans toute classe invariante C, il existe exactement deux représentants du type

$$\mathfrak{p}_{i_1} \ldots \mathfrak{p}_{i_k}, \quad 1 \leqslant i_1 < \ldots < i_k \leqslant t \ (k = 0, 1, \ldots, t)$$

14. Le sous-groupe des classes invariantes contenues dans un genre principal se décompose trivialement comme produit direct de groupes cycliques d'ordre 2. Démontrer que le nombre de ces facteurs cycliques est égal au nombre d'invariants du groupe des classes de $\mathfrak{C}$ (au sens strict) qui sont divisibles par 4 (pour la définition des invariants d'un groupe abélien fini, cf. appendice § 5-l)).

15. Démontrer que le nombre de diviseurs positifs r du discriminant D qui sont sans carré et qui satisfont à la condition

$$\left(\frac{r, D}{p}\right) = 1 \qquad \text{pour tout } p,$$

est de la forme 2". Montrer de plus que le nombre des invariants du groupe des classes de $\mathfrak{C}$ qui sont divisibles par 4 est égal à $u - 1$.

16. Soit m un entier naturel premier avec l'indice f d'un ordre $\mathfrak{D}_f$ contenu dans l'ordre maximum d'un corps quadratique $\mathbf{Q}(\sqrt{d})$. Démontrer que le nombre de modules de $\mathbf{Q}(\sqrt{d})$ d'anneau de stabilisateurs $\mathfrak{D}_f$ qui sont contenus dans $\mathfrak{D}_f$ et de norme m est égal au nombre de diviseurs entiers de norme m du corps $\mathbf{Q}(\sqrt{d})$.

17. Démontrer que le nombre de diviseurs entiers du corps quadratique $\mathbf{Q}(\sqrt{d})$ de norme m est égal à

$$\sum_{r \mid m} \chi(r),$$

où χ est le caractère du corps $\mathbf{Q}(\sqrt{d})$; r parcourt tous les diviseurs du nombre m.

18. Soit $g_1(x, y), \ldots, g_s(x, y)$ un système complet de formes quadratiques primitives positives deux à deux non équivalentes de discriminant $Df^2 < 0$ (D discriminant de l'ordre maximum du corps $\mathbf{Q}(\sqrt{d})$) et soit m un entier naturel premier avec f. Démontrer que le nombre N de représentations du nombre m par toutes les formes $g_1, \ldots, g_s$ est donné par la formule

$$N = \kappa \sum_{r \mid m} \chi(r),$$

où

$$\kappa = \begin{cases} 6 \text{ pour } D = -3, & f = 1; \\ 4 \text{ pour } D = -4, & f = 1; \\ 2 \text{ pour } Df^2 < -4. \end{cases}$$

19. Soient $g(x, y)$ une forme positive de discriminant D $f^2 < -4$ et q un entier naturel premier avec D f^2. Supposons que tout genre de formes de discriminant D f^2 est formé d'une seule classe. Démontrer que si l'équation $g(x, y) = q$ a exactement quatre solutions en nombres x, y entiers premiers alors le nombre q est premier.

20. Avec les notations de l'exercice 11 du chapitre II, § 7, démontrer que le nombre h_f des classes de modules semblables (au sens usuel) d'un corps quadratique associé à l'ordre $\mathfrak{D}_f$ est donné par la formule

$$h_f = h \frac{f}{e_f} \prod_{p \mid f} \left(1 - \frac{\chi(p)}{p}\right),$$

où χ est le caractère du corps quadratique (p parcourt tous les diviseurs premiers du nombre f).

21. Montrer qu'un nombre premier est représentable par la forme $x^2 + 3y^2$ si et seulement s'il est du type $3n + 1$.

22. Montrer que la forme $x^2 - 5y^2$ représente tous les nombres premiers du type $10n \pm 1$ et ne représente pas les nombres premiers du type $10n \pm 3$.

23. Montrer que la forme $x^2 + 2y^2$ représente un entier naturel m pour des entiers x, y premiers entre eux si et seulement si m est du type

$$m = 2^{\alpha} p_1^{\alpha_1} \ldots p_r^{\alpha_r},$$

avec $\alpha = 0$ ou 1, chacun des nombres premiers impairs p_i étant de la forme $8n + 1$ ou $8n + 3$.

24. Démontrer qu'il existe des corps quadratiques (réels ou imaginaires) admettant un nombre arbitrairement grand de classes de diviseurs.

25. Soient $p_1, \ldots, p_s$ tous les nombres premiers distincts qui figurent dans le discriminant D du corps quadratique $\mathbf{Q}(\sqrt{d})$. Les égalités

$$\left(\frac{p_i, D}{p_j}\right) = (-1)^{a_{ij}} \qquad (1 \leqslant i, j \leqslant s)$$

définissent une matrice (a_{ij}) à éléments dans le corps des résidus modulo 2. Désignons par ρ le rang de cette matrice (dans le corps GF(2)). Démontrer que les nombres des invariants du groupe des classes de diviseurs (au sens strict) du corps $\mathbf{Q}(\sqrt{d})$ qui sont divisibles par 4 est égal à $s - p - 1$.

26. Soient p et q des nombres premiers, $p \neq 2$ et $q \not\equiv p \pmod 4$; démontrer que le nombre de classe de diviseurs du corps $\mathbf{Q}(\sqrt{-pq})$ est divisible par 4 si et seulement si $\left(\frac{4}{0P}\right) = 1$.

27. Soient $p_1, \ldots, p_s$ des nombres premiers distincts de la forme $4n + 1$ et supposons $d = p_1 \ldots p_s \equiv 1 \pmod 8$. Démontrer que tout genre de diviseurs du corps $\mathbf{Q}(\sqrt{-d})$ contient un nombre pair de classes.

28. Soit $\mathbf{Q}(\sqrt{d})$ un corps quadratique réel dont le discriminant ne contient aucun nombre premier de la forme $4n + 3$ et soit ε une unité fondamentale du corps $\mathbf{Q}(\sqrt{d})$. Démontrer que si le genre principal des diviseurs du corps $\mathbf{Q}(\sqrt{d})$ contient un nombre impair de classes (au sens strict), alors $N(\varepsilon) = -1$.

29. Soit p un nombre premier de la forme $8n + 1$. Démontrer que le nombre de classes de diviseurs du corps $\mathbf{Q}(\sqrt{-p})$ est divisible par 4.

CHAPITRE IV

MÉTHODE LOCALE

Au § 7 du chapitre premier nous avons démontré le théorème de Minkowski-Hasse sur les représentations de zéro par des formes quadratiques rationnelles. La formulation de ce théorème et sa démonstration utilisent les plongements du corps Q des nombres rationnels dans les corps $\mathbf{Q}_p$ de nombres p-adiques et dans le corps Q_∞ des nombres réels, i. e. les plongements dans tous les complétés du corps Q. La méthode de résolution d'un problème de théorie des nombres par plongement du corps considéré dans son complété s'appelle la ***méthode locale.*** Cette méthode donne des résultats non seulement pour le corps des nombres rationnels mais aussi pour les corps de nombres algébriques. La méthode locale est aussi un outil fondamental pour l'étude des corps de fonctions algébriques.

Dans ce chapitre, nous étudierons une série de résultats en liaison avec la méthode locale pour un corps quelconque; nous étudierons ensuite, comme application, la représentation des nombres par des formes incomplètes (cf. définition chap. II, § l-3)). On parlera du théorème remarquable de Thue affirmant qu'une équation f (x, y) = c, où f (x, y) est un polynôme homogène à coefficients entiers, irréductible, de degré $\geqslant$ 3, a seulement un nombre fini de solutions en nombres entiers. Thue lui-même a démontré ce théorème à l'aide de la théorie des approximations rationnelles des nombres algébriques. La démonstration utilisant la méthode locale est due à Skolem. Dans la démonstration de Skolem on impose une condition au polynôme $f(x, y)$, mais cette méthode est préférable car elle permet d'aborder en général le problème de la représentation des nombres par des formes décomposables incomplètes. Plusieurs remarques à ce sujet sont faites dans le § 6-4).

Expliquons sur un exemple l'idée essentielle de la méthode de Skolem. Supposons que l'on veuille démontrer que l'équation

$$x^3 + dy^3 = c \tag{1}$$

(où c et d sont entiers et d n'est pas un cube) a un nombre fini de solutions dans les nombres entiers. Considérons le corps cubique Q(0), $\theta = \sqrt[3]{d}$. Nous pouvons alors écrire l'équation (1) sous la forme

$$N(x + y\theta) = c. \tag{2}$$

Ainsi nous sommes ramenés à la recherche dans le module incomplet $\{ 1, \theta \}$ du corps $\mathbf{Q}(\theta)$ des nombres de norme donnée. Plongeons le module $\{ 1, \theta \}$ dans le module complet $\{ 1, \theta, \theta^2 \}$ qui coïncide dans ce cas avec son anneau de stabilisateurs $\mathfrak{D}$. La résolution de l'équation (2) équivaut à la recherche des $\alpha \in \mathfrak{D}$, de norme c, pour lesquels le coefficient z est nul dans la représentation $\alpha = x + y\theta + z\theta^2$. Mais le problème de la recherche dans un module complet de tous les nombres de norme donnée a déjà été résolu (théorème 1 du chapitre II, § 5). Ici, pour le corps $\mathbf{Q}(\theta)$, nous avons $s = 1$, $t = 1$ puisque le polynôme $x^3 - d$ a une racine réelle et deux racines imaginaires conjuguées. Par suite, il existe dans l'ordre $\mathfrak{D}$ une unité ε de norme + 1 et un système fini de nombres $\mu_1, \ldots, \mu_k$ de normes c tels que tout $a \in \mathfrak{D}$ de norme c s'écrive de manière unique sous la forme $\mu_i \varepsilon^u$ pour un certain $i = 1, \ldots, k$ et un certain entier rationnel u. Soit μ un des nombres μ_i. Pour démontrer la finitude du nombre de solutions de l'équation (1), il suffit maintenant de montrer que parmi les nombres $\mu\varepsilon^u$ il en existe seulement un nombre fini du type $x + y\theta$.

Considérons, en même temps que le corps Q(0), ses conjugués $\mathbf{Q}(\theta')$ et $\mathbf{Q}(\theta'')$ et, pour tout $a \in \mathbf{Q}(\theta)$, désignons par $a' \in \mathbf{Q}(\theta')$ et $a'' \in \mathbf{Q}(\theta'')$ les conjugués de a. Si nous posons

$$\mu\varepsilon^u = x + y\theta + z\theta^2,$$

alors, par passage aux nombres conjugués, nous aurons

$$\mu'\varepsilon'^u = x + y\theta' + z\theta'^2,$$
$$\mu''\varepsilon''^u = x + y\theta'' + z\theta''^2.$$

Nous pouvons tirer la valeur de z de ces trois égalités :

$$Z = \gamma_0\varepsilon^u + \gamma_1\varepsilon'^u + \gamma_2\varepsilon''^u,$$

où $\gamma_0, \gamma_1, \gamma_2$ sont des nombres (différents de zéro) du corps $K = \mathbf{Q}(\theta, \theta', \theta'')$.

La résolution des équations (1) ou (2) nous conduit ainsi à la résolution de l'équation

$$\gamma_0\varepsilon^u + \gamma_1\varepsilon'^u + \gamma_2\varepsilon''^u = 0 \qquad (3)$$

par rapport à l'entier rationnel u. On s'attend à ce que l'équation (3) n'ait qu'un nombre fini de solutions mais c'est difficile à démontrer directement.

La méthode de Skolem consiste à considérer la partie gauche de l'équation (3) comme une fonction F(u) analytique dans un domaine p-adique. Si l'équation (1) a une infinité de solutions entières, alors la fonction F(u) a une infinité de zéros entiers. Mais, dans le chapitre premier, § 3, 4), nous avons vu que les entiers p-adiques forment un ensemble compact et par suite la fonction $F(u)$ est égale à 0 sur une suite infinie de nombres ayant une limite (dans son domaine de définition). Dans la théorie des fonctions ana-

lytiques d'une variable complexe, on montre un théorème d'unicité d'après lequel une fonction analytique possédant cette propriété est identiquement nulle. La démonstration de ce résultat se transcrit mot à mot pour les fonctions analytiques p-adiques. Ainsi, la fonction F(u) doit être identiquement nulle, d'où une contradiction.

On voit déjà dans cet exemple que les nombres p-adiques habituels introduits dans le chapitre premier ne suffisent pas. Puisque les nombres $y_{,,}$, γ_1, γ_2, ε, ε', ε'' dans l'équation (3) sont algébriques, il est nécessaire de développer l'analogue de la théorie des nombres p-adiques pour un corps k de nombres algébriques à la place du corps $\mathbf{Q}$ des nombres rationnels et pour un diviseur premier $\mathfrak{p}$ du corps k à la place du nombre premier p. Le § 1 de ce chapitre est consacré à cette généralisation.

§ 1. — CORPS COMPLETS POUR DES VALUATIONS

1) Complété d'un corps pour une valuation

Dans le chapitre premier, § 4, nous avons vu qu'à tout nombre premier p, i. e. à tout diviseur premier du corps Q des nombres rationnels, correspond une métrique p-adique φ_p du corps Q ; le complété de Q pour cette métrique est le corps $\mathbf{Q}_p$ des nombres p-adiques. Pour définir la métrique φ_p, nous n'avons utilisé aucune propriété du corps $\mathbf{Q}$ en dehors de l'existence de la valuation p-adique v_p (cf. formule (1), chap. I[er], § 4). Nous pouvons donc construire des complétés analogues pour un corps k si celui-ci admet une théorie des diviseurs. En effet, si le diviseur premier $\mathfrak{p}$ du corps k correspond à la valuation $v_\mathfrak{p} = \nu$, choisissant un nombre réel ρ, $0 < \rho < 1$, nous pouvons définir sur k une métrique $\varphi = \varphi_\mathfrak{p}$ en posant

$$\varphi(x) = \rho^{\nu(x)} \qquad (x \in k); \tag{1}$$

suivant la méthode du chapitre premier, § 4-1), nous pouvons maintenant construire le complété $\bar{k} = \bar{k}_\mathfrak{p}$ du corps k pour cette métrique (Il est clair que la fonction (1) est une métrique). Le corps $k_\mathfrak{p}$ est appelé le ***complété p-adique du corps k.*** Le complété $\bar{k} = \bar{k}_\mathfrak{p}$ ne dépend pas de la théorie des diviseurs considérée puisqu'il est complètement défini par la donnée de la valuation $\nu = v_\mathfrak{p}$; par suite, nous l'appellerons aussi le ***complété de k pour la valuation*** ν. Dans ce paragraphe, nous étudierons certaines propriétés de ces complétés et de leurs extensions finies.

Soit $\bar{k}$ le complété du corps k pour une valuation ν. Montrons que la valuation ν se prolonge ***de manière unique*** en une valuation de $\bar{k}$. En effet,

nous avons vu dans le chapitre premier, § 4-l) que la métrique φ du corps k (cf. (1)) est prolongeable en une métrique $\bar{\varphi}$ du corps $\bar{k}$ de telle sorte que si $a \in \bar{k}$ et $a = \lim_{n\to\infty} a_n$, $a_n \in k$, alors $\bar{\varphi}(a) = \lim_{n\to\infty} \varphi(a_n)$. Mais dans ce cas, 0 est l'unique point d'accumulation de l'ensemble des valeurs $\varphi(a)$, $a \in k$; par suite, la suite $\{ \varphi(a_n) \}$ ou bien tend vers 0 si $a = 0$ ou bien est constante à partir d'un certain rang si $a \neq 0$. La suite $\nu(a_n)$ tend vers l'infini pour $a = 0$ ou est constante à partir d'un certain rang pour $a \neq 0$. Nous pouvons donc poser

$$\bar{\nu}(a) = \lim_{n\to\infty} \nu(a_n).$$

Il est maintenant facile de vérifier que la fonction $\bar{\nu}(\alpha)$ (dont la valeur ne dépend pas du choix de la suite $\{ a_n \}$) est une valuation du corps $\bar{k}$ et $\bar{\nu}(a) = \nu(a)$ pour tout $a \in k$. Il est évident aussi que la métrique $\bar{\varphi}$ du corps $\bar{k}$ est liée à la valuation $\bar{\nu}$ par la relation

$$\bar{\varphi}(\alpha) = \rho^{\bar{\nu}(\alpha)}, \qquad a \in \bar{k}.$$

Dans la suite, comme nous l'avons fait pour le corps des nombres p-adiques (cf. chap. I[er], § 3-4)), nous définirons la convergence dans le corps $\bar{k}$ au moyen de la valuation $\bar{\nu}$ (à la place de la métrique $\bar{\varphi}$).

Soit $\mathfrak{O}$ l'anneau de la valuation v, i. e. l'anneau de tous les éléments $a \in k$, tels que $\nu(a) \geqslant 0$ (cf. chap. III, § 4-l)). Montrons que l'adhérence $\bar{\mathfrak{O}}$ de l'anneau $\mathfrak{O}$ dans le corps k est l'anneau de la valuation $\bar{\nu}$ (l'adhérence $\bar{A}$ d'un sous-ensemble $A \subset \bar{k}$ est l'ensemble de tous les éléments de kqui sont les limites de suites d'éléments de A). En effet, si $a \in \bar{\mathfrak{O}}$, alors $a = \lim_{n\to\infty} a_n$, avec $a_n \in \mathfrak{O}$; par suite $i(a) = \lim_{n\to\infty} \nu(a_n) \geqslant 0$. Réciproquement, supposons $\bar{\nu}(\alpha) \geqslant 0$. Puisque a est limite d'une suite d'éléments de k, alors pour tout entier naturel n, il existe un élément $a_n \in k$ tel que $\bar{\nu}(\alpha - a_n) \geqslant n$. On a alors $a = \lim_{n\to\infty} a$, et

$$\nu(a_n) = \bar{\nu}(\alpha - (a - a_n)) \geqslant \min (Y(a), \bar{\nu}(\alpha - a_n)) \geqslant 0, \quad \text{i. e. } a_n \bullet \mathfrak{O}.$$

Ceci démontre notre argument.

D'après le théorème 2 du chapitre III, § 4, il existe seulement, à associativité près, un élément premier π qui est caractérisé par la condition $\nu(\pi) = 1$. Cet élément sera également premier dans l'anneau $\bar{\mathfrak{O}}$ (puisque $\bar{\nu}(\pi) = 1$). Désignons par Σ_ν et $\Sigma_{\bar{\nu}}$ les corps résiduels respectivement des valuations ν et $\bar{\nu}$ (cf. fin du chapitre III, § 4-l)). Puisque la congruence modulo π dans l'anneau $\mathfrak{O}$ équivaut à la congruence analogue modulo $\bar{\pi}$ dans l'anneau $\bar{\mathfrak{O}}$,

alors il existe un isomorphisme naturel du corps Σ_v dans le corps $\Sigma_{\bar{v}}$. Par ailleurs, pour tout $\alpha \in \bar{\mathfrak{O}}$, il existe un élément $a \in \mathfrak{O}$ tel que $\bar{v}(\alpha - a) \geqslant 1$, i. e. $a \equiv a \pmod{\pi}$; ainsi l'application $\Sigma_v \to \Sigma_{\bar{v}}$ est un isomorphisme *sur* tout le corps $\Sigma_{\bar{v}}$. On peut donc identifier les corps Σ_v et $\Sigma_{\bar{v}}$.

2) Représentation des éléments sous forme de séries

Nous supposerons dans ce point que ***k*** est un ***corps complet pour la valuation*** v (i. e. un corps complet pour la métrique (1)). L'anneau $\mathfrak{O}$ de la valuation v s'appelle dans *ce* cas ***l'anneau des éléments entiers du corps k.*** Nous désignerons par π un élément premier fixé de l'anneau $\mathfrak{O}$.

Dans ce cas, nous appellerons le corps résiduel Σ de la valuation v le ***corps résiduel du corps k.***

Les séries dans le corps ***k*** possèdent toutes les propriétés démontrées pour les séries p-adiques dans le chapitre premier, § 3-4); en particulier, le théorème 8 du chapitre premier, § 3 s'applique.

Les a_i $(m \leqslant i < \infty)$ étant des éléments entiers fixés, considérons la série

$$\sum_{n=m}^{\infty} \alpha_n \pi^n. \tag{2}$$

Puisque $v(\alpha_n \pi^n) = v(\alpha_n) + n \geqslant n$, alors $\alpha_n \pi^n \to 0$ pour $n \to \infty$, i. e. le terme général de la série (2) tend vers zéro. La série (2) converge donc et sa somme est égale à un certain élément de ***k.*** Réciproquement, tout élément de ***k*** est-il représentable comme somme d'une série du type (2) et dans l'affirmative est-il possible (comme dans le corps des nombres p-adiques, cf. théorème 10, chap. I[er], § 3) de trouver une représentation canonique de ce type pour tout élément de ***k*** ? La réponse à ces deux questions est affirmative.

Choisissons dans l'anneau $\mathfrak{O}$ un système complet $\mathbf{S}$ de résidus modulo π. Nous supposerons que $0 \in \mathbf{S}$, i. e. que l'on a pris 0 comme représentant de la classe des éléments de $\mathfrak{O}$ divisibles par π.

THÉORÈME 1. — ***Soient k un corps complet pour une valuation v, $\mathfrak{O}$ l'anneau des éléments entiers du corps k, π un élément premier dans $\mathfrak{O}$ et S un système complet de résidus*** (contenant ***0) de l'anneau $\mathfrak{O}$ modulo π. Alors tout élément $a \in k$ est représentable comme somme d'une série***

$$a = \sum_{i=m}^{\infty} a_i \pi^i, \tag{3}$$

où $a_i \in \mathbf{S}$ $(m \leqslant i < \infty)$ et une telle représentation est unique (pour π et $\mathbf{S}$ fixés).

DÉMONSTRATION. — Pour $\alpha = 0$ nous avons la représentation $0 = \sum_{i=0}^{\infty} 0.X^i$.

Supposons $a \neq 0$; si v(a) = m, alors $v(a\pi^{-m}) = 0$. L'élément $a\pi^{-m}$ de $\mathfrak{O}$ est congru modulo π à un certain élément de S, soit a_m. Puisque $a\pi^{-m} - a_m = \pi\xi$, $\xi \in \mathfrak{O}$, alors

$$a = a_m\pi^m + \xi\pi^{m+1}.$$

Supposons que pour $n > m$, on ait obtenu la représentation

$$a = a_m\pi^m + \ldots + a_{n-1}\pi^{n-1} + \eta_n\pi^n,$$

avec $a_i \in S$ $(m \leqslant i \leqslant n-1)$, $\eta_n \in \mathfrak{O}$. Choisissons $a_n \in S$ tel que $\eta_n \equiv a \pmod{\pi}$. Puisque $\eta_n = a_n + \eta_{n+1}\pi$, $\eta_{n+1} \in \mathfrak{O}$, alors a admet la représentation

$$a = a_m\pi^m + \ldots + a_n\pi^n + \eta_{n+1}\pi^{n+1}.$$

Continuons ce processus indéfiniment. Puisque $v(\eta_n\pi^n) \geqslant n$, alors $\eta_n\pi^n \to 0$ pour $n \to \infty$; ainsi $a = \sum_{i=m}^{\infty} a_i\pi^i$.

Si tous les coefficients a_n ne sont pas nuls dans la série (3), on peut supposer $a_m \neq 0$. Dans ce cas $v(a_m) = 0$ puisque tous les éléments de $\mathfrak{O}$ qui ne sont pas divisibles par π sont des unités. Mais alors

$$v\left(\sum_{i=m}^{\infty} a_i\pi^i\right) = v(a_m\pi^m) = m.$$

Qn a donc unicité de la représentation pour a = 0. Supposons maintenant que pour $a \neq 0$ nous avons deux représentations :

$$a = \sum_{i=m}^{\infty} a_i\pi^i = \sum_{i=m'}^{\infty} a'_i\pi^i \qquad (a_i, a'_i \in S).$$

Si $a_m \neq 0$ et $a'_{m'} \neq 0$, alors, d'après ce qui précède, $m = m'$. Supposons que nous avons démontré que $a_i = a'_i$ pour $m \leqslant i < n$ $(n \geqslant m)$. Multiplions l'égalité

$$\sum_{i=n}^{\infty} a_i\pi^i = \sum_{i=n}^{\infty} a'_i\pi^i \quad \text{par } \pi^{-n}.$$

Passant à la congruence correspondante modulo π on obtient $a_n \equiv a'_n \pmod{\pi}$ et puisque $a_n, a'_n \in S$, on a $a_n = a'_n$. Le théorème 1 est démontré.

Remarquons que si $k = \mathbf{Q}_p$, $\pi = p$ et $S = \{0, 1, \ldots, p-1\}$, le théorème 1 donne le théorème 10, chapitre premier, § 3.

COROLLAIRE. — *Avec les notations du théorème 1, tout élément entier* $\alpha \in k$ *s'écrit de manière unique sous la forme*

$$a = a_1 + a_1\pi + \ldots + a_n\pi^n + \ldots \ (a_i \in S). \tag{4}$$

Il est facile de voir que le théorème 9 du chapitre premier, § 3, s'applique aux séries du corps *k*. On peut donc ajouter et multiplier les séries convergentes suivant les règles usuelles de l'analyse; en particulier, nous pouvons manipuler les séries du type (2) comme des séries de puissances de π. Remarquons cependant qu'en appliquant les règles d'addition et de multiplication aux séries du type (3), on peut obtenir une série du type (2) dans laquelle les coefficients a_i n'appartiennent pas au système de résidus S; il faut alors, pour obtenir une série du type (3), remplacer chaque coefficient $a_i \in \mathfrak{O}$ par son résidu $a_i \in S$ défini par l'égalité $a_i = a_i + \pi\gamma_i$, en ajoutant, à chaque étape, l'élément $\gamma_i \in \mathfrak{O}$ au coefficient suivant.

Remarque 1. — La représentation des éléments d'un corps valué complet *k* par des séries du type (3) dépend bien entendu du choix du système S de représentants. Parmi l'ensemble de tous les systèmes possibles de représentants, il existe, dans certains cas, des systèmes « meilleurs » que les autres, qui sont fermés multiplicativement ou qui sont des sous-corps du corps *k* (cf. les exercices 7 à 11).

Remarque 2. — Les résultats obtenus ici sont des généralisations des résultats analogues dans les corps de nombres p-adiques (cf. chap. I[er], § 3-4)). Cependant, comme c'est prévisible, le théorème 6, chapitre premier, § 3, n'est pas vrai pour des corps valués complets quelconques; il est conservé seulement pour les corps *k* tels que le corps résiduel de la valuation soit fini. Il en est de même des théorèmes 1 et 2 du chapitre premier, § 5, dans lequel F est un polynôme à coefficients dans $\mathfrak{O}$. Par contre, la démonstration du théorème 3, chapitre premier, § 5, se transpose presque sans changement au cas d'un corps valué complet quelconque *k*. Dans la suite, nous utiliserons le corollaire de ce théorème sous la forme suivante : *Soient* F(X) *un polynôme à coefficients entiers de k et* ξ *un entier de k tel que* $F(\xi) \equiv 0 \pmod{\pi}$ *et* $F'(\xi) \not\equiv 0 \pmod{\pi}$; *il existe alors un élément entier* θ *de k tel que* $\xi \equiv \theta \pmod{\pi}$ *et* $F(\theta) = 0$.

3) Extensions finies d'un corps valué complet

Soit *k* un corps complet pour une valuation v_0. Soit K une extension finie du corps *k*, de degré *n*. D'après le théorème 5 du chapitre III, § 4, il existe une valuation v de K qui prolonge v_0. Nous allons montrer que, dans ce cas, il existe un seul prolongement v tel que K soit complet pour la valuation v.

Soient L un sous-ensemble du corps K qui soit un espace vectoriel sur le corps k et $\omega_1, \ldots, \omega_s$ une base de L sur le corps k. Tout élément $\alpha \in L$ s'écrit alors de manière unique

$$a = a_1\omega_1 + \ldots + a_s\omega_s \qquad (a_i \in k). \tag{5}$$

Si $v_0(a_i) \geqslant N$ $(i = 1, \ldots, s)$, alors, d'après les propriétés des valuations,

$$v(a) \geqslant \min\, v(a_i\omega_i) \geqslant eN + \min\, v(\omega_i)$$

en désignant par e l'indice de ramification de la valuation v par rapport à v_0 (cf. définition chap. III, § 4-3)). Montrons que, réciproquement, les coefficients a_i dans la décomposition (5) sont aussi petits que l'on veut par rapport à v_0 pourvu que l'élément $a \in L$ soit suffisamment petit par rapport à v (Rappelons que les éléments « petits » par rapport à une métrique du type (1) sont caractérisés par de grandes valeurs de la valuation v). Plus précisément, cela signifie que pour tout N on peut trouver M tel que l'inégalité $v(a) \geqslant M$ entraîne les inégalités $v_0(a_i) \geqslant N$ $(i = 1, \ldots, s)$. Pour $s = 1$, c'est évident. La démonstration dans le cas général s'effectue par récurrence sur s. Soit $s \geqslant 2$ et supposons, en contradiction avec notre argument, que pour un certain N il existe des éléments $a \in L$ avec des valeurs de $v(a)$ aussi grandes que l'on désire, telles que l'un au moins des coefficients a_i de la formule (5) satisfasse à l'inégalité $v(a_i) < N$. Il est clair que l'on peut supposer que c'est le premier coefficient a, qui satisfait à cette inégalité. Pour tout entier naturel k, nous pouvons alors trouver un élément $\alpha_k \in L$ tel que $v(\alpha_k) \geqslant k + eN$ et tel que le coefficient $a_1^{(k)}$ défini par la décomposition

$$\alpha_k = a_1^{(k)}\omega_1 + \ldots + a_s^{(k)}\omega_s, \qquad a_i^{(k)} \in k,$$

satisfasse à l'inégalité $v_0\left(a_1^{(k)}\right) < N$. Considérons la suite $\{\beta_k\}$ définie par

$$\beta_k = \alpha_k a_1^{(k)^{-1}} = \omega_1 + b_2^{(k)}\omega_2 + \ldots + b_s^{(k)}\omega_s. \tag{6}$$

Puisque

$$v(\beta_k) = v(\alpha_k) - ev_0\left(a_1^{(k)}\right), \qquad \text{alors} \qquad v(\beta_k) > k.$$

Les différences

$$\beta_{k+1} - \beta_k = \sum_{i=2}^{s} \left(b_i^{(k+1)} - b_i^{(k)}\right)\omega_i$$

appartiennent toutes à un sous-espace de dimension $s - 1$ (engendré par les éléments $\omega_2, \ldots, \omega_s$) et on a

$$v(\beta_{k+1} - \beta_k) \geqslant \min\left(v(\beta_{k+1}), v(\beta_k)\right) > k,$$

i. e. $v(\beta_{k+1} - \beta_k) \to cc$ pour $k \to \infty$. Mais alors, par hypothèse de récurrence, nous aurons aussi, pour tout $i = 2, \ldots, s$,

$$v\left(b_i^{(k+1)} - b_i^{(k)}\right) \to \infty, \quad \text{pour } k \to \infty.$$

Par suite, du fait que le corps k est complet (cf. théorème 7, chap. Ier, § 3), la suite $\{ b_i^{(k)} \}_{k=1}^{\infty}$ converge vers un certain élément $b_i \in k$. Passant à la limite pour $k \to \infty$ dans l'égalité (6) et remarquant que $\beta_k \to 0$, on a

$$\omega_1 + b_2\omega_2 + \ldots + b_s\omega_s = 0,$$

ce qui contredit l'indépendance linéaire des éléments $\omega_1, \ldots, \omega_s$ sur le corps k. Notre argument est démontré.

Prenons maintenant pour L tout le corps K. Si une suite $\{ \alpha_k \}$ d'éléments de K est une suite de Cauchy, i. e. $v(\alpha_{k+1} - \alpha_k) \to \infty$ pour $k \to \infty$, alors, d'après ce qui précède, toutes les suites $\{ a_i^{(k)} \}_{k=1}^{\infty}$ définies par les décompositions

$$\alpha_k = a_1^{(k)}\omega_1 + \ldots + a_n^{(k)}\omega_n \qquad (a_i^{(k)} \in k) \tag{7}$$

($\omega_1, \ldots, \omega_n$ est une base de K sur k) sont convergentes dans le corps k. Mais alors la suite $\{ \alpha_k \}$ est aussi convergente, ce qui démontre que le corps K est complet pour la valuation v. De plus, nous voyons que la convergence dans le corps K pour la valuation v est définie sans ambiguïté à partir de la convergence dans le corps k (pour la valuation v_0).

L'unicité du prolongement de la valuation v_0 au corps K découle facilement de cette dernière remarque. En effet, soit v' un autre prolongement différent de v. D'après l'indépendance des valuations dans le corps K, il existe un élément a tel que $v(a) > 0$ et v'(a) = 0. La suite $\{ \alpha^k \}$ est convergente vers 0 pour la valuation v, mais ne sera pas convergente par rapport à la valuation v' (puisque $v'(\alpha^{k+1} - \alpha^k) = v'(a - 1)$ ne tend pas vers l'infini). On obtient une contradiction puisque, d'après ce qu'on vient de voir, la convergence dans K est indépendante du choix du prolongement v.

Nous avons démontré le théorème suivant.

THÉORÈME 2. — *Soient k un corps complet pour une valuation v_0 et K une extension finie. Il existe seulement un prolongement v de la valuation v_0 au corps* K. *Le corps K est complet pour v et, pour toute base $\omega_1, \ldots, \omega_n$ de l'extension K/k, une suite $\{ \alpha_k \}$, $\alpha_k \in$ K, est convergente si et seulement si toutes les suites $\{ a_i^{(k)} \}$, $1 \leqslant i \leqslant n$, définies par les décompositions (7), convergent dans le corps k.*

4) Éléments entiers

Revenons sur la correspondance entre l'anneau $\mathfrak{O}$ des éléments entiers d'un corps complet k pour la valuation v_0 et l'anneau $\mathfrak{D}$ des éléments entiers d'une extension finie K/k. Puisque la valuation v_0 admet un seul prolongement v au corps K, alors, d'après le théorème 6 du chapitre III, § 3, l'anneau $\mathfrak{D}$ (i. e. l'anneau de la valuation v) coïncide avec la fermeture intégrale de l'anneau $\mathfrak{O}$ dans le corps K. Par suite, la norme $N(\alpha) = N_{K/k}(\alpha)$ de tout élément $a \in \mathfrak{D}$ appartient à $\mathfrak{O}$ et la norme N(E) de toute unité ε de l'anneau $\mathfrak{D}$ est une unité de l'anneau $\mathfrak{O}$. Soit maintenant $a \notin \mathfrak{D}$. Puisque $\alpha^{-1} \in \mathfrak{D}$ n'est pas une unité dans $\mathfrak{D}$, alors $N(\alpha^{-1}) = N(\alpha)^{-1}$ appartient à $\mathfrak{O}$ et n'est pas une unité dans $\mathfrak{O}$. Mais alors $N(a) = (N(\alpha^{-1}))^{-1}$ n'appartient pas à l'anneau $\mathfrak{O}$. Nous avons démontré le théorème suivant.

THÉORÈME 3. — ***Pour qu'un élément a d'une extension finie K/k d'un corps valué complet soit entier, il faut et il suffit que sa norme $N_{K/k}(\alpha)$ soit un élément entier dans k.***

COROLLAIRE. — ***Un élément $\varepsilon \in K$ est une unité de l'anneau $\mathfrak{D}$ si et seulement si sa norme $N(E)$ est une unité de l'anneau $\mathfrak{O}$.***

Les anneaux $\mathfrak{O}$ et $\mathfrak{D}$ admettent bien entendu une théorie des diviseurs. Désignons par $\mathfrak{p}$ et $\mathfrak{P}$ des diviseurs premiers de ces anneaux. Le degré résiduelfdu diviseur $\mathfrak{P}$ par rapport à p, i. e. le degré $(\Sigma : \Sigma_0)$ du corps résiduel Σ du corps K sur le corps résiduel Σ_0 du corps k s'appelle aussi ***le degré résiduel de l'extension K/k***. De la même manière, l'indice de ramification e du diviseur $\mathfrak{P}$ par rapport à $\mathfrak{p}$ est appelé ***l'indice de ramzjîcation de l'extension K/k***. Si π_0 et π sont des éléments premiers respectivement des anneaux $\mathfrak{O}$ et $\mathfrak{D}$, alors, comme nous le savons,

$$\pi_0 = \pi^e \varepsilon, \tag{8}$$

où ε est une unité de l'anneau $\mathfrak{D}$.

Soit S_0 un certain système complet de résidus de l'anneau $\mathfrak{O}$ modulo π_0. Comme ci-dessus, nous supposerons que $0 \in S_0$. Il est facile de voir que si les classes résiduelles $\omega_1, \ldots, \overline{\omega_f}$ de Σ forment une base de l'extension Σ/Σ_0, alors l'ensemble S formé des combinaisons linéaires

$$a_1\omega_1 + \ldots + a_f\omega_f \tag{9}$$

où $a_1, \ldots . a_f$ parcourent, indépendamment l'un de l'autre tous les éléments de S_0, est un système complet de résidus modulo π dans l'anneau $\mathfrak{D}$.

DÉFINITION. — ***Une base*** $\theta_1, \ldots, \theta_n$ ***du corps*** K ***sur*** k ***est dite fondamentale si tous les*** θ_i ***sont entiers et si tout élément entier*** $\alpha \in K$ ***admet une décomposition***

$$\alpha = a_1\theta_1 + \ldots + a_n\theta_n \qquad (a_i \in k)$$

avec des a_i ***entiers dans*** k.

THÉORÈME 4. — ***Soient*** k ***un corps complet pour une valuation*** v_0 ***et*** K ***une extension finie d'indice de ramification*** e ***et de degré résiduel*** f. ***Soient de plus*** Σ_0 ***et*** Σ ***les corps résiduels des corps*** k ***et*** K ***respectivement. Si*** π ***est un élément premier de l'anneau des éléments entiers du corps*** K ***et*** $\bar{\omega}_1, \ldots, \bar{\omega}_f$ ***des classes résiduelles de*** ε ***formant une base de*** Σ ***sur*** Σ_0, ***alors le système des éléments***

$$\omega_i\pi^j, \qquad i = 1, \ldots, f; \qquad j = 0, 1, \ldots, e-1 \tag{10}$$

est une base fondamentale de l'extension K/k.

DÉMONSTRATION. — Montrons tout d'abord que les éléments (10) sont linéairement indépendants sur k. Raisonnant par l'absurde, supposons que

$$\sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}\omega_i\pi^j = 0.$$

pour des éléments non tous nuls $a_{ij} \in k$. Nous pouvons supposer que tous les a_{ij} sont entiers et que l'un d'entre eux au moins est une unité dans $\mathfrak{O}$ (s'il n'en est pas ainsi, il faut multiplier l'égalité ci-dessus par une puissance convenable de l'élément $\pi_0 \in \mathfrak{O}$). Soit j_0 ($0 \leqslant j_0 \leqslant e - 1$) le plus petit indice pour lequel il existe i_0 ($1 \leqslant i_0 \leqslant f$) tel que $a_{i_0 j_0}$ soit une unité de $\mathfrak{O}$. Par suite, si $j < j_0$, alors $v_0(a_{ij}) \geqslant 1$ pour tout i. Puisque $\sum_{i=1}^{f} \bar{a}_{ij_0}\bar{\omega}_i \neq 0$, alors la somme $\sum_{i=1}^{f} a_{ij_0}\omega_i$ n'est pas divisible par π et par suite, pour l'élément

$$\gamma = \sum_{i=1}^{J} a_{ij_0}\omega_i\pi^{j_0},$$

nous avons

$$v(\gamma) = j_0 + v\left(\sum_{i=1}^{f} a_{ij_0}\omega_i\right) = j_0.$$

D'autre part,

$$\gamma = -\sum_{i=1}^{f}\sum_{j \neq j_0}^{c} a_{ij}\omega_i\pi^j.$$

Si $j < j_0$, alors

$$v(a_{ij}\omega_i\pi^j) = f + v(a_{ij}) \geqslant ev_0(a_{ij}) \geqslant e > j_0.$$

Si maintenant $j > j_0$, alors

$$v(a_{ij}\omega_i\pi^j) = j + v(a_{ij}) \geqslant j > j_0.$$

Par suite,

$$v(y) \geqslant \min_{j \neq j_0} v(a_{ij}\omega_i\pi^j) > j_0.$$

La contradiction obtenue démontre l'indépendance linéaire des éléments (10) sur le corps **k.**

Soit maintenant a un élément quelconque de $\mathfrak{D}$. D'après le corollaire du théorème 1, nous avons la congruence

$$a \equiv \xi_0 + \xi_1\pi + \ldots + \xi_{e-1}\pi^{e-1} \pmod{\pi^e},$$

où les ξ_i sont des éléments d'un système fixé S de résidus (modulo π) dans l'anneau $\mathfrak{D}$. Nous prendrons pour S un système de résidus formé de nombres du type (9). Puisque π_0 et π^e sont associés dans $\mathfrak{D}$ (cf. égalité (8)), les congruences dans $\mathfrak{D}$ modulo π_0 et π^e sont équivalentes. Nous avons donc

$$\alpha \equiv \sum_{i=1}^{f} \sum_{j=0}^{e-1} a_{ij}^{(0)}\omega_i\pi^j \pmod{\pi_0}, \quad a_{ij}^{(0)} \in S,$$

ou encore

$$a = \sum_{i=1}^{f} \sum_{j=0}^{e-1} a_{ij}^{(0)}\omega_i\pi^i + \pi_0\alpha_1, \qquad \alpha_1 \in \mathfrak{D}.$$

De manière analogue

$$\alpha_1 = \sum_{i=1}^{f} \sum_{j=0}^{e-1} a_{ij}^{(1)}\omega_i\pi^j + \pi_0\alpha_2, \qquad \alpha_2 \in \mathfrak{D}, \ a_{ij}^{(1)} \in S.$$

Poursuivant indéfiniment cette construction, nous obtenons

$$\alpha_n = \sum_{i=1}^{f} \sum_{j=0}^{e-1} a_{ij}^{(n)}\omega_i\pi^j + \pi_0\alpha_{n+1}, \qquad \alpha_{n+1} \in \mathfrak{D}, \ a_{ij}^{(n)} \in S.$$

Pour i et j fixés, nous avons défmi une suite infinie $\{a_{ij}^{(n)}\}$. Considérons la série

$$\sum_{n=0}^{\infty} a_{ij}^{(n)}\pi_0^n.$$

Puisque les $a_{ij}^{(n)}$ sont entiers, cette série est convergente et sa somme a_{ij} est un élément entier du corps k, i. e. $a_{ij} \in \mathfrak{O}$. Démontrons que

$$a = \sum_{i=1}^{f} \sum_{j=0}^{e-1} a_{ij}\omega_i\pi^j. \tag{11}$$

En effet, d'après la construction des éléments α_1, a,, . . . , nous avons

$$\alpha = \sum_{k=0}^{n-1} \left(\sum_{i=1}^{f} \sum_{j=0}^{e-1} a_{ij}^{(k)}\omega_i\pi^j \right) \pi_0^k + \pi_0^n \alpha_n,$$

et par suite, la différence

$$\alpha - \left(\sum_{i=1}^{f} \sum_{j=0}^{e-1} a_{ij}\omega_i\pi^j \right)$$

est divisible par π_0^n (dans l'anneau 9). Puisque c'est vrai pour tout n, cette différence est donc nulle et l'égalité (11) est démontrée.

Si β est un élément quelconque de K, alors, pour un certain m, $\beta\pi_0^m$ est entier. En le représentant sous la forme (1 1), nous voyons que c'est une combinaison linéaire des éléments (10) à coefficients dans k. Ainsi, le système (10) est une base du corps K sur k et puisque, pour tout entier $a \in$ K, tous les coefficients a_{ij} de la décomposition (11) appartiennent à $\mathfrak{O}$, cette base est fondamentale. Le théorème 4 est démontré.

Puisque le nombre d'éléments de la base (10) est égal à fe, nous avons obtenu le résultat suivant :

THÉORÈME 5. — *L'indice de ramification e et le degré résiduel f d'une extension finie K/k d'un corps valué complet sont liés au degré $n = (K : k)$ par la relation*

$$fe = n.$$

Posons $N_{K/k}(\pi) = \pi_0^m u$, où u est une unité de l'anneau $\mathfrak{O}$. Passant aux normes dans l'égalité (8), nous obtenons

$$N_{K/k}(\pi_0) = \pi_0^n = N_{K/k}(\pi^e\varepsilon) = \pi_0^{me} u^e N_{K/k}(\varepsilon) = \pi_0^{me} v,$$

où v est une unité dans $\mathfrak{O}$. Il en résulte que $n = me$ (et v = 1); par suite $m = f$. Ainsi le degré résiduel f de l'extension K/k peut aussi se définir par l'égalité

$$f = v_0(N_{K/k}(\pi)), \tag{12}$$

où π est un élément premier de l'anneau des éléments entiers du corps K. Nous en tirons facilement que, pour tout $\alpha \in$ K, on a la formule

$$v_0(N_{K/k}(\alpha)) = f\, v(\alpha). \tag{13}$$

Remarquons que l'égalité (12) et le théorème 5 sont des corollaires immédiats du théorème 5 et de la formule (12) du chapitre III, § 5.

DÉFINITION. — ***Si $e = 1$, l'extension K/k est dite non ramifiée. Si maintenant $e = n$, alors K/k est dit totalement ramifié.***

Du théorème 5 résulte que le degré résiduel d'une extension non ramifiée est égal au degré de cette extension. Pour des extensions totalement ramifiées, le corps résiduel Σ coïncide avec Σ_0 (par identification naturelle), i. e. tout élément entier de K est congru modulo π à un élément entier de k.

On peut montrer (exercice 12) que, si le corps résiduel Σ du corps K est séparable sur le corps résiduel Σ_0 du corps k, il existe un corps intermédiaire T, défini de manière unique, tel que l'extension T/k soit non ramifiée et l'extension K/T soit totalement ramifiée. T est appelé le *corps d'inertie* de l'extension K/k.

5) Corps de séries formelles

A tout corps, on peut associer un corps valué complet de séries formelles de puissances défini de la manière suivante.

Soit k_0 un corps quelconque. L'ensemble $\mathfrak{O}$ de toutes les séries formelles

$$a_0 + a_1 t + \ldots + a_n t^n + \ldots \qquad (a_n \in k_0) \tag{14}$$

de la variable t est un anneau commutatif, d'unité 1, pour les opérations habituelles sur les séries de puissances. Cet anneau est sans diviseurs de zéro et il est facile de voir que ses unités sont les séries (14) telles que $a_n \neq 0$. Le corps des fractions de l'anneau $\mathfrak{O}$ est appelé le *corps des séries formelles de t à coefficients dans* le *corps* k_0. On le désignera par $k_0\{t\}$. De manière analogue au cas du corps des nombres p-adiques (cf. chap. I[er], § 3-3)), tout élément $\xi \neq 0$ du corps $k_0\{t\}$ s'écrit de manière unique sous la forme

$$\xi = t^m(c_0 + c_1 t + \ldots + c_n t^n + \ldots). \qquad c_n \in k_0,\ c_0 \neq 0,$$

où m est un certain entier (positif, négatif ou nul). Posant $v(\xi) = m$ pour $\xi \neq 0$ et $v(0) = \infty$, nous obtenons une valuation v sur le corps $k_0\{t\}$ pour laquelle ce corps est complet (comme on le vérifie facilement). L'anneau de la valuation v est égal à l'anneau $\mathfrak{O}$ des séries du type (14). On peut prendre t comme élément premier dans $\mathfrak{O}$; puisque deux séries du type (14) sont congrues modulo t si et seulement si leurs termes constants sont égaux, nous obtenons que toute classe résiduelle de l'anneau $\mathfrak{O}$ modulo t contient un unique représentant appartenant à k_0. Ainsi, le corps résiduel Σ_0 du corps $k_0\{t\}$ s'identifie de manière naturelle au corps k_0.

Il est facile de voir que le corps $k_0\{t\}$ des séries formelles n'est autre que le complété du corps k,(t) des fonctions rationnelles pour la valuation correspondant au polynôme irréductible t de l'anneau $k_0[t]$ (cf. exercice 7 du chapitre I[er], § 4).

Puisque $k_0 \subset k_0\{t\}$ et $k_0 \approx \Sigma_0$, alors la caractéristique du corps des séries formelles est la même que celle de son corps résiduel. Cette propriété caractérise les corps de séries formelles parmi tous les corps valués complets. En effet, si la caractéristique d'un corps valué complet k coïncide avec la caractéristique de son corps résiduel, on montre qu'il existe dans k un sous-corps k_0 dont les éléments forment un système complet de résidus modulo un élément premier π. Mais, pour un tel système de résidus, les opérations sur les séries (3) s'effectuent selon les règles de calcul des séries entières; cela signifie que k est le corps des séries formelles de π à coefficients dans k_0. Dans le cas général la démonstration de l'existence du sous-corps k_0 est assez compliquée et nous ne l'étudierons pas ici.

(Dans les § 7 et 11, on étudiera deux cas particuliers pour lesquels la démonstration est facile).

Si k_0' est une extension du corps k_0, alors il est clair que $k_0'\{t\}$ est une extension du corps $k_0\{t\}$; de plus si k_0'/k_0 est une extension finie, alors $k_0'\{t\}/k_0\{t\}$ est aussi finie et de même degré. Un autre moyen de construire des extensions finies du corps $k_0\{t\}$ est de plonger isomorphiquement ce corps dans le corps $k_0\{u\}$ par $t \to u^n$ (n entier naturel). Si nous identifions le corps $k_0\{t\}$ à son image par cette application, i. e. si nous posons $t = u^n$, alors $k_0\{u\}$ est une extension finie de degré n de $k_0\{t\}$. Il est clair que $k_0\{u\}$ s'obtient à partir de $k_0\{t\}$ par adjonction d'une racine $n^{\text{ième}}$ de t.

Dans le cas des corps de caractéristique 0, toute extension finie du corps $k_0\{t\}$ est d'un des deux types considérés ci-dessus. Plus précisément, on a le résultat suivant :

THÉORÈME *6.* — ***Soit k_0 un corps de caractéristique zéro. Toute extension finie K/k du corps $k = k_0\{t\}$ des séries formelles, d'indice de ramification e, est un sous-corps d'une extension de la forme $k_0'\{u\}$, où k_0' est une extension finie de k_0 et $u^e = t$.***

DÉMONSTRATION. — Désignons par Σ_0 et Σ respectivement les corps résiduels des corps k et K, par f le degré résiduel de l'extension K/k et par π un élément premier du corps K; pour tout entier $\xi \in K$, nous désignerons par $\bar{\xi}$ la classe résiduelle de ξ dans Σ. Comme nous l'avons vu, les éléments du corps forment un système naturel de représentants des classes résiduelles de Σ_0. Montrons qu'il existe un sous-corps S du corps K, contenant k_0 et qui constitue un système complet de représentants du corps résiduel Σ. Puisque toute extension finie d'un corps de caractéristique nulle est mono-

gène, alors $\Sigma = \Sigma_0(\bar{\xi})$, où $\bar{\xi}$ est une certaine classe du corps résiduel Σ. Désignons par $\bar{F}$ le polynôme minimal de l'élément $\bar{\xi}$ sur Σ_0. Remplaçant tous les coefficients du polynôme $\bar{F}$ (qui sont des classes résiduelles de Σ_0) par les résidus correspondants appartenant à k_0, nous obtenons un polynôme F de degré f, irréductible sur k_0, tel que

$$F(\xi) \equiv 0 \pmod{\pi}$$
$$F'(E) \not\equiv 0 \pmod{\pi}.$$

D'après la remarque 2, fin du point 2), il existe un élément entier θ du corps K tel que $\bar{\theta} = \bar{\xi}$ et $F(0) = 0$. Considérons le sous-corps $S = k_0(\theta)$ du corps K. Puisque θ est une racine d'un polynôme irréductible de degré f à coefficients dans k_0, alors $(S : k_0) = f$ et tout élément de S s'écrit de manière unique sous la forme

$$a_0 + a_1\theta + \ldots + a_{f-1}\theta^{f-1} \qquad (a_i \in k_0).$$

Les classes résiduelles modulo π de ces éléments (d'après l'égalité $\bar{\theta} = \bar{\xi}$) coïncident avec les classes résiduelles $\bar{a}_0 + \bar{a}_1\bar{\xi} + \ldots + \bar{a}_{f-1}\bar{\xi}^{f-1}$. Mais puisque $\Sigma = \Sigma_0(\bar{\xi})$ et $(\Sigma : \Sigma_0) = f$, alors ces combinaisons épuisent sans répétition toutes les classes résiduelles de Σ. Ainsi, les éléments du corps S (qui est une extension finie du corps k_0) forment un système complet de représentants des classes résiduelles de Σ.

D'après le théorème 1, le corps K est le corps des séries formelles en π, à coefficients dans S, i. e. $K = S\{\pi\}$. Pour démontrer le théorème (sous une forme plus forte), il suffit de montrer que l'on peut choisir l'élément premier π parmi les racines de degré e de t. Cependant, il n'est pas toujours possible de trouver un tel π dans le corps K et il nous faudra considérer une certaine extension finie k_0' du corps S des coefficients.

D'après (8), nous avons l'égalité :

$$t = \pi^e\varepsilon, \tag{15}$$

où ε est une unité de l'anneau des éléments entiers du corps K. Désignons par a l'élément de S tel que $a \equiv \varepsilon \pmod{\pi}$ et par k_0' le corps $S(\sqrt[e]{\alpha})$ (si $a = \gamma^e$ pour un élément $y \in S$, alors $k_0' = S$). Le corps des séries formelles $K' = k_0'\{\pi\}$ contient K comme sous-corps et est une extension finie de k. Montrons qu'il peut s'écrire sous la forme $k_0'\{u\}$, avec $u^e = t$. Considérons le polynôme $G(X) = X^e - \varepsilon$. Puisque dans le corps K' nous avons

$$G(y) \equiv 0 \pmod{\pi} \qquad \text{et} \qquad G'(\gamma) \not\equiv 0 \pmod{\pi},$$

en posant $y = \sqrt[e]{\alpha}$, alors il existe dans K' une unité η telle que $\eta \equiv y \pmod{\pi}$ et $\eta^e = \varepsilon$ (nous appliquons ici encore la remarque 2 du point 2)).

Remplaçons maintenant l'élément premier π du corps K' par l'élément $u = \pi\eta$. Alors, on peut considérer aussi K' comme le corps des séries formelles en u à coefficients dans le corps k'_0, i. e. $K' = k'_0\{u\}$; par suite, d'après (15), $u^e = t$. Nous avons terminé la démonstration du théorème 6.

Remarque. — Le théorème 6 n'est pas vrai en général pour des extensions finies quelconques d'un corps de séries formelles $k = k_0\{t\}$ de caractéristique $p \neq 0$. Cependant, il reste vrai, comme il est facile de le voir, pour des extensions K/k telles que le corps résiduel Σ soit séparable sur Σ_0, l'indice de ramification e n'étant pas divisible par p.

EXERCICES

1. Une métrique φ non triviale d'un corps k est dite discrète si 0 est l'unique point d'accumulation de l'ensemble des valeurs $\varphi(x)$, $x \in k$. Démontrer que toute métrique discrète est liée par la relation (1) à une certaine valuation du corps k.

2. Soient k un corps valué complet, K/k une extension finie et $\theta_1, \ldots, \theta_n$ une base fondamentale du corps K sur k. Montrer que des éléments

$$\theta'_i = \sum_{j=1}^{n} a_{ij}\theta_j, \qquad a_{ij} \in k,$$

forment une base fondamentale de K sur k si et seulement si le déterminant $\det(a_{ij})$ est une unité de k.

3. Avec les notations du théorème 4, soit

$$\alpha = \sum_{i=1}^{C}\sum_{j=0}^{C-1} a_{ij}\omega_i\pi^j \qquad (a_{ij} \in k)$$

un élément quelconque de K. On pose $m = \min v_0(a_{ij})$. Montrer que si j_0 est la plus petite valeur de l'indice j pour laquelle il existe $i = i_0$ tel que $v_0(a_{i_0 j_0}) = m$, alors

$$v(\alpha) = j_0 + em$$

est une valuation du corps K.

4. Démontrer que tout élément du corps des séries formelles $k_0\{t\}$ qui n'appartient pas à k_0 est transcendant sur le corps k_0.

5. Sous les hypothèses du théorème 6, montrer que le sous-corps $S \subset K$ contenant k_0 et qui constitue un système complet de représentants des classes résiduelles du corps K est unique.

6. Soit k_0 un corps algébriquement clos et de caractéristique nulle. Montrer que, pour tout entier naturel n, il existe seulement une extension finie de degré n du corps $k = k_0\{t\}$ des séries formelles à savoir $k(\sqrt[n]{t})$ (L'unicité est à comprendre à un isomorphisme laissant invariants les éléments de k prés).

7. Démontrer que si la caractéristique du corps résiduel Σ d'un corps valué complet K est nulle, alors il existe dans K un sous-corps S qui est un système complet de représentants des classes résiduelles de Σ et par suite $K = S\{\pi\}$,

où π est un élément premier de l'anneau des éléments entiers du corps K (Pour la démonstration, utiliser le fait que tout corps peut s'obtenir à partir de son sous-corps premier par une extension purement transcendante suivie d'une extension algébrique).

8. Montrer, dans la situation de l'exercice 8, que le sous-corps S est unique si le corps résiduel Σ est algébrique sur son sous-corps premier.

9. Soient K un corps valué complet et Σ son corps résiduel. Démontrer que si Y est un corps parfait de caractéristique p (dans lequel l'élévation à la puissance p est un automorphisme), alors il existe dans K un système S « multiplicativement clos » unique de représentants des classes résiduelles $\bar{\xi} \in \Sigma$, i. e. telles que si a, $\beta \in$ S alors $\alpha\beta \in$ S (Le représentant a $\in$ S de la classe $\bar{\xi}$ est la limite $a = \lim_{n\to\infty} \alpha_n^{p^n}$, où α_n est le représentant de la classe $\bar{\xi}^{p^{-n}}$).

10. Conservant les mêmes notations, supposons que Σ est un corps fini à p^f éléments. Démontrer que le polynôme $t^{p^f} - t$ se décompose en facteurs linéaires dans le corps K et que ses racines forment un système S multiplicativement clos de représentants des classes résiduelles de Σ.

11. Supposons que le corps K de l'exercice 9 ait la même caractéristique p que son corps résiduel parfait Σ. Demontrer qu'alors le système S multiplicativement clos de représentants est aussi « additivement clos » ce qui entraîne que c'est un sous-corps du corps K, puisque K = S $\{\pi\}$ où π est un élément premier du corps K.

12. Soit K une extension finie d'un corps valué complet k. Supposons que le corps résiduel Σ du corps K est séparable sur le corps résiduel Σ_0 du corps k. Montrer qu'alors parmi les corps intermédiaires L, $k \subset L \subset K$, qui ne sont pas ramifiés sur k, il existe un corps maximal T (contenant tous les autres corps intermédiaires non ramifiés sur k). Le corps résiduel du corps T coïncide avec Σ et son degré (T : k) est égal à (Σ : C,).

13. Soit $f(X) = X^m + a_1X^{m-1} + \ldots + a_m$ un polynôme irréductible à coefficients dans un corps valué complet. Démontrer que si le terme constant a,,, est entier, alors tous les autres coefficients a,, . . . , a,-, sont aussi entiers.

14. Soit ζ une racine primitive d'ordre p^s de 1 ($s \geqslant 1$). Démontrer que le corps $\mathbf{Q}_p(\zeta)$ est de degré $(p-1)p^{s-1}$ sur le corps $\mathbf{Q}_p$ des nombres p-adiques. Démontrer de plus que l'extension $\mathbf{Q}_p(\zeta)/\mathbf{Q}_p$ est complètement ramifiée.

15. Soit ζ une racine primitive d'ordre p de 1. Démontrer que

$$\mathbf{Q}_p(\zeta) = \mathbf{Q}_p(\sqrt[p-1]{-p}).$$

16. Soient k un corps valué complet, K/k une extension finie, Σ et Σ_0 les corps résiduels de K et k respectivement. Démontrer que si l'extension Σ/Σ_0 est séparable alors il existe une base fondamentale de K/k formée de puissances (i. e. $\mathfrak{D} = \mathfrak{O}[\theta], \theta \in \mathfrak{D}$, où $\mathfrak{D}$ et $\mathfrak{O}$ sont les anneaux des éléments entiers de K et k).

Indication. — Démontrer que si $\Sigma = C,(\ddot{e})$, alors on peut choisir le représentant $\theta \in \mathfrak{D}$ tel que f(0) soit un élément premier de $\mathfrak{D}$. Ici le polynôme $f(t) \in \mathfrak{O}[t]$ est tel que $\bar{f}(t) \in \Sigma_0[t]$ soit le polynôme minimal de l'élément $\bar{\theta} \in \Sigma$.

17. Démontrer que dans tout corps valué complet, le produit infini $\prod_{n=1}^{\infty}(1+a_n)$, $a, \neq -1$, converge si et seulement si $a_n \to 0$ pour $n \to \infty$.

§ 2. — EXTENSIONS FINIES DES CORPS VALUÉS

Soient k un corps muni d'une valuation $v_\mathfrak{p}$ et $\mathbf{K}/k$ une extension finie. L'anneau $\mathfrak{O} = \mathfrak{O}_\mathfrak{p}$ de la valuation $v_\mathfrak{p}$ admet une théorie des diviseurs avec un unique élément premier p. D'après le théorème 1 du chapitre III, § 5, la fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{O}$ dans le corps $\mathbf{K}$ admet une théorie des diviseurs avec un nombre fini de diviseurs premiers $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ (qui divisent tous p).

Soient $\mathfrak{P}$ un de ces diviseurs premiers de l'anneau $\mathfrak{D}$ et $\mathbf{K}_\mathfrak{P}$ le complété du corps $\mathbf{K}$ pour la valuation $v_\mathfrak{P}$. Les éléments de $\mathbf{K}_\mathfrak{P}$ qui sont les limites d'éléments de k forment un sous-corps isomorphe topologiquement au complété $k_\mathfrak{p}$ du corps k pour la valuation $v_\mathfrak{p}$. D'après le plongement isomorphe $k_\mathfrak{p} \to \mathbf{K}_\mathfrak{P}$, nous considérerons dans la suite que $k_\mathfrak{p}$ est un sous-corps du corps $\mathbf{K}_\mathfrak{P}$. Soit $\mathbf{K} = k(\alpha_1, \ldots, \alpha_r)$. Les éléments $\alpha_i \in \mathbf{K}$ appartiennent aussi à $\mathbf{K}_\mathfrak{P}$ puisque étant algébriques sur k ils sont aussi algébriques sur k,. Par suite, l'extension $k_\mathfrak{p}(\alpha_1, \ldots, \alpha_r)/k_\mathfrak{p}$ est finie (et son degré ne dépasse pas le degré $\mathbf{K}/k$); de plus, d'après le théorème 2 du § 1, le corps $k_\mathfrak{p}(\alpha_1, \ldots, a,)$ est complet. Tout élément de $\mathbf{K}_\mathfrak{P}$ est limite d'une suite d'éléments de $\mathbf{K}$; par suite, d'après l'inclusion $\mathbf{K} \subset k_\mathfrak{p}(\alpha_1, \ldots, \text{a,})$ et le fait que $k_\mathfrak{p}(\alpha_1, \ldots, a,)$ est complet, alors $\mathbf{K}_\mathfrak{P} \subset k_\mathfrak{p}(\alpha_1, \ldots, a,)$. L'inclusion inverse étant vraie, $\mathbf{K}_\mathfrak{P} = k_\mathfrak{p}(\alpha_1, \ldots, \alpha_r)$. Nous avons montré ainsi que l'extension $\mathbf{K}_\mathfrak{P}/k_\mathfrak{p}$ est finie et

$$(\mathbf{K}_\mathfrak{P} : k_\mathfrak{p}) \leqslant (\mathbf{K} : k).$$

Puisque les corps résiduels des valuations $v_\mathfrak{p}$ et $v_\mathfrak{P}$ coïncident respectivement avec les corps résiduels des complétés $k_\mathfrak{p}$ et $\mathbf{K}_\mathfrak{P}$ (cf. fin du § l-l)), le degré résiduel $f_\mathfrak{P}$ du diviseur $\mathfrak{P}$ par rapport à $\mathfrak{p}$ coïncide avec le degré résiduel de l'extension $\mathbf{K}_\mathfrak{P}/k_\mathfrak{p}$. Il est clair également que l'indice de ramification $e_\mathfrak{P}$ du diviseur $\mathfrak{P}$ par rapport à $\mathfrak{p}$ coïncide avec l'indice de ramification $\mathbf{K}_\mathfrak{P}/k_\mathfrak{p}$. D'après le théorème 5 du § 1, les nombres $f_\mathfrak{P}$ et $e_\mathfrak{P}$ sont liés au degré

$$n_\mathfrak{P} = (\mathbf{K}_\mathfrak{P} : k_\mathfrak{p})$$

par la relation

$$f_\mathfrak{P} e_\mathfrak{P} = n_\mathfrak{P}.$$

Rappelons que nous avons supposé dans ce paragraphe que l'extension $\mathbf{K}/k$ est séparable; sous cette hypothèse, étudions le lien entre les complétés $\mathbf{K}_{\mathfrak{P}_1}, \ldots, \mathbf{K}_{\mathfrak{P}_m}$ du corps $\mathbf{K}$ pour tous les prolongements de la valuation $v_\mathfrak{p}$.

Soit $\omega_1, \ldots, \omega_n$ une base de l'extension. Si pour un élément $a \in \mathrm{K}$, dans la représentation

$$\mathrm{a} = a_1\omega_1 + \ldots + a_n\omega_n \qquad (a_j \in k), \tag{1}$$

tous les éléments a_j sont petits par rapport à $\mathfrak{p}$ (i. e. petits pour la valuation $\nu_\mathfrak{p}$) alors cet élément est petit par rapport à tout diviseur premier $\mathfrak{P}_s$. L'inverse est aussi vrai.

LEMME 1. — *Pour tout entier N on peut trouver* M *tel que si* $\nu_{\mathfrak{P}_s}(\alpha) \geqslant \mathrm{M}$ *pour tout* $s = 1, \ldots, m$, *alors tous les coefficients* a_j *de* α *dans la décomposition* (1) *satisfont aux inégalités* $\nu_\mathfrak{p}(\alpha_j) \geqslant N$.

DÉMONSTRATION. — Soit $\omega_1^*, \ldots, \omega_n^*$ la base duale de la base $\omega_1, \ldots, \omega_n$ (cf. appendice § 2-3)); nous utilisons ici la séparabilité de l'extension K/k. On a alors

$$a_j = \mathrm{Tr}_{\mathrm{K}/k}(\alpha\omega_j^*) = \mathrm{Tr}\ \alpha\omega_j^*.$$

Désignons par e_s l'indice de ramification de $\mathfrak{P}_s$ par rapport à $\mathfrak{p}$ et par p un élément premier de l'anneau $\mathfrak{O}_\mathfrak{p}$ de la valuation $\nu_\mathfrak{p}$, tel que $e_s = \nu_{\mathfrak{P}_s}(p)$. Posons

$$\mathrm{M} = \max_{s,j}\ (e_s\mathrm{N} - \nu_{\mathfrak{P}_s}(\omega_j^*)).$$

Si maintenant nous supposons $\nu_{\mathfrak{P}_s}(\alpha) \geqslant \mathrm{M}$ pour tout s, alors, pour tout j, nous aurons

$$\nu_{\mathfrak{P}_s}(\alpha\omega_j^*) \geqslant e_s\mathrm{N} = \nu_{\mathfrak{P}_s}(p^\mathrm{N}),$$

ce qui signifie $\alpha\omega_j^* = p^\mathrm{N}\gamma$, avec $\nu_{\mathfrak{P}_s}(\gamma) \geqslant 0$ $(1 \leqslant s \leqslant m)$. D'après le théorème 6 du chapitre III, § 4, l'élément y appartient à la fermeture intégrale de l'anneau $\mathfrak{O}_\mathfrak{p}$ dans le corps K; par suite Tr $y \in \mathfrak{O}_\mathfrak{p}$, i. e. $\nu_\mathfrak{p}$ (Tr y) $\geqslant 0$, d'où

$$\nu_\mathfrak{p}(a_j) = \nu_\mathfrak{p}\,(\mathrm{Tr}\,(\alpha\omega_j^*)) = \nu_\mathfrak{p}(p^\mathrm{N}\,\mathrm{Tr}\,\gamma) \geqslant \mathrm{N},$$

et le lemme 1 est démontré.

COROLLAIRE. — *Soit* $\{\alpha_k\}$ *une suite d'éléments du corps* K *qui est de Cauchy pour tout diviseur premier* $\mathfrak{P}_s$. *Alors toutes les suites* $\{a_j^{(k)}\}_{k=1}^{\infty}$, *définies par les décompositions*

$$\alpha_k = a_1^{(k)}\omega_1 + \ldots + a_n^{(k)}\omega_n \qquad (a_j^{(k)} \in k),$$

sont de Cauchy pour $\mathfrak{p}$.

Considérons maintenant tous les complétés $\mathrm{K}_{\mathfrak{P}_1}, \ldots, \mathrm{K}_{\mathfrak{P}_m}$ du corps K pour tous les diviseurs premiers $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ et formons la somme directe $\mathrm{K}_{\mathfrak{P}_1} \oplus \ldots \oplus \mathrm{K}_{\mathfrak{P}_m}$, que nous désignerons par K,. Les éléments de cette somme directe sont les suites $\xi = (\xi_1, \ldots, \xi_m)$ où $\xi_i \in \mathrm{K}_{\mathfrak{P}_i}$, $i = 1, 2, \ldots, m$; l'addition et la multiplication de ces suites sont définies composante par composante. Ainsi $\mathrm{K}_\mathfrak{p}$ est muni d'une structure d'anneau. Pour tout $y \in k_\mathfrak{p}$, posons

$$\gamma(\xi_1, \ldots, \xi_m) = (\gamma\xi_1, \ldots, \gamma\xi_m);$$

l'anneau $\mathbf{K}_\mathfrak{p}$ devient ainsi un espace vectoriel sur le corps k,. Si nous désignons par n_s le degré de $\mathbf{K}_{\mathfrak{P}_s}$ sur k,, la dimension de l'espace $\mathbf{K}_\mathfrak{p}$ sur $k_\mathfrak{p}$ est égale à

$$n_1 + \ldots + n_m. \tag{2}$$

On peut définir de manière naturelle une notion de convergence dans l'anneau K,. Nous dirons que la suite $\{(\xi_1^{(k)}, \ldots, \xi_m^{(k)})\}_{k=1}^{\infty}$ converge vers un élément $(\xi_1, \ldots, \xi_m)$ si pour tout s la suite $\{\xi_s^{(k)}\}$ converge vers ξ_s dans le corps $\mathbf{K}_{\mathfrak{P}_s}$. Il est facile de voir que la multiplication par les éléments de $k_\mathfrak{p}$ est continue pour cette notion de convergence, i. e. si

$$y = \lim_{k\to\infty} \gamma^{(k)}, \qquad \gamma^{(k)} \in k_\mathfrak{p} \quad \text{et} \quad \xi = \lim_{k\to\infty} \xi^{(k)}, \ \xi^{(k)} \in \mathrm{K}_\mathfrak{p},$$

alors

$$\lim_{k\to\infty} \gamma^{(k)}\xi^{(k)} = \gamma\xi.$$

Définissons maintenant une application $\mathrm{K} \to \mathbf{K}_\mathfrak{p}$ en posant

$$\widehat{a}=(a, \ldots, \alpha) \in \mathbf{K}_\mathfrak{p}, \qquad \alpha \in \mathbf{K}.$$

Puisque $\mathrm{K} \subset \mathbf{K}_{\mathfrak{P}_s}$ pour tout s, la suite $(a, \ldots, a)$ est bien un élément de K,. Il est clair que l'application $a \to \widehat{\alpha}$ définit un isomorphisme du corps K dans l'anneau $\mathbf{K}_\mathfrak{p}$; nous désignerons par $\widehat{\mathrm{K}}$ l'image du corps K par cet isomorphisme.

Pour éviter une confusion, remarquons que les composantes du produit

$$\gamma\widehat{\alpha} = (\gamma\alpha, \ldots, \gamma\alpha), \qquad \gamma \in k_\mathfrak{p}$$

ne sont pas identiques, comme on pourrait le croire. En effet, le produit $\gamma\alpha$ peut avoir des valeurs différentes dans les différents corps $\mathbf{K}_{\mathfrak{P}_s}$, même si $\gamma\alpha \in k$,.

THÉORÈME 1.- *Si $\omega_1, \ldots, \omega_n$ est une base d'une extension séparable $\mathbf{K}/k$, alors $\widehat{\omega}_1, \ldots, \widehat{\omega}_n$ forment une base de l'anneau $\mathbf{K}_\mathfrak{p}$ comme espace vectoriel sur k,.*

DÉMONSTRATION. — Montrons tout d'abord que $\widehat{\mathrm{K}}$ est partout dense dans $\mathbf{K}_\mathfrak{p}$, i. e. que tout élément de $\mathbf{K}_\mathfrak{p}$ est limite d'une suite d'éléments de $\widehat{\mathrm{K}}$. Soit $\xi = (\xi_1, \ldots, \xi_n)$ un élément quelconque de $\mathbf{K}_\mathfrak{p}$, $\xi_s \in \mathbf{K}_{\mathfrak{P}_s}$ $(s = 1, \ldots m)$. Puisque K est partout dense dans $\mathbf{K}_{\mathfrak{P}_s}$, pour tout entier naturel k il existe un élément $\alpha_s^{(k)} \in \mathrm{K}$ tel que $v_{\mathfrak{P}_s}(\xi_s - \alpha_s^{(k)}) \geqslant k$. D'après le théorème 4 du chapitre III, § 4, il existe dans le corps K un élément $\alpha^{(k)}$ tel que

$$v_{\mathfrak{P}_s}(\alpha_s^{(k)} - \alpha^{(k)}) \geqslant k$$

pourtouts= 1, ... m. Nous avons, pour cet élément $\alpha^{(k)}$,

$$v_{\mathfrak{P}_s}(\xi_s - \alpha^{(k)}) \geqslant k \qquad (s = 1, \ldots m);$$

ainsi, la suite $\{\widehat{\alpha^{(k)}}\}_{k=0}^{\infty}$ d'éléments de $\widehat{K}$ converge vers l'élément ξ dans l'anneau K,.

Représentons chacun des éléments $\alpha^{(k)}$ sous la forme

$$\alpha^{(k)} = a_1^{(k)}\omega_1 + \ldots + a_n^{(k)}\omega_n, \qquad a_j^{(k)} \in k.$$

Puisque la suite $\alpha^{(k)}$ est de Cauchy pour chacun des diviseurs premier; $\mathfrak{P}_s$, alors, d'après le corollaire du lemme 1, chacune des suites $\{a_j^{(k)}\}_{k=1}^{\infty}$ est une suite de Cauchy pour $\mathfrak{p}$ et par suite converge dans k,. Posons

$$\gamma_j = \lim_{k\to\infty} a_j^{(k)} \qquad (j = 1, \ldots, n).$$

Puisque pour tout $a \in k \subset k_{\mathfrak{p}}$ et pour tout $\xi \in \mathbf{K}_{\mathfrak{p}}$ on a

$$a\xi = \widehat{a}\xi \tag{4}$$

alors

$$\widehat{\alpha_k} = \sum_{j=1}^{n} \widehat{a_j^{(k)}}\widehat{\omega_j} = \sum_{j=1}^{n} a_j^{(k)}\widehat{\omega_j}.$$

Passant à la limite dans cette égalité pour $k \to \infty$ et tenant compte de (3), nous obtenons

$$\xi = \lim_{k\to\infty} \widehat{\alpha_k} = \sum_{j=1}^{n} \gamma_j \widehat{\omega_j}.$$

Ainsi, les éléments $\widehat{\omega_j}$ forment un système de générateurs de l'espace vectoriel K,. Il reste à vérifier qu'ils sont linéairement indépendants sur k,. Supposons

$$\gamma_1\widehat{\omega_1} + \ldots + \gamma_n\widehat{\omega_n} = 0, \qquad \gamma_j \in k_{\mathfrak{p}}.$$

Puisque k est dense dans $k_{\mathfrak{p}}$, alors $\gamma_j = \lim_{k\to\infty} a_j^{(k)}$, avec $a_j^{(k)} \in k$. Posons

$$\alpha^{(k)} = a_1^{(k)}\omega_1 + \ldots + a_n^{(k)}\omega_n \in K.$$

On a alors

$$\lim_{k\to\infty} \widehat{\alpha^{(k)}} = \lim_{k\to\infty} \sum_j a_j^{(k)}\widehat{\omega_j} = \sum_j \gamma_j\widehat{\omega_j} = 0.$$

Cela signifie que la suite $\{\alpha^{(k)}\}$ est nulle par rapport à tous les diviseurs premiers $\mathfrak{P}_s$ ($s = 1, \ldots$ m). Mais alors, d'après le corollaire du lemme 1,

toutes les suites $\{a_j^{(k)}\}$ du corps k convergent vers 0 par rapport à $\mathfrak{p}$ et cela signifie

$$\gamma_1 = 0, \ldots, \gamma_n = 0.$$

La démonstration du théorème 1 est terminée.

Remarque. — En termes de produit tensoriel d'algèbres, le théorème 1 signifie que l'algèbre $\mathbf{K}_\mathfrak{p}$ sur le corps $k_\mathfrak{p}$ est isomorphe au produit tensoriel $\mathbf{K} \otimes_k k_\mathfrak{p}$, i. e. peut s'obtenir (comme algèbre sur k) par extension à $k_\mathfrak{p}$ du corps de base k.

D'après ce qui précède, la dimension de l'espace vectoriel $\mathbf{K}_\mathfrak{p}$ sur $k_\mathfrak{p}$ est égale à n = (K : k). D'autre part, cette dimension est égale à la somme (2). Rapprochant ce résultat de l'égalité $n_s = n_{\mathfrak{P}_s} = e_{\mathfrak{P}_s} f_{\mathfrak{P}_s}$, nous obtenons donc

$$\sum_{\mathfrak{P}} e_\mathfrak{P} f_\mathfrak{P} = n$$

($\mathfrak{P}$ parcourt tous les diviseurs premiers de l'anneau $\mathfrak{D}$). Ceci constitue une nouvelle démonstration du théorème 7 du chapitre III, § 5.

THÉORÈME 2. — ***Désignons par $\varphi(X)$ le polynôme caractéristique d'un élément $a \in K$ pour l'extension séparable K/k et par $\varphi_\mathfrak{P}(X)$ son polynôme caractéristique pour l'extension $K_\mathfrak{P}/k_\mathfrak{p}$. Alors on a***

$$\varphi(X) = \prod_{\mathfrak{P}} \varphi_\mathfrak{P}(X).$$

DÉMONSTRATION. — Considérons, dans l'espace vectoriel K,, la transformation linéaire $\xi \to \widehat{\alpha}\xi$ ($\xi \in \mathbf{K}_\mathfrak{p}$).

Si $a\omega_k = \sum_{l=1}^{n} a_{kl}\omega_l$, $a_{kl} \in k$, nous avons aussi, d'après (4),

$$\widehat{\alpha\,\omega_k} = \sum a_{kl}\widehat{\omega_l}.$$

Ainsi, le polynôme caractéristique de la transformation considérée est égal au polynôme caractéristique de la matrice (a_{kl}), i. e. est égal à $\varphi(X)$. Considérons maintenant dans $\mathbf{K}_\mathfrak{p}$ une autre base (sur $k_\mathfrak{p}$). Soit β_{sj} (j = 1, . . . , n,) une base de l'extension $\mathbf{K}_{\mathfrak{P}_s}/k_\mathfrak{p}$ (s = 1, . . . , m). Si nous désignons par $\bar{\beta}_{sj}$ l'élément de $\mathbf{K}_\mathfrak{p}$ dont la composantes ième est égale à β_{s_j} et toutes les autres nulles, alors, l'ensemble des éléments

$$\bar{\beta}_{sj} \ (s = 1, \ldots . m; j = 1, \ldots . n_s) \tag{5}$$

constitue une nouvelle base de l'anneau $\mathbf{K}_\mathfrak{p}$ (sur $k_\mathfrak{p}$). Posons

$$\alpha\beta_{sj} = \sum_{l=1}^{n_s} \gamma_{jl}^{(s)} \beta_{sj}, \qquad \gamma_{jl}^{(s)} \in k_\mathfrak{p} ;$$

ainsi $\varphi_{\mathfrak{P}_s}(X)$ est le polynôme caractéristique de la matrice $(\gamma_{jl}^{(s)})$. Il est facile maintenant de voir que la matrice de la transformation linéaire $\xi \to \alpha\,\widehat{\xi}$ dans la base (5) est une matrice diagonale par blocs, avec les blocs $(\gamma_{jl}^{(s)})$ sur la diagonale principale. Cela démontre le théorème 2.

Pour tout élément $\alpha \in K$, introduisons les notions de norme locale $N_\mathfrak{P}(\alpha)$ et de trace locale $Tr_\mathfrak{P}$ *(a) :*

$$N_\mathfrak{P}(\alpha) = N_{K_\mathfrak{P}/k_\mathfrak{p}}(\alpha), \qquad Tr_\mathfrak{P}(\alpha) = Tr_{K_\mathfrak{P}/k_\mathfrak{p}}(\alpha).$$

Les formules suivantes sont des conséquences évidentes du théorème 2 :

$$N_{K/k}(\alpha) = \prod_{\mathfrak{P}|\mathfrak{p}} N_\mathfrak{P}(\alpha), \qquad Tr_{K/k}(\alpha) = \sum_{\mathfrak{P}|\mathfrak{p}} Tr_\mathfrak{P}(\alpha). \tag{6}$$

La première de ces formules, réunie à l'égalité (13) du § 1, nous donne la relation

$$v_\mathfrak{p}(N_{K/k}(\alpha)) = \sum_{\mathfrak{P}|\mathfrak{p}} f_\mathfrak{P} v_\mathfrak{P}(\alpha), \tag{7}$$

qui a déjà été obtenue, par un autre procédé dans le chapitre III, § 5.

THÉORÈME *3. — Choisissons dans* le *corps* K (séparable sur *k) un élément primitif* θ *tel que* $K = k(\theta)$ *et désignons par* $\varphi(X)$ *son polynôme minimal sur k. Tous les diviseurs premiers* $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ *du corps* K *qui divisent* $\mathfrak{p}$ *sont en correspondance biunivoque avec les facteurs de la décomposition*

$$\varphi(X) = \varphi_1(X) \ldots \varphi_m(X)$$

du polynome $\varphi(X)$ *en facteurs irréductibles dans l'anneau* $k_\mathfrak{p}[X]$. *Pour tout diviseur premier* $\mathfrak{P}_s$, *le polynôme* $\varphi_s(X)$ *qui lui correspond coïncide avec le polynôme minimal de l'élément* $\theta \in K_{\mathfrak{P}_s}$ *sur le corps* $k_\mathfrak{p}$.

DÉMONSTRATION. — D'après le théorème 2, le polynôme caractéristique $\varphi(X)$ de θ pour l'extension K/k est égal au produit $\varphi_1(X) \ldots \varphi_m(X)$ où $\varphi_s(X)$ est le polynôme caractéristique de θ pour l'extension $K_{\mathfrak{P}_s}/k_\mathfrak{p}$. Le facteur $\varphi_s(X)$ est ainsi défini de manière unique par le diviseur premier $\mathfrak{P}_s$. Mais, comme nous l'avons vu au début de ce point, $K_{\mathfrak{P}_s} = k_\mathfrak{p}(\theta)$, $\theta \in K \subset K_{\mathfrak{P}_s}$; par suite, chacun des polynômes $\varphi_s(X)$ est irréductible sur $k_\mathfrak{p}$ et le thtorème est démontré.

Remarque. — Soit $\mathfrak{O}$ un anneau quelconque (de corps des fractions *k)* admettant une théorie des diviseurs et soit $\mathfrak{p}$ un des diviseurs premiers de l'anneau $\mathfrak{O}$. Pour toute extension séparable finie, le théorème 3 donne la description de tous les diviseurs premiers $\mathfrak{P}$ de la fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{O}$ dans K qui divisent $\mathfrak{p}$ (plus précisément, ce théorème donne leur nombre m et la valeur des produits $e_{\mathfrak{P}} f_{\mathfrak{P}}$).

§ 3. — DÉCOMPOSITION DES POLYNOMES EN FACTEURS DANS UN CORPS VALUÉ COMPLET

En liaison avec le théorème 3 du § 2, il est important d'étudier la décomposition des polynômes en facteurs irréductibles dans un corps valué complet. Nous montrerons dans ce paragraphe que, dans un tels corps, la décomposition d'un polynôme à coefficients entiers est complètement définie par sa décomposition modulo une certaine puissance d'un nombre premier.

LEMME. — ***Soient $\mathfrak{O}$ un sous-anneau d'un corps quelconque k et g(X) et h(X) des polynômes respectivement de degrés m et n à coefficients dans $\mathfrak{O}$. Si le résultant $\rho = R(g, h)$ de ces polynômes est non nul, alors, pour tout polynôme $Z(X) \in \mathfrak{O}[X]$ de degré $\leqslant m + n - 1$, il existe dans l'anneau $\mathfrak{O}[X]$ des polynômes $\varphi(X)$ et $\psi(X)$ de degrés $\leqslant n - 1$ et $\leqslant m - 1$ respectivement tels que***

$$\rho l(X) = g(X)\,\varphi(X) + h(X)\,\psi(X). \tag{1}$$

DÉMONSTRATION. — Posons

$$g(X) = \sum_{i=0}^{m} a_i X^{m-i}, \qquad h(X) = \sum_{i=0}^{n} b_i X^{n-i},$$

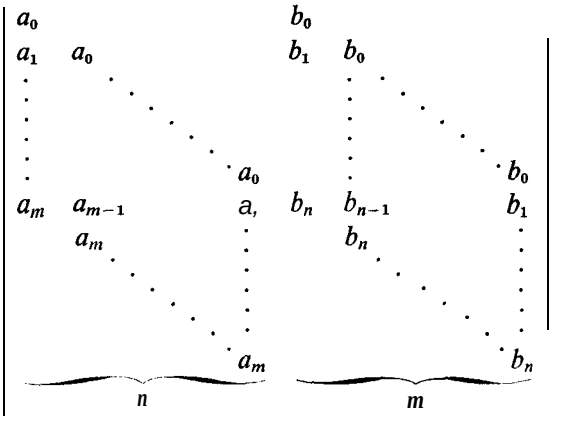
$$l(X) = \sum_{i=0}^{m+n-1} c_i X^{m+n-1-i}$$

$$\varphi(X) = \sum_{i=0}^{n-1} u_i X^{n-1-i}, \qquad \psi(X) = \sum_{i=0}^{m-1} v_i X^{m-1-i}.$$

Pour déterminer les $m + n$ coefficients inconnus $u_0, \ldots, u_{n-1}; v_0, \ldots, v_{m-1}$, nous égalerons dans l'égalité (1) les coefficients des puissances égales de X. Nous obtenons ainsi un système de $m + n$ équations :

$$\sum_{r+s=i} a_r u_s + \sum_{r+s=i} b_r v_s = \rho c_i \quad (i = 0, 1, \ldots, m + n - 1).$$

Le determinant de ce système est égal à



(2)

(les termes non précisés sont nuls), i. e. est égal au résultant $\rho = \mathrm{R}(g, \mathrm{h})$. Par hypothèse $\rho \neq 0$ et par suite le système admet une solution (unique) et puisque tous les éléments ρc_i sont divisibles par ρ, les valeurs des inconnues u_i et v_i appartiennent à l'anneau $\mathfrak{O}$. Le lemme est démontré.

Soient maintenant k un corps complet pour une valuation v, $\mathfrak{O}$ l'anneau des éléments entiers de k et π un élément premier de $\mathfrak{O}$. Deux polynômes $f(\mathrm{X})$ et $f_1(\mathrm{X})$ de l'anneau $\mathfrak{O}[\mathrm{X}]$ sont dits congrus modulo π^k et nous écrirons $f(\mathrm{X}) \equiv f_1(\mathrm{X}) \pmod{\pi^k}$, si les coefficients des mêmes puissances de X dans ces polynômes sont congrus modulo π^k.

THÉORÈME 1. — *Soit $f(\mathrm{X}) \in \mathfrak{O}[\mathrm{X}]$ un polynôme de degré $m + n$; supposons qu'il existe des polynômes $g_0(\mathrm{X})$ et $h_0(X)$, de degrés m et n respectivement, tels que* : 1° *les coefficients dominants des polynômes f et $g_0 h_0$ sont égaux;* 2° *le résultant $\mathrm{R}(g_0, h_0)$ est différent de 0;* 3° *si $\nu(\mathrm{R}(g_0, h_0)) = r$, alors*

$$f(X) \equiv g_0(\mathrm{X})\, h_0(X) \pmod{\pi^{2r+1}}. \tag{3}$$

Alors il existe dans $\mathfrak{O}[\mathrm{X}]$ des polynômes $g(X)$ et $h(X)$ de degrés respectif m et n tels que

$$f(\mathrm{X}) = g(\mathrm{X})\, h(\mathrm{X}),$$
$$g(\mathrm{X}) \equiv g_0(\mathrm{X}), \qquad h(X) \equiv h_0(X) \pmod{\pi^{r+1}},$$

les coefficients dominants de $g(X)$ et $h(X)$ étant égaux respectivement aux coefficients dominants de $g_0(X)$ et $h_0(\mathrm{X})$.

DÉMONSTRATION. — Pour tout $k \geqslant 1$, nous allons construire par récurrence des polynômes $\varphi_k \in \mathfrak{O}[\mathrm{X}]$ de degré $\leqslant m - 1$ et $\psi_k \in \mathfrak{O}[\mathrm{X}]$ de degré $\leqslant n - 1$ tels que les polynômes

$$g_k = g_0 + \pi^{r+1}\varphi_1 + \ldots + \pi^{r+k}\varphi_k,$$
$$h_k = h_0 + \pi^{r+1}\psi_1 + \ldots + \pi^{r+k}\psi_k$$

vérifient la congruence

$$f \equiv g_k h_k \pmod{\pi^{2r+k+1}}. \tag{4}$$

Supposons que l'on a déjà construit des polynômes $\varphi_1, \ldots, \varphi_{k-1}$ et $\psi_1, \ldots, \psi_{k-1}$ possédant les propriétés ci-dessus, d'où

$$f = g_{k-1} h_{k-1} + \pi^{2r+k} l, \tag{5}$$

avec $l(X) \in \mathfrak{O}[X]$. Les polynômes g_0 et g_{k-1} d'une part, h_0 et h_{k-1} d'autre part ont des coefficients dominants égaux; par suite, d'après la première condition, I(X) est de degré $\leqslant m + n - 1$. De plus, $g_{k-1} \equiv g_0$, $h_{k-1} \equiv h_0 \pmod{\pi^{r+1}}$. Ainsi,

$$R(g_{k-1}, h_{k-1}) \equiv R(g_0, h_0) \pmod{\pi^{r+1}},$$

d'où $v(R(g_{k-1}, h_{k-1})) = r$. D'après le lemme, il existe dans l'anneau $\mathfrak{O}[X]$ des polynômes φ_k et ψ_k de degrés respectifs $\leqslant m - 1$ et $\leqslant n - 1$ tels que

$$\pi^r l = g_{k-1}\psi_k + h_{k-1}\varphi_k. \tag{6}$$

Montrons que φ_k et ψ_k satisfont aux conditions demandées. Puisque

$$g_k = g_{k-1} + \pi^{r+k}\varphi_k, \qquad h_k = h_{k-1} + \pi^{r+k}\psi_k$$

alors, d'après (5) et (6),

$$\begin{aligned} f - g_k h_k &= \pi^{2r+k} l - \pi^{r+k}(g_{k-1}\psi_k + h_{k-1}\varphi_k) - \pi^{2r+2k}\psi_k\varphi_k \\ &= -\pi^{2r+2k}\varphi_k\psi_k, \end{aligned}$$

d'où la congruence (4) (puisque $2k \geqslant k + 1$).

Considérons maintenant dans $\mathfrak{O}[X]$ les polynômes

$$g(X) = g_0 + \sum_{k=1}^{\infty} \pi^{r+k}\varphi_k, \qquad h(X) = h_0 + \sum_{k=1}^{\infty} \pi^{r+k}\psi_k$$

dont les coefficients (en dehors des coefficients dominants) sont des sommes de séries convergentes. Puisque $g \equiv g_k$ et $h \equiv h_k \pmod{\pi^{r+k+1}}$, alors

$$gh \equiv g_k h_k \pmod{\pi^{r+k+1}},$$

d'où, d'après (4),

$$f \equiv gh \pmod{\pi^{r+k+1}}.$$

Cette dernière congruence étant vraie pour tout k on a $f = gh$ et le théorème 1 est démontré.

Remarque. — Il résulte facilement de la démonstration du théorème 1 que si g_0 et h_0 satisfont, à la place de la condition (3), à lacondition $f \equiv g_0 h_0 \pmod{\pi^s}$, $s \geqslant 2r + 1$, alors on peut choisir g et h tels que

$$g \equiv g_0, \qquad h \equiv h_0 \pmod{\pi^{s-r}}.$$

Considérons un cas particulier très important du théorème 1.

Un polynôme $f(X) \in \mathfrak{O}[X]$ est dit *primitif* si un au moins de ses coefficients est une unité de $\mathfrak{O}$. Soit Σ le corps résiduel de l'anneau $\mathfrak{O}$ modulo l'élément premier π. Remplaçant dans le polynôme $f \in \mathfrak{O}[X]$ chaque coefficient par sa classe résiduelle nous obtenons un polynôme $\bar{f}$ à coefficient dans Σ. Supposons que $\bar{f}$ admet dans l'anneau $\Sigma[X]$ une décomposition

$$\bar{f} = \bar{g}_0 \bar{h}_0, \tag{7}$$

en facteurs $\bar{g}_0$ et $\bar{h}_0$ premiers entre eux. On peut bien entendu choisir les polynômes f_0 et g_0 de l'anneau $\mathfrak{O}[X]$ tels que le degré de g_0 soit égal au degré de $\bar{g}_0$ et tels que les degrés et les coefficients dominants des polynômes f et $g_0 h_0$ soient égaux. Considérons le résultant $R(g_0, h_0)$ des polynômes g_0 et h_0, i. e. le déterminant du type (2). Remplaçant dans ce déterminant chaque élément par sa classe résiduelle modulo π, nous obtenons un déterminant égal au résultant $R(\bar{g}_0, \bar{h}_0)$ des polynômes $\bar{g}_0$ et $\bar{h}_0$ (il se peut que le coefficient dominant de $\bar{h}_0$ soit nul). Le résultant $R(\bar{g}_0, \bar{h}_0)$ est non nul puisque, d'après le choix de g_0, le coefficient dominant de $\bar{g}_0$ est non nul et que, par hypothèse, les polynômes $\bar{g}_0$ et $\bar{h}_0$ sont premiers entre eux (rappelons que, pour deux polynômes de coefficients dominants quelconques, le résultant est nul si et seulement si ces polynômes ont un facteur commun ou si leurs coefficients dominants sont tous deux nuls). Ainsi, $R(g_0, h_0) \not\equiv 0 \pmod{\text{x}}$, i. e. $v(R(g_0, h_0)) = r = 0$; d'autre part, l'égalité (7) équivaut à la congruence $f \equiv g_0 h_0 \pmod{\text{x}}$. Nous voyons donc que toutes les hypothèses du théorème 1 sont satisfaites pour g_0 et h_0 (et $r = 0$); par suite, on a établi le théorème suivant.

THÉORÈME 2 (lemme de Hensel). — *Soit f(X) un polynôme primitif à coefficients dans l'anneau $\mathfrak{O}$ des éléments entiers d'un corps valué complet et soit Σ le corps résiduel de $\mathfrak{O}$ modulo un élément premier. Si le polynôme $\bar{f} \in \Sigma[X]$ admet la décomposition*

$$\bar{f} = \bar{g}_0 \bar{h}_0 \qquad (g_0, h_0 \in \mathfrak{O}[X])$$

avec $\bar{g}_0$ et $\bar{h}_0$ premiers entre eux, alors il existe dans $\mathfrak{O}[X]$ des polynômes g et h tels que

$$f(X) = g(X) h(X),$$

avec $\bar{g} = \bar{g}_0$, $\bar{h} = \bar{h}_0$ et g et $\bar{g}_0$ de même degré.

Nous pouvons maintenant, en utilisant le théorème 1, résoudre le problème de la décomposition d'un polynôme à coefficients dans un corps valué complet en facteurs irréductibles. Limitons-nous au cas des polynômes $f(X)$ à coefficients entiers et de coefficient dominant 1 (si le coefficient dominant d'un polynôme de $\mathfrak{O}[X]$ de degré n est égal à a, nous pouvons multiplier ce polynôme par a^{n-1} et prendre aX pour nouvelle variable). Puisque le théorème classique de Gauss, sur la décomposition des polynômes à coefficients entiers, est valable dans l'anneau $\mathfrak{O}[X]$, alors, tous les diviseurs irréductibles des polynômes $f(X)$ de coefficient dominant égal à 1 appartiennent aussi à l'anneau $\mathfrak{O}[X]$.

Si le polynôme f(X) n'a pas de racines multiples (dans les extensions finies du corps k), son discriminant D(f) = $\pm$ R(f, f') n'est pas nul. Soit $d = v(D(f))$ et supposons que dans l'anneau $\mathfrak{O}[X]$ on ait la congruence

$$f \equiv \varphi_1 \varphi_2 \ldots \varphi_m \pmod{\pi^{d+1}}, \tag{8}$$

les coefficients dominants des polynômes φ_s (et def) étant égaux à 1. Posons $h_1 = \varphi_1 \ldots \varphi_m$. Puisque le discriminant d'un produit de deux polynômes est donné par la formule

$$D(\varphi\psi) = D(\varphi)\, D(\psi)\, R(\varphi, \psi)^2,$$

à partir de D(f) $\equiv D(\varphi_1 h_1) \pmod{\pi^{d+1}}$, i. e. $v(D(\varphi_1 h_1)) = d$, on obtient $d \geqslant 2r$ avec $r = v(R(\varphi_1, h_1))$. D'après le théorème 1 (cf. la remarque qui suit la démonstration) il existe dans l'anneau $\mathfrak{O}[X]$ des polynômes $g_1(X)$ et $f_1(X)$ tels que $f = g_1 f_1$ et $f_1 \equiv \varphi_2 \ldots \varphi_m \pmod{\pi^{d-r+1}}$. Mais

$$d - r \geqslant d - 2r \geqslant d_1 = v(D(f_1));$$

c'est pourquoi on obtient de manière analogue la décomposition $f_1 = g_2 f_2$, etc... Finalement, nous obtenons la décomposition

$$f(X) = g_1(X) \ldots g_m(X) \tag{9}$$

dans laquelle chaque polynôme $g_s \in \mathfrak{O}[X]$ a le même degré que φ_s.

Si la décomposition (8) a été choisie avec m le plus grand possible, alors tous les polynômes g_s sont irréductibles sur le corps k et nous obtenons le résultat suivant.

THÉORÈME *3. — Si on choisit une décomposition (8) du polynôme f(X) modulo* π^{d+1} *pour laquelle m est maximum, alors la décomposition de f en facteurs irréductibles dans k est de la forme* (9), *chacun des polynômes* g_s *étant de même degré que le polynôme* φ_s *correspondant.*

Signalons le cas particulier du théorème 3 qui correspond à $d = 0$,

i. e. D(f) est une unité de $\mathfrak{O}$. Dans ce cas, la décomposition (8) (par passage au corps résiduel Σ) coïncide avec la décomposition

$$\bar{f} = \bar{\varphi}_1 \dots \bar{\varphi}_m \tag{10}$$

en facteurs irréductibles dans l'anneau $\Sigma[X]$. Nous pouvons énoncer :

COROLLAIRE. — *Soit* $f(X) \in \mathfrak{O}[X]$ *un polynôme dont le discriminant* D(f) *est une unité de l'anneau* $\mathfrak{O}$. *Si la décomposition de* $\bar{f}$ *en facteurs irréductibles dans* $\Sigma[X]$ *est de la forme* (10), *alors il existe dans* $\mathfrak{O}[X]$ *des polynômes* $g_1, \dots, g_m$, *irréductibles sur k, tels que* $f = g_1 \dots g_m$ *et* $\bar{g}_1 = \bar{\varphi}_1, \dots, \bar{g}_m = \bar{\varphi}_m$.

Ce résultat découle aussi directement du théorème 2.

EXERCICES

1. Soient k un corps valué complet, K/k une extension séparable d'indice de ramification e, $\mathfrak{O}$ et $\mathfrak{D}$ les anneaux des éléments entiers des corps k et K respectivement, π_0 et π des éléments premiers de chacun de ces anneaux. Démontrer que si un élément $a \in \mathfrak{D}$ est divisible par π, alors $\mathrm{Tr}_{K/k}(\alpha)$ est divisible par π_0. En déduire que $\mathrm{Tr}_{K/k}(\pi^{1-e}\mathfrak{D}) \subset \mathfrak{O}$. Répétant les arguments des exercices 12 et 16 du § 2 chapitre II, démontrer que, si e > 1, pour tout élément $\theta \in \mathfrak{D}$ de polynôme caractéristique f(r), la valeur $f'(\theta)$ est divisible par π.

2. Soient k une extension finie du corps des nombres p-adiques, e son indice de ramification sur $\mathbf{Q}_p$ et π un élément premier du corps k. Supposons que k contient une racine primitive d'ordre p de 1 d'où e divisible par $p - 1$ (exercice 14 du § 1). Démontrer que tout entier $a \in k$ congru à 1 modulo π^{m+1}, où

$$m = \frac{p}{pe} \frac{-}{} \frac{1}{} = ps = e + s$$

est une puissance $p^{\text{ième}}$ d'un certain élément de k (Utiliser le fait que si $\beta = 1 + \pi^{e+k}\gamma$ (y entier), $k > s$, $p = \pi^e\varepsilon^{-1}$, alors $\beta \equiv (1 + \pi^k\gamma\varepsilon)^p$ (mo $\mathfrak{d}\pi^{e+k+1}$). Appliquer ensuite l'exercice 17 du § 1).

3. Sous les hypothèses de l'exercice 2, supposons que l'entier a est congru à 1 modulo π^m mais n'est pas une puissance $p^{\text{ième}}$ d'un élément de k. Démontrer qu'alors $k(\sqrt[p]{\alpha})/k$ est une extension non ramifiée de degré p (Trouver le polynôme caractéristique f(t) de l'élément $y = \pi^{-s}(\sqrt[p]{\alpha} - 1)$ et établir que f'(0) est une unité; appliquer alors le dernier résultat de l'exercice 1).

4. Conservant les hypothèses de l'exercice 2, supposons que l'entier $a \in k$ satisfait aux conditions : $a \equiv 1 \pmod{\pi^h}$, $a \not\equiv 1 \pmod{\pi^{h+1}}$, $(h, p) = 1$, $h < m = \frac{A}{P-1}$. Démontrer qu'alors a n'est pas la puissance $p^{\text{ième}}$ d'un élément de k et que l'extension $k(\sqrt[p]{\alpha})/k$ est complètement ramifié (Considérer l'exposant avec lequel l'élément premier du corps $k(\sqrt[p]{\alpha})$ figure dans la différence $1 - a = \prod_{i=0}^{p-1}(1 - \zeta^i\sqrt[p]{\alpha})$, où ζ est une racine primitive d'ordre p de 1).

§ 4. — LES MÉTRIQUES D'UN CORPS DE NOMBRES ALGÉBRIQUES

1) Description des métriques

Dans le chapitre premier, § 4-2), nous avons montré que tous les complétés possibles du corps Q des nombres rationnels sont les corps $\mathbf{Q}_p$ de nombres p-adiques et le corps $\mathbf{Q}_\infty = \mathbf{R}$ des nombres réels. Nous allons maintenant résoudre cette question pour un corps quelconque k de nombres algébriques. En accord avec le début du § 1, à tout diviseur premier $\mathfrak{p}$ du corps k correspond un complété p-adique $k_\mathfrak{p}$, i. e. un complété pour la métrique $\varphi_\mathfrak{p}(x) = \rho^{\nu_\mathfrak{p}(x)}$ $x \in k$ $(0 < \rho < 1)$. La métrique $\varphi_\mathfrak{p}$ est appelée une ***métrique p-adique du corps k.*** Pour étudier tous les complétés possibles du corps k, il nous faut expliciter, en dehors des métriques p-adiques, toutes les autres métriques des corps de nombres algébriques.

Soit φ une métrique non triviale quelconque d'un corps k de nombres algébriques. Prenant la restriction au corps des nombres rationnels, nous obtenons une métrique φ_0 du corps Q; montrons tout d'abord que la métrique φ_0 est aussi non triviale. Choisissons dans k une base quelconque $\omega_1, \ldots, \omega_n$ sur Q. Pour tout $\xi = a_1\omega_1 + \ldots + a_n\omega_n$ $(a_i \in Q)$, nous avons

$$\varphi(\xi) \leqslant \varphi_0(a_1)\,\varphi(\omega_1) + \ldots + \varphi_0(a_n)\,\varphi(\omega_n).$$

Si la métrique φ_0 était triviale, alors, puisque $\varphi_0(a_i) \leqslant 1$, on aurait l'inégalité

$$\varphi(\xi) \leqslant \sum_{i=1} \varphi(\omega_i)$$

pour tout $\xi \in k$. Mais cela est impossible puisque l'ensemble des valeurs d'une métrique non triviale n'est pas borné.

D'après le théorème 3 du chapitre premier, § 4, la métrique φ_0 est égale, soit à une métrique p-adique $\varphi_\mathfrak{p}(x) = \rho^{\nu_\mathfrak{p}(x)}$, $0 < \rho < 1$, soit à une métrique $|x|^\rho$, $0 < \rho \leqslant 1$ $(x \in \mathbf{Q})$. Considérons tout d'abord le premier cas et désignons par $\mathfrak{O}_\mathfrak{p}$ l'anneau des nombres rationnels p-entiers (i. e. l'anneau de la valuation $\nu_\mathfrak{p}$) et par $\mathfrak{D}_\mathfrak{p}$ sa fermeture intégrale dans k. Si $\omega_1, \ldots, \omega_n$ est une base fondamentale du corps k, alors tout $a \in \mathfrak{D}_\mathfrak{p}$ s'écrit

$$a = a_1\omega_1 + \ldots + a_n\omega_n$$

à coefficients $a_i \in \mathfrak{O}_\mathfrak{p}$. Mais $\varphi_\mathfrak{p}(a_i) \leqslant 1$, d'où

$$\varphi(\alpha) \leqslant \sum_{i=1}^{n} \varphi(\omega_i)$$

et puisque, avec a, toutes les puissances α^k ($k \geqslant 0$) appartiennent aussi à $\mathfrak{D}_\mathfrak{p}$, alors $\varphi(\alpha) \leqslant 1$. Il en résulte facilement maintenant que $\varphi(\varepsilon) = 1$ pour toute unité ε de l'anneau $\mathfrak{D}_\mathfrak{p}$. D'après le théorème 7 du chapitre III, § 7, tout nombre $\xi \neq 0$ de k s'écrit de manière unique

$$\xi = \varepsilon \pi_1^{k_1} \dots \pi_m^{k_m}, \tag{1}$$

où ε est une unité de $\mathfrak{D}_\mathfrak{p}$ et $\pi_1, \dots, \pi_m$ un système fixé d'éléments premiers deux à deux non associés (le nombre $\xi \in \mathfrak{D}_\mathfrak{p}$ si et seulement si $k_i \geqslant 0$). Si $\varphi(\pi_i) = 1$ pour tout i, alors $\varphi(\xi)$ serait égal à 1 pour tout $\xi \neq 0$, ce qui contredit la non-trivialité de ξ. Supposons que $\varphi(\pi_i) < 1$ et $\varphi(\pi_j) < 1$ pour deux indices i et j distincts. Soient k et l des entiers naturels tels que ;

$$\varphi(\pi_i)^k + \varphi(\pi_j)^l < 1.$$

Les nombres π_i^k et π_j^l sont premiers entre eux dans l'anneau $\mathfrak{D}_\mathfrak{p}$; par suite, d'après le lemme 2 du chapitre III, § 6, il existe des éléments α et β de $\mathfrak{D}_\mathfrak{p}$ tels que

$$1 = \alpha \pi_i^k + \beta \pi_j^l.$$

Mais alors

$$1 = \varphi(1) \leqslant \varphi(\alpha)\, \varphi(\pi_i)^k + \varphi(\beta)\, \varphi(\pi_j)^l \leqslant \varphi(\pi_i)^k + \varphi(\pi_j)^l < 1,$$

et nous avons obtenu de nouveau une contradiction. Ainsi, il existe seulement un élément premier π_i tel que $\varphi(\pi_i) < 1$. Désignons par $\mathfrak{p}$ et $\nu_\mathfrak{p}$ le diviseur premier et la valuation qui lui correspondent. Puisque dans la décomposition (1), l'exposant k est égal à $\nu_\mathfrak{p}(\xi)$ alors, désignant par ρ_1 la valeur $\varphi(\pi_i)$, nous aurons :

$$\varphi(\xi) = \rho_1^{\nu_\mathfrak{p}(\xi)}. \tag{2}$$

Faisant $\xi = p$, nous obtenons $\rho = \rho_1^e$, où e est l'indice de ramification du diviseur premier $\mathfrak{p}$. La formule (2) ainsi obtenue montre que la métrique φ coïncide avec la métrique p-adique $\varphi_\mathfrak{p}$ qui correspond au diviseur premier p.

Étudions maintenant le cas où $\varphi_0(x) = |x|^\rho$, $0 < \rho \leqslant 1$ ($x \in Q$).

Le complété du corps Q pour la métrique $|x|^\rho$ est, comme nous le savons, le corps des nombres réels (quel que soit p). Nous le désignerons par $\mathbf{Q}_\infty$ comme dans le chapitre premier, § 7-2). Le prolongement de la métrique $|x|^\rho$, $x \in Q$ au corps $\mathbf{Q}_\infty$ est, bien entendu, la métrique $|\alpha|^\rho$, $a \in \mathbf{Q}_\infty$. Adjoignant au corps Q_∞ le nombre $\sqrt{-1}$, nous obtenons le corps C des nombres complexes. Montrons que la métrique $|a|^\rho$ du corps $\mathbf{Q}_\infty$ se prolonge de manière unique au corps C en la métrique $|\xi|^\rho$, où $|\xi|$ désigne le module du nombre complexe ξ. Soit ψ un tel prolongement. Alors $\psi(\xi) = 1$ pour tout $\xi \in C$ dès que $|\xi| = 1$. En effet, dans le cas

contraire, il existerait un nombre complexe ξ tel que $|\xi| = 1$ et $\psi(\xi) > 1$; choisissant un entier naturel quelconque n et posant $\xi^n = \alpha + \beta_i$ (a, $\beta \in \mathbf{Q}_\infty$), nous obtiendrions

$$\psi(\xi^n) \leqslant \psi(\alpha) + \psi(\beta)\,\psi(i) \leqslant 1 + \psi(i),$$

puisque $\psi(\alpha) = \mathrm{d}\,\mathrm{p} \leqslant 1$ et de même $\psi(\beta) \leqslant 1$. Mais cela est impossible puisque $\psi(\xi)^n > 1 + \psi(i)$ pour n assez grand. Soit maintenant $\xi \neq 0$ un nombre complexe quelconque. D'après ce qui précède, $\psi\left(\frac{\xi}{|\xi|}\right) = 1$; par suite,

$$\psi(\xi) = \psi(|\xi|) = |\xi|^{\rho},$$

ce qu'il fallait démontrer.

Tout corps k de nombres algébriques de degré $n = s + 2t$ (cf. chap. II, § 3-l)) admet n isomorphismes distincts dans le corps C des nombres complexes (s réels et t couples d'isomorphismes complexes). Soit σ l'un d'entre eux. Si pour tout $\xi \in k$ nous posons

$$\varphi_\sigma(\xi) = |\sigma(\xi)|^{\rho},$$

la fonction φ_σ est une métrique du corps k et par suite $\varphi_\sigma(x) = |x|^{\rho}$ pour $x \in Q$. Si σ et 6 sont des isomorphismes conjugués, alors

$$|\bar{\sigma}(\xi)| = |\overline{\sigma(\xi)}| = |\sigma(\xi)|,$$

et par suite les métriques φ_σ et $\varphi_{\bar{\sigma}}$ correspondantes coïncident. Nous avons ainsi mis en évidence $s + t$ métriques du corps k qui coïncident sur Q avec la métrique $|x|^{\rho}$.

Soit maintenant φ une métrique quelconque du corps k qui coïncide sur Q avec la métrique $|x|^{\rho}$. Soit $\bar{\varphi}$ l'unique prolongement de φ au corps $\bar{k}_\varphi$ complété du corps k pour la métrique φ. Il est clair que l'adhérence $\bar{\mathbf{Q}}$ du corps des nombres rationnels dans $\bar{k}_\varphi$ est topologiquement isomorphe au corps $\mathbf{Q}_\infty$ des nombres réels. Si on désigne par σ l'isomorphisme topologique (unique) de $\bar{\mathbf{Q}}$ sur $\mathbf{Q}_\infty$, pour tout $y \in \bar{\mathbf{Q}}$, on aura $\bar{\varphi}(\gamma) = |\sigma(\gamma)|^{\rho}$. Soit θ un élément primitif de k, i. e. $k = Q(0)$, et désignons par f(X) le polynôme minimal de θ sur $\mathbf{Q}$. Le polynôme f(X) se décompose dans le corps des nombres réels en s facteurs linéaires et t facteurs du second degré. Par suite, dans le corps $\bar{\mathbf{Q}}$, on a la décomposition

$$f(X) = (X - \theta_1) \ldots (X - \theta_s)(X^2 + p_1X + 43 \ldots (X^2 + p_tX + q_t).$$

Puisque $f(\theta) = 0$, θ est racine de l'un de ces facteurs.

Supposons tout d'abord que $\theta = \theta_i$. Puisque $\theta \in \bar{\mathbf{Q}}$ et $k = Q(0) \subset \bar{\mathbf{Q}}$,

l'isomorphisme $\sigma : \overline{\mathbf{Q}} \to \mathbf{Q}_\infty$ induit sur k un isomorphisme $\sigma : k \to C$; par suite, si $\xi \in k$, on a

$$\varphi(\xi) = \bar{\varphi}(\xi) = |\sigma(\xi)|^\rho.$$

La métrique φ coïncide ainsi avec φ_σ. De plus, on voit que, dans ce cas, $\bar{k}_\varphi = \overline{\mathbf{Q}}$, i. e. le complété $\bar{k}_\varphi$ est topologiquement isomorphe au corps des nombres réels.

Supposons maintenant que θ est racine d'un des trinômes du second degré. Dans ce cas, $(\overline{\mathbf{Q}}(\theta) : \overline{\mathbf{Q}}) = 2$ et par suite l'isomorphisme $\sigma : \overline{\mathbf{Q}} \to \mathrm{Q}_\infty$ est prolongeable (de deux manières) en un isomorphisme $\sigma : \overline{\mathbf{Q}}(\theta) \to \mathrm{C}$. Le plongement $\sigma : k \to \mathrm{C}$ induit par cet isomorphisme est bien entendu un isomorphisme complexe de k dans le corps C des nombres complexes. D'après ce qu'on a vu, il existe une seule métrique sur C qui coïncide sur $\mathbf{Q}_\infty$ avec la métrique $|\alpha|^\rho$, à savoir $|\eta|^\rho$, $\eta \in \mathrm{C}$. Ainsi, pour tout $\xi \in k$, nous aurons

$$\varphi(\xi) = \bar{\varphi}(\xi) = |\sigma(\xi)|^\rho,$$

i. e. $\varphi = \varphi_\sigma$, pour l'isomorphisme complexe σ; le corps $\bar{k}_\varphi$ (égal à Q(0)) est topologiquement isomorphe au corps de tous les nombres complexes.

Nous avons démontré le théorème suivant.

THÉORÈME 1. — *Toute métrique non triviale φ d'un corps k de nombres algébriques de degré $n = s + 2t$ coïncide, soit avec une métrique p-adique*

$$\varphi_\mathfrak{p}(\xi) = \rho^{\nu_\mathfrak{p}(\xi)}, \qquad 0 < \rho < 1, \qquad \xi \in k,$$

correspondant à un certain diviseur premier $\mathfrak{p}$, soit avec une des $s + t$ métriques de la forme

$$\varphi_\sigma(\xi) = |\sigma(\xi)|^\rho, \qquad 0 < \rho \leqslant 1, \qquad \xi \in k,$$

où σ est un isomorphisme du corps k dans le corps C des nombres complexes.

DÉFINITION. — *Le complété $k_\mathfrak{p}$ d'un corps k de nombres algébriques pour la métrique $\varphi_\mathfrak{p}$ est appelé un corps de nombres p-adiques.*

Il résulte du théorème 1 que tous les complétés possibles du corps k (de nombres algébriques) sont épuisés par les corps de nombres p-adiques, le corps des nombres réels (pour $s > 0$) et le corps des nombres complexes (pour $t > 0$).

Pour souligner l'analogie entre les métriques $\varphi_\mathfrak{p}$ et φ_σ pour un corps k de nombres algébriques de degré $n = s + 2t$, nous considérerons $s + t = r$ (nouveaux objets $\mathfrak{p}_{1,\infty}, \ldots, \mathfrak{p}_{r,\infty}$ appelés *diviseurs premiers infinis* qui sont en correspondance biunivoque avec les métriques du type φ_σ. Les diviseurs premiers habituels sont alors appelés *diviseurs premiers finis*. Un diviseur

premier infini $\mathfrak{p}_{i,\infty}$ correspondant à une métrique φ_σ est dit réel si l'isomorphisme σ est réel et ***complexe*** si l'isomorphisme σ est complexe.

Dans le cas du corps Q des nombres rationnels, il existe un seul diviseur premier infini p_∞ (réel), que nous avons considéré déjà dans le chapitre premier, § 7-2) et avons désigné par le symbole ∞. Tous les diviseurs premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ du corps $\boldsymbol{k}$ qui correspondent au prolongement à $\boldsymbol{k}$ de la valuation p-adique ν_p divisent le nombre $\boldsymbol{p}$ (que nous pouvons considérer comme un diviseur du corps $\mathbf{Q}$). Par analogie, on dira que les diviseurs premiers infinis $\mathfrak{p}_{1,\infty}, \ldots, \mathfrak{p}_{r,\infty}$ divisent p_∞ puisque les métriques correspondantes sont les prolongements de la métrique $|\ x\ |^p$ du corps des nombres rationnels.

Dans le cas considéré ici de l'extension $k/\mathbf{Q}$ et du nombre premier rationnel $\boldsymbol{p}$, l'anneau $\mathbf{K}_\mathfrak{p}$ introduit au § 2 coïncide avec l'anneau k_p des suites $(\xi_1, \ldots, \xi_m)$ où $\xi_i \in k_{\mathfrak{p}_i}$. La dimension de l'anneau k_p considéré comme un espace vectoriel sur le corps $\mathbf{Q}_p$ des nombres p-adiques est égal à $n = (\boldsymbol{k} : \boldsymbol{Q})$ (théorème 1 du § 2). L'analogue de cette notion pour le diviseur premier infini $\boldsymbol{p}_\infty$ est l'anneau k_{p_∞} des suites $(\xi_1, \ldots, \xi_s, \xi_{s+1}, \ldots, \xi_{s+t})$, où ξ_i $(1 \leqslant i \leqslant s)$ appartient au corps des nombres réels et ξ_{s+j} $(1 \leqslant j \leqslant t)$ au corps des nombres complexes. L'anneau k_{p_∞} étant un espace vectoriel de dimension $n = (\boldsymbol{k} : \mathrm{Q})$ sur le corps $\mathbf{Q}_\infty$ des nombres réels coïncide donc avec l'anneau $\mathfrak{L}^{s,t}$, étudié au chapitre II, qui s'est avéré un instrument essentiel dans l'étude du groupe des unités et des classes de modules du corps $\boldsymbol{k}$ de nombres algébriques. L'anneau k_{p_∞} jouera aussi un rôle important dans le chapitre V, § 1.

2) Relations entre métriques

Pour tout diviseur premier $\mathfrak{p}$ (fini ou infini) du corps $\boldsymbol{k}$ introduisons la notion de ***métrique normée*** $\varphi_\mathfrak{p}$, définie par un choix explicite du nombre p. Si $\mathfrak{p}$ est un diviseur premier fini, nous définirons la métrique normée $\varphi_\mathfrak{p}$ par l'égalité

$$\varphi_\mathfrak{p}(\xi) = \left(\frac{1}{\mathrm{N}(\mathfrak{p})}\right)^{\nu_\mathfrak{p}(\xi)}, \qquad \xi \in k,$$

où N(p) est la norme du diviseur p. Si $\mathfrak{p}$ est un diviseur infini réel correspondant à un isomorphisme réel $\sigma : \boldsymbol{k} \to \mathrm{C}$, nous poserons

$$\varphi_\mathfrak{p}(\xi) = |\ \sigma(\xi)\ |, \qquad \xi \in k.$$

Enfin, si $\mathfrak{p}$ est un diviseur premier infini complexe correspondant aux isomorphismes complexes conjugués σ et $\bar{\sigma}$, nous définirons la métrique normée $\varphi_\mathfrak{p}$ par la formule

$$\varphi_\mathfrak{p}(\xi) = |\ \sigma(\xi)\ |^2 = |\ \bar{\sigma}(\xi)\ |^2 = \sigma(\xi)\bar{\sigma}(\xi).$$

Dans ce dernier cas, remarquons que la fonction $|\sigma(\xi)|^2$ n'est pas, à vrai dire, une métrique au sens de la définition du chapitre premier, § 4-1) puisqu'elle ne satisfait pas à l'inégalité triangulaire. Pourtant, cette fonction, étant le carré d'une métrique, peut être utilisée pour définir une notion de convergence sur le corps k et nous la mettrons sur le même plan que les métriques.

Pour tout $\xi \neq 0, \xi \in k$, il n'existe qu'un nombre fini de diviseurs premiers $\mathfrak{p}$ tels que $\varphi_{\mathfrak{p}}(\xi) \neq 1$. Cela nous permet de donner un sens au produit formel infini $\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\xi)$.

THÉORÈME 2. — *Pour tout nombre $\xi \neq 0$ d'un corps k de nombres algébriques, les valeurs $\varphi_{\mathfrak{p}}(\xi)$ de toutes les métriques normées satisfont à la relation*

$$\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\xi) = 1. \tag{3}$$

($\mathfrak{p}$ parcourt tous les diviseurs premiers, finis et infinis, du corps k).

DÉMONSTRATION. — Désignons par P et P' les produits des valeurs $\varphi_{\mathfrak{p}}(\xi)$ étendues aux $\mathfrak{p}$ infinis et finis respectivement; le produit qui figure dans la partie gauche de l'égalité (3) est ainsi égal à PP'. Par définition des métriques normées pour les $\mathfrak{p}$ infinis, nous avons

$$P = \prod_{\sigma} |\sigma(\xi)| = \left|\prod_{\sigma} \sigma(\xi)\right| = |N(\xi)|$$

(ici σ parcourt les $n = s + 2t$ isomorphismes de k dans le corps C). Par ailleurs, d'après la formule (1) du chapitre III, § 7, la norme du diviseur principal $(\xi) = \prod_{\mathfrak{P}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\xi)}$ (ici $\mathfrak{p}$ parcourt tous les diviseurs premiers finis) est égale à

$$|N(E)| = N\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\xi)}\right) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{\nu_{\mathfrak{p}}(\xi)} = \frac{1}{P'},$$

ce qui démontre le théorème.

EXERCICES

1. Soient $\varphi_1, \ldots, \varphi_r$ $(r = s + t)$ les métriques d'un corps k de nombres algébriques de degré $n = s + 2t$ qui correspondent aux diviseurs premiers infinis. Démontrer que pour tout $i = 1, \ldots, r$ il existe un nombre $\xi_i \in k$ tel que

$$\varphi_i(\xi_i) > 1, \qquad \varphi_j(\xi_i) < 1, \qquad j \neq i.$$

En déduire que les métriques $\varphi_1, \ldots, \varphi_r$ définissent des notions de convergence distinctes sur k.

2. Montrer que toute relation de la forme

$$\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\xi)^{m_{\mathfrak{p}}} = 1, \qquad \xi \in k^*,$$

entre les métriques normées $\varphi_{\mathfrak{p}}$ d'un corps k de nombres algébriques est une conséquence de la relation (3), i. e. n'est satisfaite pour tout $\xi \in k^*$ que si $m_{\mathfrak{p}} = m$ pour tout p.

§ 5. — FONCTIONS ANALYTIQUES DANS LES CORPS COMPLETS

1) Séries entières

Nous avons déjà donné quelques propriétés de ces séries dans un corps valué complet k (pour une valuation v; cf. § 1, 2) de ce chapitre et chapitre premier, § 3, 4). Comme nous l'avons vu, la série $\sum_{n=1}^{\infty} a_n$ converge dans le corps k si et seulement si $a_n \to 0$ pour $n \to \infty$; on peut additionner et multiplier terme à terme les séries convergentes ou les multiplier par un facteur constant. On sait de plus que la convergence et la somme d'une série ne changent pas par modification de l'ordre des termes. Il en résulte facilement que si les produits $a_i b$ des termes de deux séries convergentes

$$\sum_{i=1}^{\infty} a_i = S \qquad \text{et} \qquad \sum_{j=}^{\infty} b_j = t$$

sont regroupés et organisés en une série, alors cette série est convergente et sa somme est égale à st.

Donnons un théorème simple sur les séries doubles. Rappelons qu'une série double

$$\sum_{i,j=1}^{\infty} a_{ij} \tag{1}$$

est dite convergente, de somme s, si $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} \to s$ pour $m, n \to \infty$. Les séries

$$\sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} a_{ij} \right), \qquad \sum_{j=1}^{\infty} \left(\sum_{i=1}^{\infty} a_{ij} \right)$$

sont appelées les séries itérées de la série double (1).

THÉORÈME 1. — *Si pour tout N, nous avons* $\nu(a_{ij}) > N$ *pour presque tout (i, j), alors la série double* (1) *est convergente et sa somme est égale aux sommes des deux séries itérées, qui sont également convergentes. Si à partir des termes de la série double* (1) *on constitue par un moyen quelconque une série* (simple), *alors cette série est aussi convergente de même somme.*

Nous laissons au lecteur la démonstration de ce théorème.

Une série entière dans le corps k est une série de la forme

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + \ldots + a_n x^n + \ldots \qquad (2)$$

où $a_n \in k$. Si la série (2) converge pour $x = x_0 \in k$, elle converge aussi pour tout $x \in k$ tel que $v(x) \geqslant v(x_0)$. En effet, pour de tels x, nous avons

$$v(a_n x^n) \geqslant v(a_n x_0^n),$$

et par suite le terme général $a_n x^n$ tend vers 0 avec $a_n x_0^n$ pour $n \to \infty$. Ainsi, si nous posons $\mu = \min v(x)$ où x parcourt les valeurs de k pour lesquelles la série (2) converge, le domaine de convergence de cette série est caractérisé par la condition $v(x) \geqslant \mu$ (ou bien cette série ne converge pour aucun x).

Considérons deux séries entières $f_1(x) = \sum_{n=0}^{\infty} a_n x^n$ et $f_2(x) = \sum_{n=0}^{\infty} b_n x^n$; par définition, leur produit h(x) est la série entière obtenue par multiplication formelle des séries données, i. e. la série $\sum_{n=0}^{\infty} c_n x^n$, avec $c_n = \sum_{i+j=n} a_i b_j$. Supposons que les séries $f_1(x)$ et $f_2(x)$ convergent respectivement pour $v(x) \geqslant \mu_1$ et $v(x) \geqslant \mu_2$; il est clair qu'alors h(x) converge pour $v(x) \geqslant \max(\mu_1, \mu_2)$ et que sa somme est égale dans ce cas à $f_1(x) f_2(x)$.

Une série entière $f(x)$ est une fonction continue de x dans son domaine de convergence. En effet, tous les termes $a_n x^n$ pour $n \geqslant 1$ sont arbitrairement petits pourvu que la valeur de x soit assez petite. Il en résulte que

$$f(x) \to a_0 = f(0) \qquad \text{pour} \qquad x \to 0,$$

i. e. la fonction f(x) est continue au point x = 0. Soit maintenant c une valeur quelconque du domaine de convergence de la série $f(x)$. Remplaçons chaque terme $a_n x^n$ par l'expression $a_n(c + y>$". Développant chacune de ces parenthèses et faisant la somme des polynômes obtenus, nous obtenons une série entière $f_c(y)$. Nous avons donc la formule

$$f(c + Y) = f_c(y) \qquad (3)$$

valable pour tout y appartenant au domaine de convergence de la série $f(x)$. D'après ce qui précède, $f_c(y) \to f_c(0)$ pour $y \to 0$ et par suite $f(x) \to f(c)$ pour $x \to c$ et la continuité de $f(x)$ est démontrée.

Une fonction $f(x)$, définie dans un certain domaine d'un corps valué complet et représentable dans ce domaine comme somme d'une série entière convergente est appelée /une ***fonction analytique.*** Considérons une série entière

$$g(y) = b_1 y + \ldots + b_n y^n + \ldots$$

sans terme constant. Le résultat de la substitution formelle de la série g(y) dans la série $f(x)$ (à la place de x), est une série entière F(y) de y. Posant

$$a_n g(y)^n = c_{nn} y^n + c_{n,n+1} y^{n+1} + \ldots \qquad (4)$$

nous aurons

$$F(y) = a_0 + c_{11} y + (c_{12} + c_{21}) y^2 + \ldots + (c_{1n} + c_{2n} + \ldots + c_{nn} y^n) + \ldots$$

THÉORÈME 2 (sur la substitution d'une série dans une autre) (*). — *Soit $f(x)$ une série entière convergente pour $v(x) \geqslant \mu$. Avec les notations ci-dessus, si la série $g(y)$ converge pour un certain y et $v(b_m y^m) \geqslant \mu$ pour tout $m \geqslant 1$, alors la série* F(y) *est convergente et*

$$F(y) = f(g(y)).$$

DÉMONSTRATION. — Considérons la série double

$$\sum_{i,j} c_{ij} y^j; \qquad (5)$$

d'après (4), nous avons

$$c_{nm} y^m = \sum_{\substack{\alpha_1, \ldots, \alpha_n \geqslant 1 \\ \alpha_1 + \ldots + \alpha_n = m}} a_n b_{\alpha_1} y^{\alpha_1} \ldots b_{\alpha_n} y^{\alpha_n}.$$

Posons $N = \min_m v(b_m y^m)$. Alors

$$v(c_{nm} y^m) \geqslant \min_{\alpha_1, \ldots, \alpha_n} \left(v(a_n b_{\alpha_1} y^{\alpha_1} \ldots b_{\alpha_n} y^{\alpha_n}) \right) \geqslant v(a_n) + nN.$$

Puisque $N = v(x_0)$ pour un certain x_0 et puisque la série $f(x)$ est convergente pour $x = x_0$, alors $v(a_n) + nN = v(a_n x_0^n) \to \infty$;par suite $v(c_{nm} y^m) \to \infty$

(*) Ce théorème a été formulé par D. K. Faddeev.

pour $n \to \infty$, uniformément en m. De plus, pour n fixé, la série (4) est convergente (comme produit de séries convergentes). Par suite, $\nu(c_{nm}y^m) \to \infty$ pour $m \to \infty$. Ceci démontre que la série (5) satisfait aux hypothèses du théorème. D'après ce théorème, les deux séries itérées de (5) convergent et ont la même somme. Il reste à constater que

$$F(y) = a_0 + \sum_j \left(\sum_i c_{ij} y^j\right) \qquad \text{et} \qquad f(g(y)) = a_0 + \sum_i \left(\sum_j c_{ij} y^j\right),$$

et le théorème 2 est démontré.

Dans les deux paragraphes suivants, nous considérerons des fonctions analytiques à n variables i. e. des fonctions représentables comme somme de séries entières

$$f(x_1, \ldots, x_n) = \sum_{\alpha_1, \ldots, \alpha_n \geqslant 0} a_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Supposons que la série $f(x_1, \ldots, x_n)$ converge dans le domaine n dimensionnel $\nu(x_i) \geqslant N$ $(i = 1, \ldots, n)$. Si c = $(c_1, \ldots, c_n)$ est un point de ce domaine, alors, par analogie avec le cas d'une variable (en appliquant le théorème 1), on obtient facilement l'identité

$$f(x_1 + c_1, \ldots, x_n + c_n) = f_c(x_1, \ldots, x_n)$$

valable pour tous les points du domaine $\nu(x_i) \geqslant N$ (dans cette identité, la série entière f(c) est aussi convergente pour $\nu(x_i) \geqslant N$).

2) Fonctions exponentielle et logarithmique

Nous supposerons dans ce point que k est une extension finie du corps $\mathbf{Q}_p$ des nombres p-adiques. Nous désignerons par ν la valuation du corps k, par e l'indice de ramification de k par rapport à $\mathbf{Q}_p$ et par π un élément premier de l'anneau des éléments entiers dans k. Considérons, dans le corps k, les séries entières

$$\exp x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} + \ldots \tag{6}$$

$$\operatorname{Log}(1 + x) = x - \frac{x^2}{2} + \ldots + (-1)^{n-1} \frac{x^n}{n} \tag{7}$$

Étudions le domaine de convergence de la série (6). Puisque le nombre premier p figure dans $n!$ avec l'exposant $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots$, alors

$$\nu(n!) = e\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots\right) < en \sum_{k=1}^{\infty} \frac{1}{p^k} = \frac{en}{p-1};$$

par suite

$$v\left(\frac{x^n}{n!}\right) = nv(x) - v(n!) > n\left(v(x) - \frac{e}{p-1}\right). \tag{8}$$

Si nous supposons $v(x) > \frac{e}{p-1}$, alors $v\left(\frac{x^n}{n!}\right) \to \infty$ pour $n \to \infty$ et la série (6) est convergente. D'autre part, pour $v(x) \leqslant \frac{e}{p-1}$ et pour $n = p^s$ nous avons

$$v\left(\frac{x^n}{n!}\right) = nv(x) - e(p^{s-1} + \ldots + p + 1) = nv(x) - e\frac{n-1}{p-1}$$
$$= n\left(v(x) - \frac{e}{p-1}\right) + \frac{e}{p-1} \leqslant \frac{e}{p-1};$$

cela signifie que, pour un tel x, le terme général de la série (6) ne tend pas vers 0. Nous avons ainsi démontré que la série (6) est convergente si et seulement si $x \geqslant \varkappa$, avec

$$\varkappa = \left[\frac{e}{p-1}\right] + 1.$$

La multiplication formelle des séries exp x et exp y donne la série exp (x + y) ; par suite, pour $v(x) \geqslant \varkappa$ et $v(y) \geqslant \varkappa$, nous avons la formule

$$\exp(x + y) = \exp x . \exp y. \tag{9}$$

Revenons maintenant à la série (7). Si $v(x) \leqslant 0$, alors $v\frac{x^n}{0^n}$ ne tend pas vers l'infini pour $n \to \infty$ et par suite la série (7) ne converge pas pour un tel x. Supposons maintenant $v(x) \geqslant 1$; si $n = p^a n_1$ $((n_1, p) = 1)$, alors $p^a \leqslant n$ et

$$v(n) = eu \leqslant e\frac{\operatorname{Log} n}{\operatorname{Log} p},$$

d'où

$$v\frac{x^n}{0^n} = nv(x) - v(n) \geqslant nv(x) - e\frac{\operatorname{Log} n}{\operatorname{Log} p},$$

et par suite $v\frac{x^n}{0^n} \to \infty$ pour $n \to \infty$. Ainsi, la série (7) converge si et seulement si $v(x) \geqslant 1$.

Si $v(x) \geqslant 1$, l'élément $\varepsilon = 1 + x$ est une unité dans l'anneau $\mathfrak{O}$ des éléments entiers du corps k. Par suite $\varepsilon \equiv 1 \pmod{x}$. Réciproquement, si une unité ε satisfait à cette dernière congruence, alors elle est de la forme $1 + x$ avec $v(x) \geqslant 1$. Une telle unité de l'anneau $\mathfrak{O}$ s'appelle une *unité principale* du corps k. La série (7) définit ainsi une fonction Log ε sur le groupe multi-

plicatif de toutes les unités principales du corps k. Montrons que pour deux unités principales ε_1 et ε_2 on a la formule

$$\text{Log } \varepsilon_1\varepsilon_2 = \text{Log } \varepsilon_1 + \text{Log } \varepsilon_2. \tag{10}$$

Soient $\varepsilon_1 = 1 + x$, $\varepsilon_2 = 1 + y$ et supposons $v(y) \geqslant v(x)$, i. e. $y = tx$ pour un certain entier t, d'où

$$(1 + x)(1 + y) = 1 + (t + 1)x + tx^2.$$

Nous considérerons l'expression $(t + 1)x + tx^2$ comme une série entière en x dont tous les éléments appartiennent au domaine de convergence de la série Log (1 + z). Puisque la substitution formelle de cette expression dans la série Log (1 + z) donne Log (1 + x) + Log (1 + tx), alors, d'après le théorème 2, nous obtenons l'égalité

$$\text{Log } (1 + (t + 1)x + tx^2) = \text{Log } (1 + x) + \text{Log } (1 + tx),$$

ce qui démontre la formule (10).

La substitution formelle de la série (7) dans la série (6), ou de la série exp $(x - 1)$ dans la série (7) donne les identités formelles suivantes

$$\exp(\text{Log } (1 + x)) = 1 + x, \tag{11}$$

$$\text{Log } (\exp x) = x. \tag{12}$$

Pour expliquer dans quelles conditions on peut considérer les identités (11) et (12) comme des égalités dans le corps k, utilisons le théorème 2. En accord avec ce théorème, l'égalité (11) sera vraie si tous les termes de la série 1 + x satisfont à la condition $v\frac{x^n}{0n} \geqslant x$. Pour n = 1, cela nous donne la condition $v(x) \geqslant x$. Mais si $v(x) \geqslant x$, alors $v\frac{x^n}{0n} = nx \geqslant x$ pour $1 \leqslant n \leqslant p - 1$ et

$$v\left(\frac{x^n}{n}\right) - x \geqslant (n - 1)x - v(n) > (n - 1)\frac{e}{p - 1} - e\frac{\text{Log } n}{\text{Log } p}$$

$$\frac{e(n - 1)}{\text{Log } p}\left(\frac{\text{Log } p}{p - 1} - \frac{\text{Log } n}{n}\right) \geqslant 0$$

pour $n \geqslant p \geqslant 2$ (nous avons utilisé ici le fait que la fonction $\frac{\text{Log } t}{t - 1}$ est monotone pour $t \geqslant 2$). Ainsi, l'égalité (11) est vraie pour la condition $v(x) \geqslant x$. On voit aussi que, sous cette même condition, $v(\text{Log } (1 + x)) \geqslant x$. Passons à la formule (12). Il résulte de (8) que pour $v(x) \geqslant x$ tous les termes de la série exp (x - 1) appartiennent au domaine de convergence de la série Log (1 + x); par suite la formule (12) est valable pour tout x tel que exp x ait un sens.

Désignons par A le groupe additif des éléments $x \in k$ tels que $v(x) \geqslant \varkappa$ et par M le groupe multiplicatif des unités $\varepsilon = 1 + x$, $x \in A$. D'après ce qui précède, l'application $\varepsilon \to \operatorname{Log}_E \varepsilon$, $\varepsilon \in M$ est un homomorphisme du groupe M dans le groupe A. Montrons que l'application $x \to \exp x$ est un homomorphisme de A dans M. D'après (9), il suffit de vérifier que

$$v\left(\frac{x^n}{n!}\right) \geqslant \varkappa$$

pour tout $x \in A$ et tout $n \geqslant 1$. Soit $p^s \leqslant n < p^{s+1}$. Alors

$$v\left(\frac{x^n}{n!}\right) - \varkappa \geqslant (n-1)\varkappa - e\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^s}\right]\right)$$
$$\geqslant \frac{(n-1)e}{p-1} - \frac{en}{p^s}\frac{p^s-1}{p-1} \geqslant 0,$$

ce qu'il fallait démontrer. Les formules (11) et (12) montrent maintenant que les applications $\operatorname{Log} : M \to A$ et $\exp : A \to M$ sont bijectives et inverses l'une de l'autre. Nous avons démontré le théorème suivant.

THÉORÈME 3. — ***L'application*** $x \to \exp x$ ***est un isomorphisme du groupe additif de tous les nombres entiers du corps k divisibles par*** $\pi^{\varkappa}\left(\varkappa = \left[\frac{e}{p-1}\right] + 1\right)$ ***sur le groupe multiplicatif des unités principales*** $\varepsilon \equiv 1 \pmod{\pi^{\varkappa}}$. ***L'isomorphisme inverse est l'application*** $\varepsilon \to \operatorname{Log} \varepsilon$ ***(pour*** $\varepsilon \equiv 1 \pmod{\pi^{\varkappa}}$***).***

En général, l'application $\varepsilon \to \operatorname{Log} \varepsilon$ étendue ***à tout*** le groupe des unités principales n'est pas un isomorphisme (exercice 5). De plus, la valeur $\operatorname{Log} \varepsilon$ n'est pas forcément entière.

Dans l'analyse réelle, on considère, simultanément avec la fonction e^x, la fonction exponentielle $a^x = e^{x \operatorname{Log} a}$. Son analogue dans le corps k est la fonction

$$\eta^x = \exp(x \operatorname{Log} \eta) \tag{13}$$

où η est une unité principale du corps k. Cette fonction est définie pour la condition $v(x) \geqslant \varkappa - v(\operatorname{Log} \eta)$. Par suite, si $\eta \equiv 1 \pmod{\pi^{\varkappa}}$, alors η^x sera définie pour tout entier x de k et pour ces valeurs on a la congruence

$$\eta^x \equiv 1 \pmod{\pi^{\varkappa}}.$$

Dans le cas $\eta \equiv 1 \pmod{\pi^{\varkappa}}$, pour des entiers x, y quelconques du corps k on a les formules

$$\eta^{x+y} = \eta^x \eta^y,$$
$$(\eta^x)^y = \eta^{xy}.$$

EXERCICES

1. Démontrer qu'une fonction f(x) analytique pour $v(x) \geqslant \mu$ (dans un corps complet pour la valuation v) et admettant une infinité de zéros dans la région $v(x) \geqslant \mu$ est identiquement nulle.

2. Soit k un corps de caractéristique zéro complet pour une métrique non archimédienne φ (exercice 4 du chapitre Ier, § 4). Supposons que la métrique φ est telle que $\varphi(p) < 1$ pour un certain nombre premier rationnel p. Démontrer que la région de convergence de la série Log (1 + x) dans le corps k est définie par la condition $\varphi(x) < 1$ et la région de convergence de la série exp x par la condition $\varphi(x) < \sqrt[p-1]{\varphi(p)}$.

3. Sous les mêmes hypothèses, définir la région de convergence des séries

$$\sin x = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^{2n-1}}{(2n-1)!}, \qquad \cos x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}.$$

4. Trouver une erreur dans la démonstration suivante de l'irrationalité du nombre π. Le nombre π est le plus petit nombre > 0 tel que $\sin \pi = 0$. Supposons π rationnel. Puisque $\pi > 3$, alors son numérateur doit être divisible ou bien par un nombre premier impair p, ou bien par 2^2. Dans ce dernier cas posons $p = 2$. Il en résulte que les séries sin x et cos x convergent pour $x = \pi$ dans le corps des nombres p-adiques. Mais, d'après la formule

$$\sin (x + y) = \sin x \cos y + \cos x \sin y,$$

l'égalité $\sin \pi = 0$ entraîne $\sin n\pi = 0$ pour tout entier naturel n. La fonction sin x a ainsi une infinité de zéros dans sa région de convergence et par suite, d'après l'exercice 1, elle est identiquement nulle. Nous avons obtenu une contradiction.

5. Soient k une extension finie du corps $\mathbf{Q}_p$ des nombres p-adiques et ε une unité principale du corps k. Montrer que $\operatorname{Log} \varepsilon = 0$ si et seulement si ε est une racine d'ordre p^s $(s \geqslant 0)$ de 1.

6. Conservons toutes les notations du point 2). Il est clair que les unités principales ε qui sont congrues à 1 modulo π^n forment un groupe multiplicatif M_n. Tous les nombres entiers du corps k qui sont divisibles par π^n forment un groupe additif A_n. Montrer que pour $n \geqslant \varkappa$, l'application $\varepsilon \to \operatorname{Log} \varepsilon$, $\varepsilon \in M_n$, est un isomorphisme du groupe M_n sur le groupe A_n (l'isomorphisme inverse est l'application $x \to \exp x$, $x \in A_n$).

7. Démontrer que dans un corps valué complet, la région de convergence de la série entière $f(x) = \sum_{n=0}^{\infty} a_n x^n$ est contenue dans la région de convergence de la série dérivée $\sum_{n=0}^{\infty} n a_n x^{n-1}$. Montrer par un exemple que les régions de convergence des deux séries $f(x)$ et $f'(x)$ peuvent ne pas coïncider (même dans le cas d'un corps de caractéristique nulle).

8. Démontrer que dans l'anneau des nombres 2-entiers la somme

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots + \frac{2^n}{n}$$

est divisible par des puissances de 2 aussi grandes que l'on veut pourvu que n soit assez grand.

9. Démontrer que tous les coefficients a_n de la série

$$E_p(x) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \dots\right) = \sum_{n=}^{\infty} a_n x^n$$

sont des nombres rationnels p-entiers (p premier).

Indication. — Démontrer que le nombre

$$T_n = a_n n\,! = \sum_{\substack{p^{\alpha_1}+\dots+p^{\alpha_s}=n \\ \alpha_1 \geqslant 0, \dots, \alpha_s \geqslant 0}} \frac{n\,!}{s\,! p^{\alpha_1} p^{\alpha_2} \dots p^{\alpha_s}}$$

est égal au nombre d'éléments du $n^{\text{ième}}$ groupe symétrique dont l'ordre est une puissance de p et appliquer le théorème qui affirme que pour tout diviseur d de l'ordre d'un groupe fini G, le nombre des éléments $u \in G$ qui satisfont à l'équation $u^d = 1$ est divisible par d.

10. Démontrer que

$$E_p(x) = \prod_{(m,p)=1} (1 - x^m)^{\frac{\mu(m)}{m}}$$

(m parcourt tous les entiers naturels premiers avec p; $\mu(m)$ est la fonction de Moebius).

11. Soient η une unité principale d'une extension finie du corps des nombres p-adiques et x un nombre entier p-adique. Choisissons une suite d'entiers naturels $\{ a_n \}$ qui converge vers x. Démontrer que la limite $\lim_{n\to\infty} \eta^{a_n}$ existe et est indépendante du choix de $\{ a_n \}$. Montrer de plus que la fonction

$$\eta^x = \lim_{n\to\infty} \eta^{a_n}$$

coïncide avec la fonction (13) sur les nombres entiers p-adiques x.

§ 6. — MÉTHODE DE SKOLEM

Nous exposerons dans ce paragraphe la méthode, due à Skolem, de résolution des équations du type

$$F(x_1, \dots, x_m) = c, \tag{1}$$

où F est une forme irréductible décomposable incomplète (cf. chap. II, § 1, 3)) et c un nombre rationnel. Cette méthode repose sur quelques propriétés simples des ensembles analytiques sur les corps de nombres $\mathfrak{P}$-adiques, qui seront démontrés dans le paragraphe suivant. On a donné au début de ce chapitre un exemple introduisant l'idée de Skolem.

1) Représentation des nombres par des formes décomposables incomplètes

D'après le chapitre II, § 1, 3)), l'équation (1) peut s'écrire

$$N(x_1\mu_1 + \ldots + x_m\mu_m) = a \tag{2}$$

ou encore

$$N(\alpha) = a, \qquad \alpha \in M, \tag{3}$$

$\mu_1, \ldots, \mu_m$ étant des nombres d'un corps k de nombres algébriques et $M = \{\mu_1, \ldots, \mu_m\}$ le module engendré par ces nombres (a est un nombre rationnel). Remplaçant éventuellement la forme F par une forme à coefficients entiers équivalente, nous pouvons supposer que les générateurs $\mu_1, \ldots, \mu_m$ du module M sont linéairement indépendants sur le corps Q des nombres rationnels. Par hypothèse, le module M est incomplet, i. e.

$$m < n = (k : Q).$$

Au chapitre II, nous avons expliqué comment on peut trouver toutes les solutions de l'équation (3) dans le cas où M est un module complet du corps k. C'est pourquoi, pour résoudre l'équation (3), nous plongerons le module M dans un module complet $\overline{M}$; utilisant alors les méthodes du chapitre II, on trouvera toutes les solutions de l'équation $N(\alpha) = a$, $\alpha \in \overline{M}$ et il restera à choisir les solutions α qui appartiennent à M.

Il est évident qu'on peut plonger tout module de k dans un module complet. Il suffit de compléter le système des nombres linéairement indépendants $\mu_1, \ldots, \mu_m$ en une base $\mu_1, \ldots, \mu_n$ du corps k et poser

$$M = \{\mu_1, \ldots, \mu_m\}.$$

Si on a résolu l'équation $N(\alpha) = a$, $a \in \overline{M}$, on obtiendra toutes les solutions de l'équation (3) en prenant les solutions $\alpha \in M$ pour lesquelles, dans la représentation

$$\alpha = x_1\mu_1 + \ldots + x_n\mu_n,$$

les coefficients $x_{m+1}, \ldots, x_n$ sont nuls. Soit $\mu_1^*, \ldots, \mu_n^*$ la base duale de la base $\mu_1, \ldots, \mu_n$ (cf. appendice § 2, 3)). Puisque la trace $\mathrm{Tr}\ \mu_j\mu_j^*$ est égale à 0 pour $i \neq j$ et à 1 pour $i = j$, alors $x = \mathrm{Tr}\ a\mu_i^*$ $(1 \leqslant i \leqslant n)$. Il en résulte que les nombres $\alpha \in \overline{M}$ qui appartiennent au sous-module M sont caractérisés par les conditions

$$\mathrm{Tr}\ \alpha\mu_i^* = 0 \qquad (i = m+1, \ldots, n). \tag{4}$$

D'après le théorème 1 du chapitre II, § 5, les solutions de l'équation N(a) = a, a $\in \overline{\mathbf{M}}$ sont de la forme

$$\mathbf{a} = \gamma_j \varepsilon_1^{u_1} \dots \varepsilon_n^{u_n} \qquad (1 \leqslant j \leqslant k), \tag{5}$$

où $\gamma_1, \dots, \gamma_k$ est un système fini de nombres de norme a du module $\overline{\mathbf{M}}$ et $\varepsilon_1, \dots, \varepsilon$, un système d'unités indépendantes du corps k; $u_1, \dots, u_r$ sont des nombres entiers rationnels quelconques. D'après (4), la résolution de l'équation (3) est équivalente à la résolution de k systèmes d'équations

$$\operatorname{Tr}\left(\gamma \mu_i^* \varepsilon_1^{u_1} \dots \varepsilon_r^{u_r}\right) = 0 \qquad (i = m+1, \dots, n), \tag{6}$$

par rapport aux entiers rationnels $u_1, \dots, u_r$ (ici γ est un des γ_j).

Soit K un corps de nombres algébriques contenant tous les corps conjugués de k et soient $\sigma_1, \dots, \sigma_n$ tous les isomorphismes de k dans K. Puisque

$$\operatorname{Tr}(\xi) = \sigma_1(\xi) + \dots + \sigma_n(\xi)$$

pour tout $\xi \in k$, le système (6) peut s'écrire :

$$\sum_{j=1}^{n} \sigma_j(\gamma \mu_i^*) \sigma_j(\varepsilon_1)^{u_1} \dots \sigma_j(\varepsilon_r)^{u_r} = 0 \qquad (i = m+1, \dots, n). \tag{7}$$

Il est clair que pour démontrer que l'équation (3) a un nombre fini de solutions, il suffit de montrer que chacun des systèmes (7) a seulement un nombre fini de solutions $u_1, \dots, u_r$ entiers rationnels.

Remarque. — Nous appellerons sous-groupe multiplicatif du corps k l'ensemble des nombres du corps k qui s'écrivent sous la forme $\varepsilon_1^{u_1} \dots \varepsilon_r^{u_r}$, où $u_1, \dots, u_2$ parcourent tous les entiers rationnels et nous le désignerons par U. Toutes les solutions de l'équation (3) coïncident avec les éléments des intersections

$$\mathbf{M} \cap \gamma_j \mathbf{U} \qquad (j = 1, \dots, k). \tag{8}$$

On peut remplacer chacun des ensembles (8) par l'ensemble $\gamma_j^{-1}\mathbf{M} \cap \mathbf{U}$ qui lui est semblable. Ainsi, le problème de la recherche des solutions de l'équation (1) équivaut au problème de l'intersection d'un module et du sous-groupe multiplicatif du corps k. Remarquons que dans les intersections (8) on peut remplacer le module M par l'espace vectoriel L (sur le corps Q) engendré par $\mu_1, \dots, \mu_m$. En effet, puisque $\gamma_j \mathbf{U} \subset \overline{\mathbf{M}}$ et $\mathrm{L} \cap \mathrm{M} = \mathrm{M}$, alors $\mathrm{L} \cap \gamma_j \mathbf{U} = \mathrm{M} \cap \gamma_j \mathbf{U}$.

2) Lien avec les germes d'ensembles analytiques

L'idée de la méthode de Skolem réside dans le fait que, dans certains cas, on peut démontrer la finitude du nombre de solutions, de l'équation (1) en montrant que le système (7) n'a déjà qu'un nombre fini de solutions $u_1, \ldots, u_r$ qui soient des nombres entiers $\mathfrak{P}$-adiques (i. e. des Cléments entiers du complété $\mathbf{K}_\mathfrak{P}$), $\mathfrak{P}$ étant un certain diviseur premier du corps K. Pour une extension convenable de l'ensemble dans lequel varient les inconnues, nous pourrons interpréter l'ensemble des solutions du système (7) comme un ensemble analytique dans un espace r-dimensionne1 et pour l'étudier appliquer les propriétés de ces ensembles.

Pour donner des valeurs $\mathfrak{P}$-adiques aux variables $u_1, \ldots, u_r$ dans les parties gauches des équations (7), nous nous heurtons à la difficulté suivante : la fonction exponentielle $\varepsilon^u = \exp(u \operatorname{Log} \varepsilon)$ n'est défini pour tout entier $\mathfrak{P}$-adique u que si ε satisfait à la congruence $\varepsilon \equiv 1 \pmod{\mathfrak{P}^\varkappa}$ ($\varkappa$ est un nombre entier qui dépend seulement du corps $\mathbf{K}_\mathfrak{P}$; cf. fin du § 5). On peut surmonter ainsi cette difficulté : d'après l'exercice 6 du chapitre III, § 7, il existe un entier naturel q tel que pour tout nombre entier $\alpha \in K$ non divisible par $\mathfrak{P}$, on ait la congruence

$$\alpha^q \equiv 1 \pmod{\mathfrak{P}^\varkappa}. \tag{9}$$

Dans la formule (5), on peut écrire chacun des exposants u sous la forme

$$u_i = \rho_i + qv_i, \qquad 0 \leqslant \rho_i < q, \qquad v_i \in \mathbf{Z},$$

et, par suite, l'unité $\varepsilon = \varepsilon_1^{u_1} \ldots \varepsilon_r^{u_r}$ s'écrit aussi

$$\varepsilon = \delta_l \varepsilon_1^{qv_1} \ldots \varepsilon_r^{qv_r} \qquad (l = 1, \ldots, q^r)$$

où δ est un des q^r nombres

$$\varepsilon_1^{\rho_1} \ldots \varepsilon_r^{\rho_r}, \qquad 0 \leqslant \rho_i < q.$$

Nous obtenons ainsi une nouvelle représentation des nombres α du type (5) dans laquelle ε_i est remplacé par ε_i^q et l'ensemble fini des nombres γ_j est remplacé par l'ensemble fini des nombres $\gamma_j \delta_l$. Puisque les ε_i sont des unités, ces nombres et les nombres $\sigma_j(\varepsilon_i)$ vérifient la congruence (9) et la fonction $\sigma_j(\varepsilon_i^q)^u$ est définie pour tout entier $\mathfrak{P}$-adique $u \in \mathbf{K}_\mathfrak{P}$. Nous avons démontré le résultat suivant.

LEMME 1. — ***Pour un choix convenable des y et ε_i dans la formule (5), les fonctions $\sigma_j(\varepsilon_i)^u$ sont définies pour tous les nombres entiers u du corps $\mathbf{K}_\mathfrak{P}$.***

Nous supposerons toujours dans la suite que cette condition est satisfaite.

Revenons au système d'équations (7). Utilisant les formules (9) et (13) du § 5, ces équations peuvent s'écrire

$$\sum_{j=1}^{n} A_{ij} \exp L_j(u_1, \ldots, u_r) = 0 \qquad (i = m+1, \ldots, n) \tag{10}$$

avec

$$L_j(u_1, \ldots, u_r) = \sum_{k=1}^{r} u_k \operatorname{Log} \sigma_j(\varepsilon_k),$$

$$A_{ij} = \sigma_j(\gamma\mu_i^*).$$

Puisque les parties gauches des équations (10) s'expriment comme des séries entières convergentes pour tous les entiers $\mathfrak{P}$-adiques $u_1, \ldots, u_r$ et par suite sont des fonctions analytiques, on peut interpréter l'ensemble des solutions du système (10) comme un germe d'ensemble analytique (au voisinage de toute solution) au sens de la définition du § 7.

Le nombre des inconnues du système (10) est égal à r et le nombre des équations est égal à $n - m$. On s'attend intuitivement à ce que la variété définie par ce système soit formée d'un nombre fini de points isolés si $n - m \geqslant$ Y. Rappelons que le nombre r, lié au théorème de Dirichlet sur les unités, est égal à $s + t - 1$, s étant le nombre d'isomorphismes réels et t le nombre de paires d'isomorphismes complexes conjugués du corps k. Puisque $n = s + 2t$, la condition $n - m \geqslant r$ équivaut à la condition $t \geqslant m - 1$. Dans le cas très simple $m = 2$, cette condition signifie que $t \geqslant 1$, i. e. qu'il existe au moins une paire de corps complexes conjugués à k. Ce cas, réduit au théorème de Thue, sera étudié dans le point suivant.

Supposons que le système (10) ait une infinité de solutions $(u_{1s}, \ldots, u_{rs})$, $s = 1, 2, \ldots$ D'après la compacité de l'anneau des nombres entiers $\mathfrak{P}$-adiques (cf. théorème 6 du chapitre premier, § 3 et remarque 2 à la fin du § 1, 2) de ce chapitre), on peut en extraire une sous-suite convergente dont nous désignerons la limite par $u_1^*, \ldots, u_r^*$. Il est clair que le point $(u_1^*, \ldots, u_r^*)$ satisfait aussi au système (10); par suite, c'est un point de l'ensemble analytique défini par ces équations, qui possède la propriété que chacun de ses voisinages contient une infinité de points de cette variété. Introduisons à la place de $u_1, \ldots, u_r$ de nouvelles variables $v_1, \ldots, v_r$ par les formules

$$u_i = u_i^* + v_i \qquad (1 \leqslant i \leqslant \text{Y}).$$

Le système (10) s'écrit

$$\sum_{j=1}^{n} A_{ij}^* \exp L_j(v_1, \ldots, v_r) = 0 \qquad (i = m+1, \ldots, n) \tag{11}$$

en posant

$$A_{ij}^* = A_{ij} \exp L_j(u_1^*, \ldots, u_r^*).$$

Les termes constants des séries qui figurent dans la partie gauche des équations (11) sont nuls. Désignons par V le germe d'ensemble analytique (au voisinage du point $(0, \ldots, 0)$) défini par le système (11) (cf. définition du § 7). Puisque ce germe n'est pas réduit à un point (tout voisinage de l'origine contient par hypothèse une infinité de points de cet ensemble), alors, d'après le théorème 2 du § 7, il existe sur V une courbe analytique, i. e. il existe un système de séries entières formelles

$$\omega_1(t), \ldots, \omega_r(t)$$

(non nulles simultanément et sans termes constants), à coefficients dans une extension finie du corps $K_{\mathfrak{P}}$, telle que les séries

$$P_j(t) = L_j(\omega_1(t), \ldots, \omega_r(t)) \tag{12}$$

satisfassent identiquement aux relations

$$\sum_{j=1}^{n} A_{ij}^* \exp P_j(t) = 0 \qquad (i = m+1, \ldots, n).$$

Nous avons obtenu le résultat suivant :

THÉORÈME 1. — ***Si l'équation (1) admet une infinité de solutions, le germe d'ensemble analytique défini par le système*** (11) (pour un certain $y = \gamma_j$ et un certain point $(u_1^*, \ldots, u_r^*)$) ***contient une courbe analytique.***

Ce théorème est l'étape fondamentale de la méthode de Skolem. 11 réduit la démonstration de la finitude du nombre de solutions de l'équation (1) à la démonstration du fait que le système (11) n'a pas de solutions dans les séries entières formelles à une variable, i. e. que le germe analytique correspondant ne contient pas de courbe analytique.

Remarquons que, parmi les n séries $P_j(t)$ définies par les égalités (12), il existe $n - r$ relations linéaires

$$\sum_{j=1}^{n} B_{ij} P_j(t) = 0, \qquad 1 \leqslant j \leqslant n - r,$$

puisque ce sont des combinaisons linéaires des r séries entières $w_k(t)$. Ainsi, la présence sur le germe V d'une courbe analytique implique que le système

$$\left.\begin{aligned} \sum_{j=1}^{n} A_{ij}^* \exp P_j(t) &= 0 \qquad (m+1 \leqslant i \leqslant n) \\ \sum_{i=1}^{n} B_{ij} P_j(t) &= 0 \qquad (1 \leqslant i \leqslant n - r = t+1) \end{aligned}\right\} \tag{13}$$

est résoluble (dans les séries entières formelles Pi(t) sans terme constant); les équations des première et deuxième lignes sont ici respectivement linéairement indépendantes (l'indépendance des équations de la première ligne résulte du fait que le déterminant det $\sigma_j(\gamma\mu_i^*)$, dont le carré est égal au discriminant de la base $\gamma\mu_i^*$, est différent de zéro puisque le rang de la matrice (A_{ij}) $(m+1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ et par suite aussi de la matrice (A_{ij}^*), est égal à m — n). Si nous supposons que $n - m \geqslant r$, alors le nombre des équations du système (13) est $\geqslant n$.

3) Théorème de Thue

Ce théorème affirme que si une forme

$$f(x, y) = a_0x^n + a_1x^{n-1}y + \ldots + a_ny^n$$

de deux variables, à coefficients entiers rationnels, est irréductible et de degré $n \geqslant 3$, alors l'équation

$$f(x, Y) = c \tag{14}$$

n'admet qu'un nombre fini de solutions dans les nombres entiers. Puisqu'une forme de deux variables est toujours décomposable, et incomplète pour $n > 2$, l'équation (14) est une équation du type (1) que nous avons étudié. Ici $m = 2$; la condition $t \geqslant m - 1$, sur laquelle repose la méthode de Skolem, signifie donc que $t \geqslant 1$, i. e. que l'équation $f(x, 1) = 0$ a au moins une racine complexe. On dit dans ce cas que la forme $f(x, y)$ admet une racine complexe. Sous cette hypothèse, nous démontrerons le théorème de Thue par la méthode de Skolem, i. e. l'argument suivant :

THÉORÈME 2. — ***Si la forme irréductible à coefficients entiers $f(x, y)$ de degré $n \geqslant 3$ admet au moins une racine complexe, alors l'équation***

$$f(x, Y) = c$$

n'admet qu'un nombre fini de solutions en nombres entiers.

DÉMONSTRATION. — Nous supposerons que le coefficient a, de x^n dans $f(x, y)$ est égal à 1 (sinon, nous multiplierons l'équation (14) par a_0^{n-1} et remplacerons a_0x par x). Posons $k = Q(O)$, $K = Q(\theta_1, \ldots, 0,)$ où les nombres $\theta = \theta_1, \theta_2, \ldots, \theta_n$ sont définis par la décomposition

$$f(x, 1) = (x + \theta_1) \ldots (x + \theta_n).$$

Pourtoutj= 1, ... *n,* désignons par σ_j l'isomorphisme du corps k dans K tel que $\theta \to \theta_j$. Puisquef(x, y) = $N(x + y\theta)$ (N est la norme pour l'extension k/Q), nous pouvons écrire l'équation (14) sous la forme (3), M étant le module { 1, θ }. Ainsi, dans ce cas, $\mu_1 = 1$, $\mu_2 = \theta$ ($m = 2$).

Supposons que l'équation (3) pour le module M = { 1, θ } admette une infinité de solutions a = x + $y\theta$. Alors, pour un certain y = $\gamma_j \in k$, une infinité de ces solutions s'écrivent sous la forme (5) pour des unités indépendantes $\varepsilon_1, \ldots, \varepsilon_r$ du corps k, qui satisfont aux hypothèses du lemme 1. Les exposants $u_1, \ldots, u_r$ correspondant à ces nombres a satisfont au système (10). Choisissons parmi ces solutions a une suite $\alpha_1, \alpha_2, \ldots$, telle que les points correspondants

$$(u_{1s}, \ldots, u_{rs}), \qquad s = 1, 2, \ldots \tag{15}$$

convergent vers un certain point $u_1^*, \ldots, u_r^*$. D'après le point 2), le germe d'ensemble analytique défini par le système (11) contient une courbe analytique $\omega_1(t), \ldots, w_r(t)$, i. e. les séries (12) correspondantes satisfont aux équations (13).

La démonstration du théorème 2 repose sur l'important lemme suivant :

LEMME 2. — *Soit donné le système d'équations*

$$\left.\begin{aligned} \sum_{j=1}^{n} a_{ij} \exp P_j &= 0 \qquad (i = 1, \ldots, n_1) \\ \sum_{j=1}^{n} b_{ij} P_j &= 0 \qquad (i = 1, \ldots, n_2) \end{aligned}\right\} \tag{16}$$

dans lequel les équations de la première et de la seconde ligne sont respectivement linéairement indépendantes. Si $n_1 = n - 2$, $n_2 \geqslant 2$ et si le système a une solution $P_1(t), \ldots, P_n(t)$ dans les séries entières formelles sans terme constant, alors $P_k(t) = P_j(t)$ pour au moins deux indices k et j distincts (Les coefficients a_{ij} et b_{ij}, de même que les coefficients des séries entières $P_j(t)$, appartiennent à un corps de caractéristique 0).

Nous donnerons plus loin la démonstration de ce lemme. Montrons tout de suite qu'il entraîne le théorème 2.

D'après le lemme 2, pour toute courbe $\omega_1(t), \ldots, \omega_r(t)$ de V il existe au moins deux indices distincts k et j tels que $P_k(t) = P_j(t)$, i. e.

$$L_k(\omega_1(t) \ldots, \omega_r(t)) = L_j(\omega_1(t), \ldots, \omega_r(t)). \tag{17}$$

Considérons dans l'espace r-dimensionne1 des points $(v_1, \ldots, v_r)$ l'ensemble analytique W défini par l'équation

$$\prod_{1 \leqslant k < j \leqslant n} (L_k(v_1, \ldots, v_r) - L_j(v_1, \ldots, v_r)) = 0.$$

Il résulte de (17) que toute courbe contenue dans le germe analytique V appartient aussi à W. Mais alors, d'après le théorème 3 du § 7, V ⊂ W,

i. e. tous les points de V contenus dans un voisinage assez petit de l'origine appartiennent aussi à W.

D'autre part, montrons que W contient seulement un nombre fini des points $(v_{1s}, \ldots, v_{sr}) \in \mathbf{V}$, $s = 1, 2, \ldots$) liés aux points (15) par la relation $u_{is} = u_i^* + v_{is}$, qui convergent vers l'origine. La contradiction obtenue démontre le théorème 2.

Soient $\alpha = x + y\theta$ et $\alpha' = x' + y'\theta$ deux nombres de la suite $\{\alpha_s\}$ tels que les points correspondants de V appartiennent à l'ensemble analytique $\mathbf{L}_k = \mathbf{L}_j$. Si $a = \gamma\varepsilon_1^{u_1} \ldots \varepsilon_r^{u_r}$ et $u_i = u_i^* + v_i$, alors

$$\sigma_j(\alpha) = \sigma_j(\gamma)\,\sigma_j(\varepsilon_1)^{u_1^*} \ldots \sigma_j(\varepsilon_r)^{u_r^*}\sigma_j(\varepsilon_1)^{v_1} \ldots \sigma_j(\varepsilon_r)^{v_r} = c_j \exp \mathbf{L}_j(v_1, \ldots, v_r)$$

et, de manière analogue,

$$\sigma_k(\alpha) = c_k \exp.\ \mathbf{L}_k(v_1 \ldots, v),$$

d'où

$$\frac{\sigma_j(\alpha)}{c_j} = \frac{\sigma_k(\alpha)}{c_k}.$$

Nous obtiendrions de même

$$\frac{\sigma_j(\alpha')}{c_j} = \frac{\sigma_k(\alpha')}{c_k}$$

Ces deux égalités nous donnent

$$\frac{x + y\theta_j}{x' + y'\theta_j} = \frac{x + y\theta_k}{x' + y'\theta_k},$$

d'où

$$(xy' - x'y)(\theta_k - \theta_j) = 0,$$

et, puisque $\theta_j \neq \theta_k$, nous obtenons finalement

$$xy' - x'y = 0.$$

Cette dernière égalité exprime que $x + y\theta = d(x' + y'\theta)$ pour un certain nombre rationnel d. Prenant les normes et tenant compte du fait que

$$N(a) = N(a') = 1,$$

nous obtenons l'égalité $d^n = 1$, d'où $d = \pm 1$; par suite $a' = \pm a$.

Ainsi, chacun des $\frac{n(n-1)}{2}$ ensembles analytiques $\mathbf{L}_k = \mathbf{L}_j$, dont la réunion coïncide avec W, contient au plus deux points de V qui correspondent à des points de la suite $\{\alpha_s\}$. Mais alors W contient au plus $n(n-1)$ tels points. Ainsi tout voisinage de l'origine contient des points de V qui

n'appartiennent pas à W et cela signifie que V (comme germe analytique) ne peut pas être contenu dans W, en contradiction avec l'inclusion obtenue ci-dessus $V \subset W$. Comme nous l'avons dit, cela redémontre le théorème 2.

DÉMONSTRATION DU LEMME 2. — Puisque, par hypothèse, les équations de la première ligne de (16) sont linéairement indépendantes, nous pouvons (en modifiant éventuellement l'ordre des indices) exprimer $\exp \mathbf{P}_i$ ($i = 1, 2, \ldots, n-1$) au moyen de $\exp \mathbf{P}_{n-1}$ et $\exp \mathbf{P}_n$:

$$\exp \mathbf{P}_i = a_i \exp \mathbf{P}_{n-1} + b_i \exp \mathrm{P}_n. \tag{18}$$

Si $a_i = 0$, alors, égalant les termes constants dans l'égalité $\exp \mathbf{P}_i = b_i \exp \mathrm{P}_n$, nous obtenons $b_i = 1$, d'où $\mathbf{P}_i = \mathrm{P}_n$. Nous pouvons donc supposer que tous les a_i sont différents de zéro. Posons

$$\mathrm{P}_i - \mathrm{P}_n = \mathrm{Q}_i \qquad (i = 1, \ldots, n-1)$$

et supposons que tous les $\mathbf{Q}_i$ sont différents de zéro. L'égalité (18) donne

$$\exp \mathrm{Q}_i = a_i \exp \mathrm{Q}_{n-1} + b_i \tag{19}$$

d'où, en dérivant par rapport à t (cf. exercice 10),

$$\mathrm{Q}_i' \exp \mathrm{Q}_i = a_i \mathrm{Q}_{n-1}' \exp \mathrm{Q}_{n-1}. \tag{20}$$

Réunissant les égalités (19) et (20), nous obtenons

$$\mathrm{Q}_i' = \mathrm{Q}_{n-1}' \exp \mathrm{Q}_{n-1} \frac{1}{c_i + \exp \mathrm{Qn\text{-}1}} \qquad (\mathrm{i} = 1, \ldots, \mathrm{n}-2) \tag{21}$$

avec

$$c_i = b_i a_i^{-1}.$$

Étudions maintenant les équations de la deuxième ligne de (16). Par hypothèse, il en existe au moins deux qui sont linéairement indépendantes; mais alors, on peut trouver une relation non triviale entre $\mathrm{Q}_1, \ldots, \mathrm{Q}_{n-1}$:

$$\sum_{i=1}^{n} d_i \mathrm{Q}_i = 0.$$

Dérivant cette identité et remplaçant les Q_i' par les équations (21), nous obtenons

$$\mathrm{Q}_{n-1}' \exp \mathrm{Q}_{n-1} \left(\sum_{i=1}^{n-2} \frac{d_i}{c_i + \exp \mathrm{Q}_{n-1}} + \frac{d_{n-1}}{\exp \mathrm{Q}_{n-1}} \right) = 0,$$

et, puisque $\mathrm{Q}_{n-1}' \neq 0$ et $\exp \mathrm{Q}_{n-1} \neq 0$, alors

$$\sum_{i=1}^{n-1} \frac{d_i}{c_i + \exp \mathrm{Q}_{n-1}} = 0 \tag{22}$$

(en posant ici $c_{n-1} = 0$).

L'égalité (22) ne peut avoir lieu que si la fonction rationnelle

$$\sum_{i=1}^{n-1} \frac{d_i}{c_i + z} \tag{23}$$

est identiquement nulle. En effet, dans le cas contraire, i. e. si la fonction (23) est égale à $\frac{\varphi(z)}{\psi(z)}$ avec $\varphi(z) \neq 0$, alors, d'après l'égalité cp(exp Q_{n-1})=0, nous obtenons que la série entière formelle exp Q_{n-1}, non constante, est racine d'une équation algébrique, en contradiction avec l'exercice 4 du §1. Il est clair que la fonction (23) ne peut s'annuler identiquement que si $c_k = c_j$ pour au moins deux indices k et j distincts. Mais alors, il résulte des égalités (19) que

$$\exp P_k = \frac{a_k}{a_j} \exp P_j ;$$

on en déduit facilement que $P_k = P_j$, ce qui démontre le lemme 2.

Remarque. — La méthode de Skolem permet de démontrer la finitude du nombre de solutions entières de l'équation (14). Cependant, elle ne donne pas d'algorithme pour trouver ces solutions. Toutes les méthodes de démonstration connues présentent cet inconvénient.

4) Remarques sur les formes à un plus grand nombre de variables

En liaison avec le théorème de Thue il est naturel de se poser la question suivante : à quelles conditions une équation du type (1), pour une forme décomposable incomplète, a-t-elle seulement un nombre fini de solutions dans les nombres entiers. De telles équations peuvent, dans certains cas, avoir une infinité de solutions, Considérons, à titre d'exemple, l'équation

$$x^4 + 4y^4 + 9z^4 - 4x^2y^2 - 6x^2z^2 - 12y^2z^2 = N(x + y\sqrt{2} + z\sqrt{3}) = 1$$

(la norme est prise pour l'extension $Q(\sqrt{2}, \sqrt{3})/\mathbf{Q}$). Cette équation admet deux séries infinies de solutions données par les formules

$$x + y\sqrt{2} = \pm(1 + \sqrt{2})^n, \qquad z = 0 ;$$
$$x + z\sqrt{3} = \pm(2 + \sqrt{3})^n, \qquad y = 0.$$

La raison de ce phénomène est que, si nous posons z = 0 ou y = 0, nous obtenons des carrés parfaits $(x^2 - 2y^2)^2$ et $(x^2 - 3z^2)^2$ respectivement. Cela

entraîne que le module $\{1, \sqrt{2}, \sqrt{3}\}$ qui correspond à notre forme contient des sous-modules complets de corps plus petits, à savoir

$$\{1, \sqrt{2}\} \subset \mathbf{Q}(\sqrt{2}) \qquad \text{et} \qquad \{1, \sqrt{3}\} \subset \mathbf{Q}(\sqrt{3}).$$

Étudions une classe de formes qui possèdent cette propriété. Écrivons l'équation (1) sous la forme (3) et considérons le sous-espace vectoriel L (sur Q) engendré par les nombres du module M. Nous dirons que le module (sur Q) engendré par les nombres du module M. Nous dirons que le module M est *dégénéré* si l'espace L qu'il engendre contient un sous-espace L' semblable à un sous-corps $k' \subset k$, k' n'étant ni le corps des nombres rationnels, ni un corps quadratique imaginaire.

Montrons que, pour un module dégénéré, l'équation (3) a une infinité de solutions (pour certaines valeurs de a). En effet, si $L = \gamma k'$ ($\gamma \in k$) *et* $M' = L' \cap M$, alors $\gamma^{-1}M'$ est un module complet du corps k'. Par définition d'un module dégénéré, tout ordre du corps k' contient au moins une unité fondamentale et par suite l'équation

$$N_{k'/\mathbf{Q}}(\xi) = a, \qquad \xi \in \gamma^{-1}M' \tag{24}$$

a une infinité de solutions dès qu'elle en admet une. Posons $a, = N_{k/\mathbf{Q}}(\gamma)a^r$, où $r = (k : k')$. Puisque

$$N_{k/\mathbf{Q}}(\xi\gamma) = (N_{k'/\mathbf{Q}}(\xi))^r N_{k/\mathbf{Q}}(\gamma) = a$$

et $\xi\gamma \in M' \subset M$ (pour tout ξ satisfaisant à l'équation (24)), alors l'équation $N_{k/\mathbf{Q}}(\eta) = a,$, $\eta \in M$ a une infinité de solutions.

La conjecture principale relative aux équations du type (1) est la suivante : *une telle équation n'a qu'un nombre fini de solutions dans les nombres entiers si et seulement le module qui lui correspond n'est pus dégénéré.*

Le seul procédé d'approche de cette conjecture est actuellement la méthode de Skolem (avec l'hypothèse restrictive $t \geqslant m - 1$).

Pour démontrer le théorème 2, on utilise de manière essentielle l'hypothèse $m = 2$ dans le lemme 2. L'extension de ce lemme au cas général $n_1 + n_2 \geqslant n$ (à la place de $n_1 = n - 2$ et $n_2 \geqslant 2$) apparaît comme la principale difficulté pour démontrer la conjecture ci-dessus dans le cas $m > 2$ (et bien entendu $t \geqslant m - 1$). Skolem a obtenu une telle généralisation pour n = 5, $m = 2$, $n_2 = 3$ et en a déduit la finitude du nombre de solutions de l'équation (1) pour $n = 5$, $m = 3$, $t = 2$ (Th. Skolem, Einige Sätz über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen. *Math. Ann.*, 1935, 111, n° 3, 399-424). Cela montre que la conjecture est vraie pour $n = 5$ (avec la condition $t \geqslant m - 1$; la condition de non-dégénérescence du module n'intervient pas puisqu'ici le corps k est de degré premier et par suite n'a pas sous-corps).

Chabauty a démontré la conjecture ci-dessus pour $m = 3$ (et $t \geqslant 2$)

(C. Chabauty, Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques fini. *Ann. di Mat. pura e applicata,* 1938, 17, 127-168). Sa démonstration est de nature différente et utilise des propriétés plus précises des équations du type (16). Ainsi, on ne connaît pas de généralisation du lemme 2 pour $n_1 = n - 3$ (en dehors du cas $n = 5$ étudié par Skolem).

EXERCICES

1. Soit $f(t) = a_0 + a_1 t + a_2 t^2 + \ldots$ une série à coefficients entiers p-adiques qui converge pour tout entier p-adique t. Démontrer que si

$$v_p(a_1) < v_p(a_k), \qquad k = 2, 3, \ldots >$$

alors l'équation f(t) = 0 a une solution dans les entiers p-adiques pour

$$v_p(a_0) \geqslant v_p(a_1)$$

et n'a pas de solution dans les entiers p-adiques pour $v_p(a_0) < v_p(a_1)$.

2. Soit $d > 1$ un entier naturel sans carrés et soient (a, b) et (a_1, b_1) deux solutions non triviales (différentes de (1, 0)) de l'équation

$$x^3 + dy^3 = 1$$

(dans les nombres entiers rationnels). Posons, dans le corps cubique $K = \mathbf{Q}(\sqrt[3]{d})$, $\varepsilon = a + b\sqrt[3]{d}$, $\varepsilon_1 = a, + b_1\sqrt[3]{d}$. Démontrer qu'alors

$$\varepsilon^u = \varepsilon_1^v$$

pour certains entiers rationnels u et v dont l'un des deux au moins n'est pas divisible par 3.

3. Conservant les notations de l'exercice précédent, supposons $d \not\equiv \pm 1 \pmod 9$. On a alors dans le corps K la décomposition $3 = \mathfrak{p}^3$ (cf. exercice 24, chap. III, § 7) et ainsi le degré du complété p-adique $\mathbf{K}_\mathfrak{p}$ du corps K sur le corps des nombres 3-adiques $\mathbf{Q}_3$ est égal à 3. Supposant $v \not\equiv 0 \pmod 3$, posons $t = \frac{u}{v}$. Démontrer que le nombre t (considéré comme un nombre entier 3-adique) est racine de l'équation

$$\sum_{n=2}^{\infty} a_n t^n = 0 \qquad (*)$$

où $a_n = \frac{1}{n!}\,\mathrm{Tr}\,((\mathrm{Log}\ \eta)^n)$, $\eta = \varepsilon^3$ (ici Tr désigne la trace pour l'extension $\mathbf{K}_\mathfrak{p}/\mathbf{Q}_3$). Démontrer que la série de gauche dans (*) converge pour t entier 3-adique.

Indication. — Démontrer que $\mathrm{Tr}\,(\mathrm{Log}\ \eta) = 0$ et $\mathrm{Tr}\ \eta_1 = 3$, $\eta_1 = \varepsilon_1^3$.

4. Démontrer que les coefficients a_n de la série (*) sont tels que

$$v_3(a_2) = v_3(a_3) = \mu + 3, \qquad v_3(a_n) > \mu + 3 \qquad \text{pour} \qquad n > 3,$$

où $\mu = v_3(a^3 b^3 d)$ (v_3 est la valuation 3-adique).

Indication. — Utiliser le fait que si $\eta = 1 + 3x$, $\chi = ab\sqrt[3]{d}\,\varepsilon$, alors

$$\operatorname{Log}\eta \equiv 3x - \frac{9}{2}x^2 + 9x^3 \pmod{3^{4+\mu}}$$

et aussi le fait que la trace d'un élément de l'anneau $\mathbf{Z}_3[\sqrt[3]{d}]$ est divisible par 3 ($\mathbf{Z}_3$ est l'anneau des nombres entiers 3-adiques).

5. Utilisant les exercices 1 à 4, démontrer que l'équation $x^3 + dy^3 = 1$ pour $d \not\equiv \pm 1 \pmod 9$ a au plus une solution non triviale dans les nombres entiers rationnels.

6. Démontrer l'argument de l'exercice précédent dans le cas où $d \equiv \pm 1 \pmod 9$.

Indication. — Remarquer que dans le corps $K = \mathbf{Q}/(\sqrt[3]{d})$ le nombre 3 se décompose en un produit $3 = \mathfrak{p}^2\mathfrak{q}$ (exercice 24 du chapitre III, § 7) et transposer les raisonnements des exercices 3 et 4 à la somme directe $K_3 = K_\mathfrak{p} \oplus K_\mathfrak{q}$ (cf. § 2). La fonction logarithme sur K_3 est définie exactement comme sur un corps : la série sera convergente pour les $\xi = (\alpha, \beta) \in K_3$ tels que α et β soient des unités principales des corps $K_\mathfrak{p}$ et $K_\mathfrak{q}$ respectivement. La trace Tr ξ est définie comme étant la trace de la matrice de l'application linéaire $\xi' \to \xi\xi'$ ($\xi' \in K_3$); par suite, elle coïncide sur tout élément de $\hat{K}$ avec la trace de l'élément correspondant de K.

7. Supposons que la série

$$f(t) = a_0 + a_1 t + a_2 t^2 + \ldots >$$

à coefficients entiers p-adiques, converge pour tout t entier p-adique. Démontrer que si a, est une unité p-adique et $a_s \equiv 0 \pmod p$ pour tout $s > n$ alors l'équation f(r) = 0 a au plus n solutions dans les nombres entiers p-adiques.

8. Soit

$$y, u_1, \ldots, u_n, \ldots \qquad (**)$$

une suite de nombres entiers satisfaisant à la relation de récurrence

$$u_n = a_1 u_{n-1} + \ldots + a_m u_{n-m} \qquad (a_m \neq 0)$$

à coefficients a,, . . ., a_m entiers rationnels. Supposons que le polynôme

$$\varphi(x) = x^m - a_1 x^{m-1} - \ldots - a_m$$

n'a pas de racine multiple. Démontrer qu'alors il existe un entier naturel M tel que pour les indices n d'une même classe résiduelle modulo M ou bien toutes les valeurs u_n coïncident ou bien il n'existe pas de nombre répété une infinité de fois.

Indication. — Utiliser la formule $u_n = A_1\alpha_1^n + \ldots + A_m\alpha_m^n$ (α_i racines de $\varphi(x)$) et le fait que pour un nombre premier p convenable et un certain entier naturel M les fonctions $\alpha_i^{Mx} = \exp(x \operatorname{Log} x_i^M)$ sont des fonctions analytiques pour tout entier p-adique x.

9. Avec les notations de l'exercice précédent, supposons que toutes les racines α_i ($1 \leqslant i \leqslant m$) du polynôme $\varphi(x)$ et tous les rapports $\frac{\alpha_i}{\alpha_j}$ ($i \neq$ j) ne sont pas des racines de 1. Démontrer qu'alors aucun nombre entier n'est répété une infinité de fois dans la suite récurrente (**) (si cette suite n'est pas constituée entièrement par des zéros).

10. Soient f(y) une série entière quelconque et g(x) une série entière sans terme constant à coefficients dans un certain corps. Posons $F(x)$ =f(g(x)). Démontrer que

$$F'(x) = f'(g(x))g'(x).$$

11. Soit P(t) $\not\equiv 0$ une série entière formelle sans terme constant sur un corps quelconque. Démontrer que si

$$\sum_{i=1}^{n} a_i \exp \gamma_i P(t) = 0,$$

où tous les a_i ne sont pas nuls, alors $\gamma_k = \gamma_j$ pour au moins deux valeurs des indices $k \neq j$.

12. Démontrer l'argument du lemme 2 sous les hypothèses $n_1 = n - 1$, $n_2 = 1$ et $n_1 = 1$, $n_2 = n - 1$.

§ 7. — GERMES D'ENSEMBLES ANALYTIQUES

Soient k un corps de caractéristique zéro, complet pour une valuation ν et φ la métrique correspondante. Dans ce paragraphe, nous désignerons par $\tilde{k}^n$ l'espace n-dimensionne1 des systèmes $(\alpha_1, \ldots, a_n)$, appelés points, dont les composantes appartiennent à k ou à des extensions finies du corps k. Nous appellerons E-voisinage du point zéro dans $\tilde{k}^n$ l'ensemble des points $(\alpha_1, \ldots, \alpha_n)$ qui satisfont aux conditions $\varphi(\alpha_i) < \varepsilon$ $(i = 1, \ldots, n)$ (ε est un nombre réel > 0).

Considérons l'ensemble des séries entières $f(x_1, \ldots, x_n)$ de n variables, à coefficients dans k, qui convergent dans un certain E-voisinage du point zéro (c dépend de la série considérée). Il est facile de voir que toutes ces séries forment un anneau, que nous désignerons par $\mathfrak{D}$. Nous écrirons souvent f(X) à la place de $f(x_1, \ldots, x_n)$.

DÉFINITION. — *L'ensemble* V *des points* $(\alpha_1, \ldots, a_n) \in \tilde{k}^n$ *qui appartiennent à un certain* ε*-voisinage de zéro et qui vérifient le système des équations*

$$f_1(X) = 0, \ldots, f_m(X) = 0 \qquad (1)$$

où $f_1(X), \ldots, f_m(X)$ *sont des séries entières de l'anneau* $\mathfrak{D}$*, sans terme constant, est appelé un germe d'ensemble analytique* (ou, en abrégé, un germe analytique).

Nous considérerons que deux germes analytiques sont égaux s'ils coïncident dans un certain c-voisinage de zéro.

Bien entendu, on peut considérer des germes analytiques au voisinage d'un point quelconque de $\tilde{k}^n$. Nous avons choisi le point zéro pour simplifier les notations.

Soit V un germe analytique. L'ensemble de toutes les séries entières $f(X) \in \mathfrak{D}$ qui s'annulent en tous les points de V appartenant à un c-voisinage convenable de zéro forment un idéal de l'anneau $\mathfrak{D}$ que nous désignerons par $\mathfrak{U}_V$. Il est évident que chaque élément de l'anneau quotient $\mathfrak{D}/\mathfrak{U}_V = \overline{\mathfrak{D}}$ peut être

considéré comme une fonction définie sur les points du germe V qui appartiennent à un certain c-voisinage de zéro (le voisinage dépend de la fonction). Par suite, l'anneau $\mathfrak{D}$ est appelé ***l'anneau des fonctions analytiques sur*** V.

DÉFINITION. — ***Un germe analytique*** V ***est dit irréductible si l'anneau*** $\mathfrak{D}/\mathfrak{U}_V$ ***des fonctions analytiques sur*** V ***n'a pas de diviseurs de zéro. Dans le cas contraire,*** V ***est dit réductible.***

L'étude des germes analytiques repose sur trois résultats simples, dont l'un est algébrique et les deux autres conséquences des propriétés des séries entières. Nous les énoncerons sans démonstration, en donnant des références.

LEMME 1. — ***Soient*** $g_1(t), \ldots, g_m(t)$ ***des polynômes de l'anneau*** $k[t]$ ***dont le coefficient dominant est égal à*** 1. ***Il existe un système*** $h_1, \ldots, h_r$ ***de polynômes sur*** **Z** (i. e. à coefficients entiers) ***de leurs coefficients tels que, pour chaque choix de ces coefficients dans*** k, ***les conditions*** $h_1 = 0, \ldots, h_r = 0$ ***soient des conditions nécessaires et suffisantes pour que*** $g_1(t), \ldots, g_m(t)$ ***ait une racine commune dans une extension finie du corps*** k.

Si $m = 2$, $r = 1$ et h_1 est le résultant des polynômes g_1 et g_2. Le cas général se ramène facilement au cas $m = 2$. La démonstration est faite dans le livre de Van der Waerden, ***Algèbre moderne,*** tome II, chapitre XI, § 77.

LEMME 2. — ***Soit*** $f(x_1, \ldots, x_n) \in \mathfrak{D}$ ***une série entière dont le plus petit degré des termes qu'elle contient est égal à*** $k \geqslant 1$ ***et dont le coefficient de*** x_n^k ***est différent de zéro. Alors on peut trouver dans l'anneau*** $\mathfrak{D}$ ***une série*** $e(x_1, \ldots, x_n)$, ***de terme constant non nul, telle que***

$$f(X)e(X) = x_n^k + \varphi_1(x_1, \ldots, x_{n-1})x_n^{k-1} + \ldots + \varphi_k(x_1, \ldots, x_{n-1})$$

où $\varphi_1, \ldots, \varphi_k$ sont des séries des variables $x_1, \ldots, x_{n-1}$, de terme constant nul.

La démonstration de ce théorème est faite dans le livre de Siegel, ***Fonctions automorphes de plusieurs variables complexes,*** chapitre premier, § 2, pages 8-10 (Moscou, 1954).

Remarquons que la condition de non-nullité du coefficient de x_n^k peut toujours être obtenue par une transformation linéaire non singulière de la variable. De plus, partant de plusieurs séries entières $f_1, \ldots, f_m$, il est facile de voir qu'on peut choisir cette transformation linéaire pour que cette condition soit satisfaite simultanément pour toutes ces séries.

LEMME 3. — ***Tout idéal $\mathfrak{U}$ de l'anneau $\mathfrak{D}$ admet un système fini de générateurs,*** i. ***e. il contient des séries $h_1, \ldots, h_s$ telles que toute série $h \in \mathfrak{U}$ s'écrive***

$$h = g_1 h_1 + g_2 h_3 + \ldots + g_s h_s,$$

où $g_1, \ldots, g_s$ sont des séries de $\mathfrak{D}$.

Pour la démonstration de ce lemme, on pourra consulter le livre de Bochner et Martin, ***Several Complex Variables,*** chapitre X, § 1. Dans ce livre et dans le livre de Siegel, les démonstrations sont faites pour des séries sur le corps des nombres complexes, mais ces démonstrations s'appliquent aussi au cas d'un corps valué complet (*).

Nous utiliserons le lemme 3 pour démontrer le résultat suivant.

THÉORÈME 1. — ***Tout germe analytique est réunion d'un nombre fini de germes analytiques irréductibles.***

DÉMONSTRATION. — Supposons que le germe V est défini par les équations (1). Si V est réductible, il existe dans $\mathfrak{D}$ des séries entières f et g ne s'annulant pas en des points de V aussi voisins que l'on veut du point 0 et telles que fg s'annule sur tous les points de V contenus dans un certain e-voisinage de zéro. Dtsignons par V_1 et V_1' les germes définis par les équations (1) augmentées respectivement des équations $f(X) = 0$ et g(X) = 0. 11 est clair que V_1 et V_1' sont des sous-germes de V et que

$$v = V_1 \cup v;.$$

Si les germes V_1 et V_1' sont irréductibles, le théorème est démontre. Si l'un d'entre eux est réductible, nous pouvons de la même manière le représenter comme réunion de deux sous-germes propres. Répétant ce procédé, nous obtiendrons ou bien une représentation du germe V comme réunion d'un nombre fini de germes irréductibles (ce que nous voulons), ou bien une suite infinie de germes

$$v = V_0 \supsetneq V_1 \supsetneq V_2 \supset \ldots \supset \ldots \qquad (2)$$

Démontrons que ce dernier cas est impossible. Considérons les idéaux $\mathfrak{U}_{v_i}$ des germes V_i. Il résulte de (2) que

$$\mathfrak{U}_v \subsetneq \mathfrak{U}_{v_2} \subsetneq \mathfrak{U}_{v_3} \subset \ldots \qquad (3)$$

Désignons par $\mathfrak{U}$ la réunion des idéaux $\mathfrak{U}_{v_i}$. D'après le lemme 3, l'idéal $\mathfrak{U}$ est engendré par un système fini de séries $h_1, \ldots h_n$. Puisque toute série de $\mathfrak{U}$ appartient à un des idéaux $\mathfrak{U}_{v_i}$, il existe $\mathfrak{U}_k$ qui contient toutes les séries

(*) Pour la démonstration des lemmes 2 et 3, on pourra consulter également le livre de P. Samuel et 0. Zariski, ***Commutative Algebra***, vol. 2, *p.* 145 et 148, Princeton University Press, 1960 (N. d. T.).

$h_1, \ldots, h_s$. Mais alors $\mathfrak{U} \subset \mathfrak{U}_{v_k}$ et par suite $\mathfrak{U}_{v_k} = \mathfrak{U}_{v_{k+1}} = \ldots$, ce qui contredit (3). Le théorème (1) est ainsi démontré.

Nous allons maintenant exposer une méthode générale d'étude des germes analytiques par réduction du nombre des variables.

Soit **V** un germe analytique dans l'espace $\tilde{k}^n$, défini par les équations (1). Si V est différent de $\tilde{k}^n$, nous pouvons supposer que les séries $f_1, \ldots, f_m$ ($m \geqslant 1$) ne sont pas identiquement nulles; nous effectuerons éventuellement une transformation linéaire des variables de telle sorte que tous les polynômes f_i satisfassent aux conditions du lemme 2. Il existe alors dans l'anneau $\mathfrak{D}$ des séries entières $e_1(X), \ldots, e_m(X)$ à termes constants non nuls, telles que

$$f_i e_i = g_i = x_n^{k_i} + \varphi_{i1} x_n^{k_i - 1} + \ldots + \varphi_{ik_i} \tag{4}$$

où $\varphi_{ij} = \varphi_{ij}(x_1, \ldots, x_{n-1})$ sont des séries entières de $n - 1$ variable sans terme constant. Puisque $e_i(X) \neq 0$ dans un certain E-voisinage de 0, le germe V est aussi défini par le système d'équations

$$g_1(X) = 0, \ldots, g_m(X) = 0,$$

dont les termes de gauche sont des polynômes en x_n de coefficients dominants égaux à 1. Nous pouvons appliquer le lemme 1 à ces polynômes; les polynômes $h_1, \ldots, h_r$ correspondants sont des séries entières de $x_1, \ldots, x_{n-1}$, sans terme constant et puisque les φ_{ij} convergent dans un certain E-voisinage de zéro, les séries $h_1, \ldots, h_s$ seront convergentes dans ce voisinage.

Considérons, dans l'espace $\tilde{k}^{n-1}$, le germe analytique W défini par les équations

$$h_1(x_1, \ldots, x_{n-1}) = 0, \ldots, h_r(x_1, \ldots, x_{n-1}) = 0.$$

Il est clair qu'un point $(\alpha_1, \ldots, \alpha_{n-1}) \in \tilde{k}^{n-1}$ appartient à W si et seulement si tous les polynômes $g_i(\alpha_1, \ldots, \alpha_{n-1}, x_n)$ ont une racine commune, i. e. s'il existe a, tel que $(a, \ldots, \alpha_{n-1}, \alpha_n) \in$ V. Ainsi, le germe W est la projection du germe V sur l'hyperplan $x_n = 0$. Il en résulte que tout point

$$(\alpha_1, \ldots, \alpha_{n-1}) \in W$$

est la projection d'un nombre fini de points $(a, \ldots, \alpha_{n-1}, a_n) \in$ V puisque a, est une racine commune des polynômes $g_i(\alpha_1, \ldots, \alpha_{n-1}, x_n)$. Le passage du germe V à sa projection W est une méthode fondamentale d'étude des germes analytiques.

DÉFINITION. — ***On appelle courbe dans l'espace $\tilde{k}^n$ un système de n séries entières formelles $\omega_1(t), \ldots, \omega_n(t)$, sans termes constants, à coefficients dans le corps k ou dans une extensionfinie de k, les $\omega_i(t)$ n'étant pas tous identiquement nuls.***

Pour le propos qui nous intéresse, il n'est pas nécessaire de supposer que

les séries $\omega_i(t) = a_{i1}t + a_{i2}t^2 + \ldots$ sont convergentes; il est donc plus simple ici de ne pas faire cette hypothèse. Ainsi une courbe n'est pas donnée par l'ensemble de ses points mais par les séries $\omega_i(t)$. Dire que la courbe appartient à un germe analytique aura un sens un peu différent du sens usuel.

DÉFINITION. — *Nous dirons qu'une courbe $w_i(t), \ldots, \omega_n(t)$ appartient à un germe* V *si pour toute série $f(x_1, \ldots, x_n)$ de l'idéal $\mathfrak{U}_V$ la série entière formelle $f(\omega_1(t), \ldots, \omega_n(t))$ est identiquement nulle.*

La propriété essentielle des germes d'ensembles analytiques est la suivante :

THÉORÈME 2. — *Tout germe analytique, ou bien est réduit au point zéro, ou bien contient au moins une courbe.*

La démonstration se fait par récurrence sur la dimension n.

D'après le lemme 3, l'idéal $\mathfrak{U}$, a un nombre fini de générateurs; on peut donc prendre comme système (1) définissant le germe analytique V un système de générateurs de l'idéal $\mathfrak{U}_V$. Pour $n = 1$, le germe V est réduit au point 0 si l'une au moins des séries f_i n'est pas identiquement nulle et coïncide avec k^1 si tous les f_i sont identiquement nuls. Dans ce dernier cas, toute série $w(t)$ convient.

Soit maintenant $n > 1$; l'argument du théorème est évident si tous les f_i sont identiquement nulles (ou si $m = 0$). On peut donc supposer qu'aucune des séries $f_1, \ldots, f_m$ $(m > 0)$ n'est nulle; nous supposerons aussi que ces séries satisfont aux hypothèses du lemme 2, de telle sorte que nous puissions remplacer les équations (1) par les équations (5) pour définir V (les g_i sont définies par les égalités (4)). Considérons la projection W du germe V dans l'espace $\tilde{k}^{n-1}$. Le théorème 2 est vrai pour W, par hypothèse de récurrence. Si W est réduit au point zéro, alors le germe V est défini par le systéme d'équations

$$g_i(0, 0, \ldots, 0, x_n) = 0 \qquad (1 \leqslant i \leqslant m),$$

i. e. coïncide aussi avec le point zéro. Si maintenant W contient la courbe $\omega_1(t), \ldots, \omega_{n-1}(t)$, désignons par k_1 une extension finie du corps k qui contienne les coefficients des séries $\omega_1, \ldots, \omega_{n-1}$. Par substitution des séries $\omega_1(t), \ldots, w_i(t)$ dans les séries $g_1, \ldots, g_m$ à la place de $x_1, \ldots, x_{n-1}$, nous obtenons m polynômes en x_n :

$$g_i(\omega_1(t), \ldots, \omega_{n-1}(t), x_n), \qquad 1 \leqslant i \leqslant m, \tag{6}$$

dont les coefficients appartiennent au corps $k_1\{t\}$ des séries formelles de t sur k; ces polynômes ont une racine commune $x_n = \xi$ dans une certaine extension finie Ω du corps $k_1\{t\}$. D'après le théorème 6 du § 1 le corps Ω est contenu dans un corps de séries formelles $k'\{u\}$, avec $u^e = t$, pour un certain entier e et une certaine extension finie k' de k. On peut donc consi-

dérer l'élément $\xi = \omega(u)$ comme une série entière à coefficients dans k'. Puisque ξ est racine des polynômes (6) dont les coefficients dominants sont égaux à 1 et les autres coefficients des éléments entiers du corps $k_1\{t\}$, la série $\omega(u)$ est un élément entier du corps $k'\{u\}$, i. e. ne contient pas de puissances négatives de u. De plus, dans la représentation (4), les séries φ_{ij} sont sans terme constant; remplaçant dans (4) $x_1, \ldots, x_{n-1}$ par les séries $\omega_1(u^e), \ldots, \omega_{n-1}(u^e)$ et x_n par la série $\omega(u)$, nous obtenons que le terme constant de la série $\omega(u)$ est nul et que l'on a l'identité :

$$g_i(\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)) = 0 \qquad (1 \leqslant i \leqslant m).$$

Puisque les séries $\omega_1, \ldots, \omega_{n-1}$ ne sont pas toutes nulles, la donnée des séries entières $\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)$ définit une courbe de $\tilde{k}^n$. Par hypothèse, les séries $f_1, \ldots, f_m$ et par suite les séries $g_1, \ldots, g_m$ engendrent l'idéal $\mathfrak{U}_v$; pour toute série $f(x_1, \ldots, x_n) \in \mathfrak{U}_v$, on a donc l'identité

$$f(\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)) = 0$$

et par suite la courbe $\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)$ appartient au germe V. Le théorème 2 est démontré.

THÉORÈME 3. — *Soient* V *et* V' *deux germes analytiques de* $\tilde{k}^n$, V *non contenu dans* V'. *Il existe dans* $\tilde{k}^n$ *une courbe qui appartient à* V *et qui n'appartient pas à* V'.

DÉMONSTRATION. — Nous pouvons supposer que le germe V est irréductible car sinon on peut le remplacer par une de ses composantes irréductibles.

Supposons que le germe V' est défini par les équations

$$F_1(X) = 0, \ldots, F_l(X) = 0,$$

où les F_j sont des séries de l'anneau $\mathfrak{D}$. Puisque $V \not\subset V'$, l'une au moins des séries F_j ne s'annule pas identiquement sur V (dans tout voisinage, aussi petit que l'on veut, du point zéro). Désignons cette série par F(X) et montrons qu'il existe une courbe $\omega_1(t), \ldots, \omega_n(t)$ appartenant au germe V et telle que

$$F(\omega_1(t), \ldots, \omega_n(t)) \neq 0.$$

Nous procéderons par récurrence sur n.

Il est clair que nous pouvons supposer que la série F(X) satisfait à la condition du lemme 2; il existe alors une série $e(X) = e(x_1, \ldots, x_n) \in \mathfrak{D}$, de terme constant non nul, telle que

$$e(X)F(X) = G(x_1, \ldots, x_n) = x_n^k + \psi_1 x_n^{k-1} + \ldots + \psi_k, \qquad (7)$$

où $\psi_1, \ldots, \psi_k$ sont des séries en $x_1, \ldots, x_{n-1}$.

Si V = $\tilde{k}^n$ (en particulier pour $n = 1$), l'argument du théorème 3 est trivialement vrai : il suffit par exemple de prendre $\omega_1(t) = \ldots = \omega_{n-1}(t) = 0$,

$w_1(t) = t$. Si maintenant $V \neq k^n$, nous pouvons considérer la projection $W \subset \tilde{k}^{n-1}$ du germe V (nous supposons ici que, en plus de F(X), toutes les séries $f_1, \ldots, f_m$ définissant le germe V, satisfont à la condition du lemme 2; il suffit pour cela, comme nous le savons, de faire une transformation linéaire des variables). Le germe W est irréductible en même temps que V puisque son anneau de fonctions, i. e. l'anneau quotient

$$\mathfrak{D}_{n-1}/\mathfrak{U}_W = \overline{\mathfrak{D}}_{n-1}$$

est un sous-anneau de l'anneau des fonctions de V, $\mathfrak{D}/\mathfrak{U}_V = \overline{\mathfrak{D}}$ (en plus de l'inclusion $\mathfrak{D}_{n-1} \subset \mathfrak{D}$, nous avons aussi l'inclusion $\mathfrak{U}_W \subset \mathfrak{U}_V$). Pour toute série $f \in \mathfrak{D}$, désignons parf la fonction correspondante de $\overline{\mathfrak{D}}$. Les égalités (4) entraînent que

$$\overline{x}_n^{k_i} + \overline{\varphi}_{i1}\overline{x}_n^{k_i-1} + \ldots + \overline{\varphi}_{ik_i} = 0,$$

et cela signifie que la fonction $\overline{x}_n$ est un élément entier de l'anneau $\overline{\mathfrak{D}}$ sur le sous-anneau%,-,. Il en résulte que la fonction

$$\overline{G} = \overline{x}_n^k + \overline{\psi}_1\overline{x}_n^{k-1} + \ldots + \overline{\psi}_k \qquad (\overline{\psi}_i \in \overline{\mathfrak{D}}_{n-1})$$

est aussi un élément entier sur $\overline{\mathfrak{D}}_{n-1}$.

Considérons l'égalité

$$@ + \overline{L}_1\overline{G}^{s-1} + \ldots + \overline{L}_s = 0 \qquad (L_j \in \mathfrak{D}_{n-1}), \tag{8}$$

s étant le plus petit possible. Il est clair que $\overline{L}_s \neq 0$ puisque sinon nous pourrions diviser les deux membres par $\overline{G}$ et obtenir une égalité analogue pour une plus petite valeur de s. La série $L_s \in \mathfrak{D}_{n-1}$ ne s'annule donc pas sur W (dans un certain voisinage). Par récurrence, il existe dans l'espace k^{n-1} une courbe $\omega_1(t), \ldots, \omega_{n-1}(t)$ qui appartient au germe W et telle que

$$L_s(\omega_1(t), \ldots, \omega_{n-1}(t)) \neq 0.$$

Dans la démonstration du théorème 2, nous avons vu qu'il existe alors dans $\tilde{k}^n$ une courbe du type $\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)$ qui appartient au germe V. Vérifions que, pour cette courbe,

$$G(\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)) \neq 0,$$

i. e. cette courbe n'appartient pas au germe V'. En effet, si la série de gauche était identiquement nulle, alors, d'après (8), nous aurions l'égalité

$$L_s(\omega_1(u^e), \ldots, \omega_{n-1}(u^e)) = 0$$

d'où, en remplaçant u^e par t,

$$L_s(\omega_1(t), \ldots, \omega_{n-1}(t)) = 0,$$

en contradiction avec le choix de la courbe $\omega_1(t), \ldots, \omega_{n-1}(t)$.

CHAPITRE V

MÉTHODE ANALYTIQUE

Au chapitre III, nous avons vu qu'une importante **caractéristique** arithmétique d'un corps de nombres algébriques est le nombre h de ses classes de diviseurs. Il serait donc souhaitable de trouver une expression explicite de ce nombre h au moyen de grandeurs liées au corps K considéré. Ce problème n'est pas encore résolu pour un corps quelconque de nombres algébriques; cependant on a trouvé de telles formules dans des cas particuliers importants (par exemple pour les corps quadratiques et les corps cyclotomiques).

La méthode de l'analyse donne de nombreux résultats en théorie des nombres. Dans ce chapitre, nous l'appliquerons au problème de la recherche du nombre de classes de diviseurs.

§ 1. — EXPRESSION ANALYTIQUE DU NOMBRE DE CLASSES DE DIVISEURS

1) Fonction zêta de Dedekind

La recherche du nombre h de classes de diviseurs d'un corps K de nombres algébriques repose sur l'examen de la fonction suivante, appelée ***fonction zêta de Dedekind*** :

$$\zeta_K(s) = \sum_a \frac{1}{N(a)^s}, \tag{1}$$

où a parcourt tous les diviseurs entiers du corps K; N(a) désigne la norme du diviseur a. Nous montrerons que la série qui figure dans la partie droite de l'égalité (1) converge pour $1 < s < \infty$, représente dans cet intervalle une fonction continue de la variable réelle s et que l'on a la formule :

$$\lim_{s \to 1+0} (s-1)\zeta_K(s) = \kappa h \tag{2}$$

où κ est une constante simple, liée au corps K, qui sera calculée explicitement.

L'importance de la formule (2) tient au fait que la fonction $\zeta_K(s)$ admet une décomposition en produit infini

$$\zeta_K(s) = \prod_p \frac{1}{1 - \frac{1}{N(p)^s}}, \tag{3}$$

étendu à tous les diviseurs p du corps K, appelée identité d'Euler. Si nous connaissons bien les diviseurs premiers d'un certain corps K (plus précisément, si nous connaissons les lois de décomposition des nombres premiers rationnels comme produits de diviseurs premiers du corps K), les formules (2) et (3) nous donnerons une expression satisfaisante de h. C'est ainsi que nous obtiendrons, dans les paragraphes suivants, l'expression de h si K est un corps quadratique ou cyclotomique.

Décomposons la série (1) en une somme de h séries

$$\zeta_K(s) = \sum_C \left(\sum_{a \in C} \frac{1}{N(a)^s} \right),$$

où a parcourt tous les diviseurs entiers d'une classe donnée C de diviseurs, la première sommation étant effectuée suivant les h classes C. Pour démontrer la convergence de la série (1), il suffit de montrer que chacune des séries

$$f_C(s) = \sum_{a \in C} \frac{1}{N(a)^s} \tag{4}$$

converge pour $s > 1$. De plus, si nous démontrons que pour chaque classe C la limite $\lim_{s \to 1+0} (s - 1) f_C(s)$ existe et est la même pour toutes les classes C, alors, désignant cette limite par κ, nous obtenons la formule (2).

Transformons la série (4) en une série étendue à certains nombres entiers du corps K. Choisissons un diviseur entier a' dans la classe inverse C^{-1}. Pour tout $a \in C$, le produit a. a' est un diviseur principal :

$$aa' = (a), \qquad \alpha \in K.$$

11 est clair que l'application

$$a \to (\alpha) \qquad a \in C$$

établit une correspondance bijective (pour a' fixé) entre les diviseurs entiers a de la classe C et les diviseurs principaux (a) divisibles par a'. Utilisant l'égalité

$$N(a)N(a') = |N(\alpha)|,$$

nous obtenons

$$f_c(s) = \mathrm{N}(\mathfrak{a}')^s \sum_{\substack{(\alpha) \\ \alpha \equiv 0 \bmod \mathfrak{a}'}} \frac{1}{|\mathrm{N}(\alpha)|^s}, \qquad (5)$$

la sommation étant étendue à tous les diviseurs principaux du corps K divisibles par a'. Puisque deux diviseurs principaux (α_1) et (α_2) sont égaux si et seulement les nombres α_1 et α_2 sont associés, on peut considérer que la sommation dans la série (5) est étendue à un ensemble complet de nombres entiers non nuls, deux à deux non associés du corps K et, divisibles par a'.

Pour interpréter la série (5), nous utiliserons la représentation géométrique des nombres du corps K comme points de l'espace n-dimensionne1 réel $\mathcal{R}^n = \mathfrak{L}^{s,t}$ et de l'espace logarithmique $\mathcal{R}^{s+t}$ (ici $n = s + 2t$ est le degré du corps K, cf. chap. II, § 3-1) et 3)). Définissons dans $\mathcal{R}^n$ un cône X tel que parmi les nombres associés du corps K il en existe un et un seul dont l'image géométrique appartient à X (par cône on entend ici un sous-ensemble de $\mathcal{R}^n$ qui, avec tout point $x \neq 0$ contient toute la demi-droite ξx, $0 < \xi < \infty$).

Dans le chapitre II, § 3 (dont nous conserverons ici les notations), on a défini, en utilisant l'égalité (13), un homomorphisme $x \to l(x)$ du groupe multiplicatif des points $x \in \mathcal{R}^n$ de norme N(x) non nulle dans le groupe additif des vecteurs de l'espace logarithmique $\mathcal{R}^{s+t}$. Si $\varepsilon_1, \ldots, \varepsilon_r$ est un système d'unités fondamentales du corps K, alors les vecteurs $l(\varepsilon_1), \ldots, l(\varepsilon_r)$, comme nous le savons, forment une base d'un sous-espace de dimension $Y = s + t - 1$ formé des points $(\lambda_1, \ldots, \lambda_{s+t}) \in \mathcal{R}^{s+t}$ tels que

$$A, + \ldots + \lambda_{s+t} = 0.$$

Puisque le vecteur

$$l^* = (\underbrace{1; \ldots 1}_{s}; \underbrace{2; \ldots 2}_{t})$$

n'appartient pas à ce sous-espace, le système des vecteurs

$$l^*, l(\varepsilon_1), \ldots, l(\varepsilon_r) \qquad (6)$$

est une base de $\mathcal{R}^{s+t}$. Chaque vecteur $l(x) \in \mathcal{R}^{s+t}$ ($x \in \mathcal{R}^n$, $\mathrm{N}(x) \neq 0$) s'écrit donc

$$l(x) = \xi l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r), \qquad (7)$$

$\xi, \xi_1, \ldots, \xi_r$ étant des nombres réels.

Désignons par m l'ordre du groupe des racines de 1 qui sont contenues dans le corps K.

DÉFINITION. — ***On appelle domaine fondamental du corps*** K le sous-***ensemble X de l'espace*** $\mathfrak{R}^n$ ***formé des points x qui remplissent les trois conditions suivantes*** :

1° $$N(x) \neq 0;$$

2° ***Dans la décomposition*** (7), ***les coefficients*** ξ_i $(1 \leqslant i \leqslant r)$ ***satisfont aux inégalités*** $0 \leqslant \xi_i < 1$;

3° $0 \leqslant \arg x_1 < \dfrac{2\pi}{m}$, x_1 ***étant la première composante du point x.***

Remarquons que pour $s \geqslant 1$, alors $m = 2$ et la condition 3° signifie simplement que $x_1 > 0$.

Dans le point suivant, nous verrons que le domaine fondamental X est un cône dans $\mathfrak{R}^n$ et nous démontrerons le théorème suivant :

THÉORÈME 1. — ***Dans toute classe de nombres entiers*** $(\neq 0)$ ***associés entre eux du corps*** K ***il existe un nombre et un seul dont l'image géométrique dans l'espace*** $\mathfrak{R}^n$ ***appartient au domaine fondamental X.***

Revenons à la série (5). Si nous désignons par $\mathfrak{M}$ le lattice n-dimensionne1 de $\mathfrak{R}^n$ formé des images x(a) $\in \mathfrak{R}^n$ des nombres entiers a $\in$ K divisibles par a', alors, d'après l'égalité $|\,N(a)\,| = |\,N(x(a))\,|$, nous pouvons écrire la série (5) sous la forme

$$f_c(s) = N(\mathfrak{a}') \sum_{x \in \mathfrak{M} \cap X} \frac{1}{|\,N(x)\,|^s}, \tag{8}$$

où la sommation est étendue à tous les points x = x(a) du lattice $\mathfrak{M}$ qui appartiennent à X.

Dans le point 4), nous démontrerons un théorème général sur les séries où la sommation est étendue à tous les points d'un lattice qui appartiennent à un certain cône (théorème 3). Appliqué ici, ce théorème montrera que la série (8) est convergente pour $s > 1$ et que

$$\lim_{s \to 1+0} (s-1) \sum_{x \in \mathfrak{M} \cap \Delta} \frac{1}{|\,N(x)\,|^s} = \frac{v}{\Delta}, \tag{9}$$

A étant le volume d'un parallélépipède fondamental du lattice $\mathfrak{M}$ et v le volume de l'ensemble T formé des points x du domaine fondamental X tels que $|\,N(x)\,| \leqslant 1$.

D'après le théorème 2 du chapitre II, § 4 et l'égalité 3) du chapitre II, § 6, A est donné par la formule

$$\Delta = \frac{1}{2^t} N(\mathfrak{a}') \sqrt{|\,D\,|}, \tag{10}$$

où D est le discriminant du corps K. Le volume v de l'ensemble T sera acculé au point 3). Nous obtiendrons

$$v = \frac{2^s \pi^t R}{m}, \tag{11}$$

où R est le régulateur du corps K. Il résulte maintenant de (9), (10) et (11) que l'on a

$$\lim_{s \to 1+0} (s-1) f_C(s) = \frac{2^{s+t} \pi^t R}{m \sqrt{|D|}},$$

et, puisque $\zeta_K(s) = \sum_C f_C(s)$, nous avons obtenu le résultat fondamental suivant :

THÉORÈME 2. — *Soit* K *un corps de nombres algébriques de degré* $n = s + 2t$. *La série*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

est convergente pour $s > 1$ ***et on a la formule***

$$\lim_{s \to 1+0} (s-1) \zeta_K(s) = \frac{2^{s+t} \pi^t R}{m \sqrt{|D|}} h,$$

où h est le nombre de classes de diviseurs; D ***et*** R ***sont respectivement le discriminant et le régulateur du corps*** K ***et m est le nombre de racines de*** 1 ***contenues dans*** **K.**

Passons maintenant à la démonstration des arguments que nous avons utilisés pour établir le théorème 2.

2) Domaine fondamental

ξ étant un nombre réel positif, calculons $l(\xi x) \in \mathfrak{L}^{s,t}$ pour $x \in \mathfrak{R}^n$, $N(x) \neq 0$. D'après l'égalité (12) du chapitre II, § 3, nous avons

$$l_k(\xi x) = \text{Log } \xi + l_k(x) \qquad \text{pour} \qquad 1 \leqslant k \leqslant s;$$

$$l_{s+j}(\xi x) = 2 \text{ Log } \xi + l_{s+j}(x) \qquad \text{pour} \qquad 1 \leqslant j \leqslant s.$$

Il en résulte que

$$l(\xi x) = \text{Log } \xi . l^* + l(x);$$

par suite, pour les décompositions des vecteurs $l(x)$ et $l(\xi x)$ dans la base (6), les coefficients de $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ sont identiques pour ces deux vecteurs.

Puisque $N(\xi x) = \xi^n N(x) \neq 0$ et arg $(\xi x)_1 = \arg x_1$, pour tout point x du domaine fondamental X, toute la demi-droite ξx appartient aussi à X, i. e. le domaine X est un cône dans $\mathcal{R}^n$ (X n'est pas vide puisqu'il contient par exemple l'image $x(1)$ du nombre $1 \in K$).

LEMME 1. — ***Tout point $y \in \mathcal{R}^n$ tel que $N(y) \neq 0$ s'écrit de manière unique sous la forme***

$$y = xx(\varepsilon), \tag{12}$$

où x est un point du domaine fondamental X et ε une unité du corps K.

DEMONSTRATION. — Décomposons le vecteur Z(y) dans la base (6) :

$$l(y) = \gamma l^* + \gamma_1 l(\varepsilon_1) + \ldots + \gamma_r l(\varepsilon_r);$$

chacun des nombres réels γ_j $(j = 1, \ldots, r)$ s'écrit

$$\gamma_j = k_j + \xi_j,$$

où k_j est un entier rationnel et $0 < \xi_j < 1$. Posant $\eta = \varepsilon_r^{k_1} \ldots \varepsilon_1^{k_r}$, considérons le point $z = yx(\eta^{-1})$. Nous avons

$$\begin{aligned} l(z) = l(y) + l(\eta^{-1}) &= l(y) - k_1 l(\varepsilon_1) - \ldots - k_r l(\varepsilon_r) \\ &= \gamma l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r). \end{aligned}$$

Soit $\arg z_1 = \varphi$; pour un certain entier k, nous aurons

$$0 \leqslant \varphi - \frac{2\pi k}{m} < \frac{2\pi}{m}.$$

Par l'isomorphisme $a \to \sigma_1(\alpha)$ $(a \in K)$, les racines $m^{\text{ièmes}}$ de 1 du corps K s'envoient sur les racines $m^{\text{ièmes}}$ de 1 du corps de tous les nombres complexes. Désignons par ζ la racine $m^{\text{ième}}$ de 1 (elle sera primitive) telle que

$$\sigma_1(\zeta) = \cos \frac{2x}{m} + i \sin \frac{2\pi}{m}.$$

Démontrons que le point $x = zx(\zeta^{-k})$ appartient au domaine fondamental X. En effet

$$l(x) = l(z) + l(\zeta^{-k}) = l(z) = \gamma l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r),$$

avec $0 \leqslant \xi_j < 1$ et les conditions 1^o et 2^o sont remplies. De plus,

$$x_1 = z_1 x(\zeta^{-k})_1 = z_1 \sigma_1(\zeta)^{-k}$$

d'où

$$\arg x_1 = \arg z_1 - k \frac{2x}{m} = \varphi - \frac{2xk}{m};$$

par suite,

$$0 \leqslant \arg x_1 < \frac{2\pi}{m}.$$

Ainsi $x \in X$. Remarquant maintenant que $x(\alpha^{1-}) = x(\alpha)^{-1}$, nous obtenons

$$y = zx(\eta) = xx(\zeta^k)x(\eta) = XX(E)$$

avec $\varepsilon = \zeta^k\eta$. Nous avons ainsi écrit le point y sous la forme (12). II reste à démontrer l'unicité d'une telle décomposition. Supposons que l'on ait, en plus de (12), $y = x'x(\varepsilon')$ avec $x' \in X$ et ε' unité de K. Puisque

$$XX(E) = x'x(\varepsilon'),$$

alors

$$l(x) + l(\varepsilon) = l(x') + l(\varepsilon').$$

Les vecteurs $l(\varepsilon)$ et $l(\varepsilon')$ sont des combinaisons linéaires à coefficients entiers des vecteurs $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ et les coefficients de $l(x)$ et I(x') dans la base (6) sont tous positifs et inférieurs à l'unité (condition 2° de la définition du domaine fondamental). Il résulte donc de la dernière égalité que $l(\varepsilon') = l(\varepsilon)$, d'où $\varepsilon' = \varepsilon\zeta_0$, ζ_0 étant une racine $m^{\text{ième}}$ de 1 (cf. chap. II, § 3, 4)). De l'égalité $X(E') = x(\varepsilon)x(\zeta_0)$ résulte maintenant que $x = x'x(\zeta_0)$ et par suite

$$x_1 = x_1'\sigma_1(\zeta_0).$$

D'après la condition 3°, les points x et x' appartenant au domaine fondamental vérifient les conditions

$$0 \leqslant \arg x_1 < \frac{2\pi}{m}, \qquad 0 \leqslant \arg x_1' < \frac{2\pi}{m}$$

c'est pourquoi $0 \leqslant |\arg \sigma_1(\zeta_0)| < \frac{2x}{m}$; puisque $\sigma_1(\zeta_0)$ est une racine $m^{\text{ième}}$ de 1, cette dernière inégalité n'est possible que si $\arg \sigma_1(\zeta_0) = 0$. Mais dans ce cas, $\sigma_1(\zeta_0) = 1$ et $\zeta_0 = 1$. Ainsi $\varepsilon' = \varepsilon$, d'où x' = x et le lemme 1 est démontré.

DÉMONSTRATION DU THÉORÈME 1. — Soit β un nombre entier $\neq 0$ de K. D'après le lemme 1, on a la décomposition $x(\beta) = xx(\varepsilon)$, avec $x \in X$ et ε unité. Le nombre $a = \beta\varepsilon^{-1}$ est associé à β et son image géométrique x(a) (qui coïncide avec le point x) appartient au domaine X. De plus, d'après l'unicité de la décomposition (12), le nombre a est défini de manière unique par les conditions $\beta = \alpha\varepsilon$, $x(a) \in X$. Le théorème 1 est démontré.

A titre d'exemple, déterminons le domaine fondamental d'un corps quadratique. Supposons tout d'abord que K est un corps quadratique réel i. e.

$n = s = 2$, $t = 0$, $r = s + t - 1 = 1$. Nous considérerons K comme un sous-corps du corps C de tous les nombres complexes ; le premier isomorphisme $\sigma_1 : K \to C$ (cf. chap. II, § 3, 1)) sera l'isomorphisme identité. Si ε est une unité fondamentale du corps, alors $-\varepsilon, \frac{1}{\varepsilon}$ et $-\frac{1}{\varepsilon}$ sont aussi des unités fondamentales; on peut donc supposer $\varepsilon > 1$. Si $x = (x_1, x_2) \in \mathcal{R}^2$, $N(x) = x_1, x_2 \neq 0$, alors $l(x) = (\text{Log} \mid x_1 \mid, \text{Log} \mid x_2 \mid)$. La décomposition (7) s'écrit dans ce cas

$$l(x) = \xi(1, 1) + \xi_1 (\text{Log}\, \varepsilon, -\text{Log}\, \varepsilon).$$

Le domaine fondamental X est donc défini ici par les conditions

$$x_1 > 0, \qquad x_2 \neq 0, \qquad 0 \leqslant \xi_1 < 1.$$

Il est facile de voir que

$$\text{Log} \mid x_1 \mid = \text{Log} \mid x_2 \mid + 2\xi_1 \text{Log}\, \varepsilon,$$

ce qui signifie

$$\mid x_1 \mid = \mid x_2 \mid e^{2\xi_1}.$$

La condition $0 \leqslant \xi_1 < 1$ peut donc être remplacée par la condition :

$$1 \geqslant \frac{\mid x_2 \mid}{\mid x_1 \mid} > \varepsilon^{-2}.$$

Le domaine fondamental est donc l'ensemble hachuré dans la figure 7 (les côtés des angles les plus proches de la demi-droite positive Ox_1 n'appartiennent pas à X).

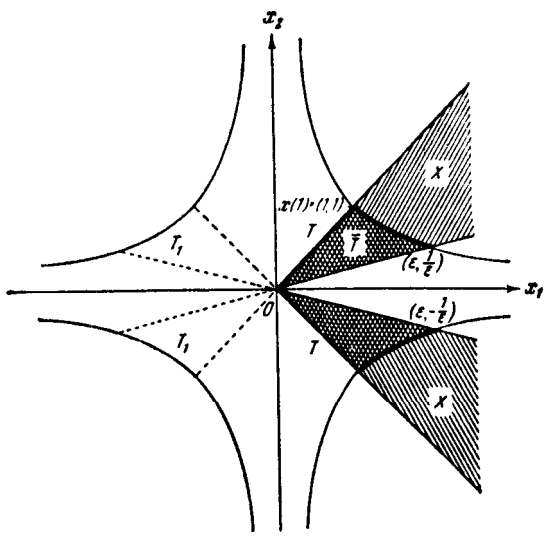


FIG. 7.

Supposons maintenant que K est un corps quadratique imaginaire. Puisqu'ici $s = 0$, $t = 1$, alors $r = s + t - 1 = 0$. Le domaine fondamental est formé des points $x = y + iz$ tels que

$$N(x) = x^2 + y^2 \neq 0, \qquad 0 \leqslant \arg x < \frac{2\pi}{m}$$

(cf. figure 8, K = $\mathbf{Q}(\sqrt{-3})$, $m = 6$).

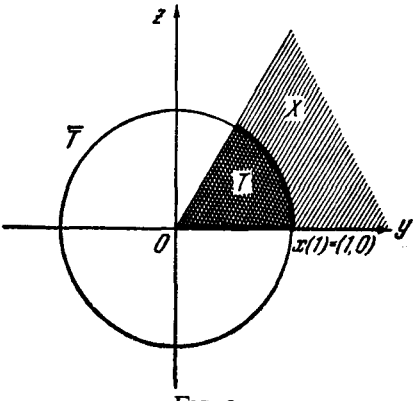


FIG. 8.

3) Calcul du volume

Calculons maintenant le volume n-dimensionnel de l'ensemble T formé des points x du domaine fondamental X tels que $|N(x)| \leqslant 1$. Nous démontrerons au cours de ce calcul que ce volume existe et n'est pas nul (dans le cas d'un corps quadratique, l'ensemble T est indiqué par des doubles hachures sur les figures 7 et 8).

Démontrons tout d'abord que l'ensemble T est borné. Sur toute demi-droite appartenant au cône X, il existe un point x et un seul tel que $|N(x)| = 1$. Désignons par S l'ensemble de tous ces points. Il est clair que T est la réunion de tous les segments ξx ($0 < \xi \leqslant 1$) quand x parcourt S.

Soit $x \in \mathcal{R}^n$ un point quelconque de norme non nulle et comparons la somme des composantes des vecteurs de gauche et de droite dans la formule (7). D'après la formule (15) du chapitre II, § 3, la somme des composantes de gauche est égale à $\operatorname{Log}|N(x)|$ et, d'après la relation (18) chapitre II § 3, celle de droite est égale à $\xi(s + 2t) = n\xi$. Cela montre que $\xi = \frac{1}{n}\operatorname{Log}|N(x)|$ et nous pouvons écrire la décomposition (7) sous la forme

$$l(x) = \frac{1}{n}\operatorname{Log}|N(x)| \cdot l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r). \qquad (13)$$

Si maintenant $x \in S$, alors Log $|N(x)| = 0$ et par suite le point

$$l(x) = (l_1(x), \ldots, l_{s+t}(x)) \in \mathcal{R}^{s+t}$$

se représente sous la forme $l(x) = \xi_1 l(\varepsilon_1), \ldots, \xi_r l(\varepsilon_r)$, avec $0 \leqslant \xi < 1$. Il en résulte qu'il existe une constante ρ telle que $l_j(x) < \rho$, d'où $|x_k| < e^{\rho}$ pour $1 \leqslant k \leqslant s$ et $|x_{s+j}| < e^{\frac{\rho}{2}}$ pour $1 \leqslant j \leqslant t$, pour tout $x \in S$ (cf. définitions (12) et (13), chap. II, § 3). Ainsi, l'ensemble S et par suite l'ensemble T sont bornés.

Nous considérerons à la place de l'ensemble T un autre ensemble, lié à T, défini par des conditions plus simples.

LEMME 2. — *Si ε est une unité du corps* K, *les volumes des ensembles de $\mathcal{R}^n$ sont invariants par la transformation linéaire $x \to x\varepsilon(\varepsilon)$.*

En effet, par une transformation linéaire non singulière de l'espace euclidien, le volume d'un ensemble est multiplié par la valeur absolue du déterminant de cette transformation linéaire (cf. formule (2), chap. II, § 4). D'après ce qui a été établi dans le chapitre II, § 3-1), le déterminant de la transformation $x \to x\varepsilon(\varepsilon)$ est égal à $N(x(\varepsilon)) = \pm 1$; d'où notre affirmation.

Désignons maintenant, comme ci-dessus, par ζ la racine $m^{\text{ième}}$ de 1 telle que $\sigma_1(\zeta) = \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m}$. Considérons les ensembles T_k ($k = 0, 1, \ldots, m-1$) qui sont les images de T par les transformations linéaires $x \to x\varepsilon(\zeta^k)$ ($T_0 = T$). D'après le lemme 2, on a vu $v(T_k) = v(T)$ (si l'un au moins de ces volumes existe). Puisque

$$|N(x\varepsilon(\zeta^k))| = |N(x)N(\zeta^k)| = |N(x)|,$$
$$l(x\varepsilon(\zeta^k)) = l(x) + l(\zeta^k) = l(x),$$
$$\arg (x\varepsilon(\zeta^k))_1 = \arg x_1 + \frac{2\pi}{m} k,$$

alors (cf. définition du domaine fondamental X, point 1)) l'ensemble T_k est formé des points $x \in \mathcal{R}^n$ tels que

1° $$0 < |N(x)| \leqslant 1;$$

2° dans la décomposition (13), les coefficients ξ_i satisfont aux inégalités

$$0 \leqslant \xi < 1;$$

3° $$\frac{2\pi k}{m} \leqslant \arg x_1 < \frac{2\pi}{m}(k+1).$$

Il en résulte que $T_0, T_1, \ldots, T_{m-1}$ sont deux à deux disjoints et que leur réunion $\bigcup_{k=0}^{m-1} T_k$ est définie par les conditions 1° et 2° (sans la condition 3°).

Désignons par $\overline{T}$ l'ensemble des points $x \in \bigcup_{k=0}^{m-1} T_k$ tels que $x_1 > 0, \ldots, x_s > 0$ (cf. (2), chap. II, § 3). Fixons arbitrairement s signes $\delta_1, \ldots, \delta_s$ ($\delta_i = \pm 1$); la multiplication des points de $\mathcal{R}^n$ par le point $(\delta_1, \ldots, \delta_s; 1, \ldots, 1) \in \mathfrak{L}^{s,t} = \mathcal{R}^n$ est une transformation linéaire de $\mathcal{R}^n$ qui ne change pas le volume des ensembles (puisque la norme de ce point est égale à ± 1). Transformant l'ensemble $\overline{T}$ par toutes ces transformations linéaires, nous obtenons 2^s ensembles deux à deux disjoints et dont la réunion est égale à $\bigcup_{k=o}^{m-1} T_k$. Si nous démontrons que $\overline{T}$ a un volume v non nul, alors il en résultera l'existence du volume de T, donné par la formule

$$u(T) = \frac{2^s}{m} v. \tag{14}$$

(Pour un corps quadratique réel, $\overline{T}$ est la partie de T située dans le premier quadrant; pour un corps quadratique imaginaire, $\overline{T}$ coïncide avec le disque unité privé de son centre, cf. fig. 7 et 8).

L'égalité vectorielle (13) est équivalente aux égalités suivantes :

$$l_j(x) = \frac{e_j}{n} \operatorname{Log} |N(x)| + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k) \quad (j = 1, \ldots, s+t),$$

avec $e = 1$ si $1 \leqslant j \leqslant s$ et $e_j = 2$ si $s+1 \leqslant j \leqslant s+t$.

Effectuons le changement de variable indiqué par les formules

$$\left.\begin{aligned} x_k &= \rho_k & k &= 1, \ldots, s \\ y_j &= \rho_{s+j} \cos \varphi_j \\ z_j &= \rho_{s+j} \sin \varphi_j \end{aligned}\right\} \quad (j = 1, \ldots, t)$$

(avec les notations du chapitre II, § 3-1)), les nombres réels y et z_j sont définis par les égalités $x_{s+j} = y_j + iz_j$, $1 \leqslant j \leqslant t$. Le jacobien de cette transformation est égal à $\rho_{s+1} \ldots \rho_{s+t}$. Puisque $l_j(x) = \operatorname{Log} \rho_j^{e_j}$ et

$$N(x) = \prod_{j=1}^{s+t} \rho_j^{e_j}$$

(nous supposons $x_1 > 0, \ldots, x_s > 0$), alors, pour ces nouvelles variables $\rho_1, \ldots, \rho_{s+t}, \varphi_1, \ldots, \varphi_t$, l'ensemble Test défini par les conditions

$$1)\ \rho_1 > 0, \ \ldots, \ \rho_{s+t} > 0, \ \prod_{j=1}^{s+t} \rho_j^{e_j} \leqslant 1 ;$$

2) dans les égalités

$$\operatorname{Log} \rho_j^{e_j} = \frac{e_j}{n} \operatorname{Log}\left(\prod_{i=1}^{s+t} \rho_i\right) + \sum_{k=1} \xi_k l_j(\varepsilon_k)$$

$(j = 1, \ldots, s+t)$, les coefficients ξ_k satisfont aux inégalités

$$0 \leqslant \xi_k < 1 \qquad (k = 1, \ldots, r).$$

Puisque ces conditions n'imposent rien aux variables $\varphi_1, \ldots, \varphi_t$, chacune d'entre elles parcourt (indépendamment des autres) l'intervalle $[0, 2\pi]$. A la place de $\rho_1, \ldots, \rho_{s+t}$, introduisons maintenant de nouvelles variables ξ, $\xi_1, \ldots, \xi_r$ par les formules

$$\operatorname{Log} \rho_j^{e_j} = \frac{e_j}{n} \operatorname{Log} \xi + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k) \qquad (j = 1, \ldots, s+t) \tag{15}$$

Ajoutant toutes ces égalités et remarquant que

$$\sum_{j=1}^{s+t} e_j = n, \qquad \sum_{i=1}^{s+t} l_j(\varepsilon_k) = 0, \tag{16}$$

nous obtenons

$$\xi = \prod_{j=1}^{s+t} \rho_j^{e_j}. \tag{17}$$

L'ensemble $\overline{T}$ est maintenant défini par les conditions

$$0 < \xi \leqslant 1, \qquad 0 \leqslant \xi_k < 1 \qquad (k = 1, \ldots, r).$$

L'existence du volume $\bar{v} = v(\overline{T})$ est maintenant évidente. Puisque

$$\frac{\partial \rho_j}{\partial \xi} = \frac{\rho_j}{n\xi}, \qquad \frac{\partial \rho_j}{\partial \xi_k} = \frac{\rho_j}{e_j} l_j(\varepsilon_k),$$

le **jacobien** de la transformation (15) est égal à

$$J = \begin{vmatrix} \frac{\rho_1}{n\xi} & \frac{\rho_1}{e_1} l_1(\varepsilon_1) & \ldots & \frac{\rho_1}{e_1} l_1(\varepsilon_r) \\ \cdot & \cdot & \cdot & \cdot \\ \frac{\rho_{s+t}}{n\xi} & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\varepsilon_1) & \ldots & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\varepsilon_r) \end{vmatrix} = \frac{\rho_1 \ldots \rho_{s+t}}{n\xi 2^t} \begin{vmatrix} e_1 & l_1(\varepsilon_1) & \ldots & l_1(\varepsilon_r) \\ \cdot & \cdot & \cdot & \cdot \\ e_{s+t} & l_{s+t}(\varepsilon_1) & \ldots & l_{s+t}(\varepsilon_r) \end{vmatrix}$$

Ajoutons dans ce dernier déterminant toutes les lignes à la première. Tenant compte de (16) et (17) et de la définition du régulateur R du corps K (cf. chap. II, § 4, 4)), nous obtenons

$$|J| = \frac{R}{2^t \rho_{s+1} \dots \rho_{s+t}}.$$

Il est maintenant facile de calculer le volume $\bar{v}$:

$$\begin{aligned}
\bar{v} &= \int \dots \int dx_1 \dots dx_s dy_1 dz_1 \dots dy_t dz_t \\
&= \int_{(\bar{T})} \dots \int \rho_{s+1} \dots \rho_{s+t} d\rho_1 \dots d\rho_{s+t} d\varphi_1 \dots d\varphi_t \\
&= \int_{(\bar{T})} \int_0^{2\pi} d\varphi_1 \dots \int_0^{2\pi} d\varphi_t \int \dots \int \rho_{s+1} \dots \rho_{s+t} d\rho_1 \dots d\rho_{s+t} \\
&= 2^t \pi^t \int \dots \int |J| \rho_{s+1} \dots \rho_{s+t} d\xi d\xi_1 \dots d\xi_r \\
&= \pi^t R \int_0^1 d\xi \int_0^1 d\xi_1 \dots \int_0^1 d\xi_r = \pi^t R.
\end{aligned}$$

Substituant dans (14) la valeur obtenue pour $\bar{v}$, nous obtenons finalement :

$$v(T) = \frac{2^s \pi^t R}{m}.$$

4) Principe de Dirichlet

Considérons tout d'abord la fonction $\zeta_K(s)$ dans le cas où K est le corps Q des nombres rationnels. Puisque dans le corps Q on peut identifier les diviseurs entiers aux nombres entiers naturels n, d'où N(n) = n, alors

$$\zeta_Q(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{18}$$

Ainsi, pour le corps des nombres rationnels, la fonction zêta de Dedekind coïncide avec la fonction $\zeta(s)$ de Riemann. Démontrons que pour $s > 1$ la série (18) converge. Puisque la fonction $\frac{1}{x^s}$ est décroissante pour $x > 0$, alors

$$\int_n^{n+1} \frac{dx}{x^s} < \frac{1}{n^s} < \int_{n-1}^{n} \frac{dx}{x^s},$$

l'inégalité de gauche ayant lieu pour $n \geqslant 1$ et celle de droite pour $n \geqslant 2$. Pour tout entier naturel $N > 1$, nous obtenons donc

$$\int_1^{N+1} \frac{dx}{x^s} < \sum_{n=1}^{N} \frac{1}{n^s} < 1 + \int_1^N \frac{dx}{x^s}.$$

Puisque pour $s > 1$ l'intégrale $\int_1^{\infty} \frac{dx}{x^s}$ est convergente, l'inégalité de droite démontre la convergence de la série (18). De plus, pour $s > 1$, nous avons

$$\int_1^{\infty} \frac{dx}{x^s} < \zeta(s) < 1 + \int_1^{\infty} \frac{dx}{x^s},$$

ou

$$\frac{1}{s-1} < \zeta(s) < 1 + \frac{1}{s-1}.$$

Multipliant ces inégalités par $s - 1$, puis faisant tendre s vers l'unité, nous obtenons l'importante relation

$$\lim_{s \to 1+0} (s-1)\zeta(s) = 1, \tag{19}$$

qui donne l'ordre de croissance de la fonction $\zeta(s)$ pour $s \to 1$.

Démontrons maintenant un théorème analytico-géométrique, dû à Dirichlet, sur les séries.

Soient donnés un cône X de l'espace et une fonction F(x) à valeurs réelles positives définie sur X (nous considérerons que le point (0, . . ., 0) n'appartient pas au cône X). Nous ferons les hypothèses suivantes sur le cône X et la fonction F :

1° pour tout point $x \in X$ et pour tout nombre réel $\xi > 0$, on a l'égalité

$$F(\xi x) = \xi^n F(x);$$

2° l'ensemble T formé des points $x \in X$ tels que $F(x) \leqslant 1$ est borné et a un volume n-dimensionne1 non nul $v = v(T)$.

Les points du cône tels que F(x) = 1 forment une surface qui coupe toute demi-droite du cône en un seul point et limite une partie bornée du cône, de volume non nul. Il est clair que la donnée d'une telle surface dans X équivaut à la donnée de la fonction F(x).

Supposons donné dans $\mathcal{R}^n$ un lattice n-dimensionne1 $\mathcal{M}$ dont le volume du parallélépipède fondamental est égal à A. Considérons la série

$$\tilde{\zeta}(s) = \sum_{x \in \mathcal{M} \cap X} \frac{1}{F(x)^s}, \qquad s > 1, \tag{20}$$

où la sommation est étendue à tous les points x du lattice $\mathcal{M}$ qui appartiennent au cône X. Ainsi, cette série dépend du cône X, de la fonction F et du lattice $\mathcal{M}$.

THÉORÈME 3. — *Avec les définitions et les hypothèses ci-dessus, la série (20) est convergente pour tout $s > 1$ et*

$$\lim_{s \to 1+0} (s-1)\tilde{\zeta}(s) = \frac{v}{\Delta}. \tag{21}$$

DÉMONSTRATION. — Pour tout nombre réel $r > 0$, désignons par $\mathcal{M}_r$ le lattice déduit de $\mathcal{M}$ par homothétie de rapport $\frac{1}{r}$. Le volume du parallélépipède fondamental du lattice $\mathcal{M}_r$ est égal à $\frac{\Delta}{r^n}$. Si $N(r)$ est le nombre de points du lattice $\mathcal{M}_r$ contenus dans l'ensemble T, on a, par définition du volume,

$$v = v(T) = \lim_{r \to \infty} N(r) \frac{\Delta}{r^n} = A \lim_{r \to \infty} \frac{N(r)}{r^n}. \tag{22}$$

Considérons l'ensemble rT homothétique de T par l'homothétie de rapport r. Il est clair que $N(r)$ est aussi égal au nombre de points du lattice $\mathcal{M}$ contenus dans rT et ce nombre est à son tour égal au nombre de points $x \in \mathcal{M} \cap X$ tels que $F(x) \leqslant r^n$. Tous les points de $\mathcal{M} \cap X$ s'ordonnent en une suite $\{ x_k \}$ telle que

$$0 < F(x_1) \leqslant F(x_2) \leqslant \ldots \leqslant F(x_k) \leqslant \ldots$$

Posons

$$\sqrt[n]{F(x_k)} = r_k.$$

Les points $x_1, \ldots, x_k$ appartiennent à l'ensemble $r_k T$; par suite, $N(r_k) \geqslant k$. De plus, pour tout $\varepsilon > 0$, le point x_k n'appartient pas à l'ensemble $(r_k - \varepsilon)T$, d'où $N(r_k - \varepsilon) < k$. Ainsi,

$$N(r_k - \varepsilon) < k \leqslant N(r_k),$$

d'où

$$\frac{N(r_k - \varepsilon)}{(r_k - \varepsilon)^n} \left(\frac{r_k - \varepsilon}{r_k}\right)^n < \frac{k}{r_k^n} \leqslant \frac{N(r_k)}{r_k^n}.$$

Passant à la limite pour $k \to \infty$, i. e. pour $r_k \to \infty$, et tenant compte de la formule (22), nous obtenons

$$\lim_{k \to \infty} \frac{k}{F(x_k)} = \frac{v}{\Delta}. \tag{23}$$

Comparons la série $\tilde{\zeta}(s) = \sum_{k=1}^{\infty} \frac{1}{F(x_k)^s}$ à la série (18). Puisque

$$\lim_{s\to\infty} \frac{k^s}{F(x_k)^s} = \left(\frac{v}{\Delta}\right)^s \neq 0,$$

la série (20) converge en même temps que la série (18) (pour $s > 1$, bien entendu). Soit ε un nombre réel positif aussi petit que l'on veut. D'après (23), nous avons

$$\left(\frac{v}{\Delta} - \varepsilon\right)\frac{1}{k} < \frac{1}{F(x_k)} < \left(\frac{v}{\Delta} + \varepsilon\right)\frac{1}{k}$$

pour tout entier assez grand $k \geqslant k_0$, d'où

$$\left(\frac{v}{\Delta} - \varepsilon\right)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s} < \sum_{k=k_0}^{\infty} \frac{1}{F(x_k)^s} < \left(\frac{v}{\Delta} + \varepsilon\right)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s}$$

pour tout $s > 1$. Multiplions cette inégalité par $s - 1$ et faisons tendre s vers 1 à droite. Puisque

$$\lim (s-1) \sum_{k=1}^{k_0-1} \frac{1}{k^s} = 0,$$

alors, d'après (19),

$$\lim_{s\to 1+0} (s-1) \sum_{k=k_0}^{\infty} \frac{1}{k^s} = 1.$$

Tenant compte du fait que

$$\lim_{s\to 1} (s-1) \sum_{k=1}^{k_0-1} \frac{1}{F(x_k)^s} = 0,$$

nous obtenons les inégalités

$$\frac{v}{\Delta} - \varepsilon \leqslant \lim_{s\to 1+0} (s-1)\tilde{\zeta}(s) \leqslant \lim_{s\to 1+0} (s-1)\tilde{\zeta}(s) \leqslant \frac{v}{\Delta} + \varepsilon,$$

ce qui démontre le théorème 3, puisque ε est quelconque.

Remarque. — Il est facile de mettre en évidence des analogies entre les égalités (21) et (22). Pour accentuer cette ressemblance, supposons que le

volume A du parallélépipède fondamental du lattice $\mathcal{M}$ soit égal à 1 et écrivons ces égalités sous la forme

$$\lim_{s \to 1+0} (s-1)\tilde{\zeta}(s) = v \tag{21'}$$

$$\lim_{r \to \infty} \frac{1}{r_n} \mathrm{N(r)} = v. \tag{22'}$$

Ces deux limites définissent le même nombre, à savoir le volume de l'ensemble T. La définition du volume par l'égalité (22') utilise les opérations suivantes : le lattice $\mathcal{M}$ est réduit r fois et on considère le nombre N(r) de points du lattice $\mathcal{M}_r$ contenus dans T. Ensuite, on multiplie le nombre N(r) par le volume $\frac{1}{r^n}$ du parallélépipède fondamental du lattice $\mathcal{M}_r$. Enfin, on prend la limite du produit $\frac{1}{r^n}$ $N(r)$ pour $r \to \infty$. Nous obtenons le volume dans l'égalité (21') par un procédé analogue. Ici la somme $\tilde{\zeta}(s)$ joue le rôle du nombre $N(r)$, le facteur $s-1$ correspond au facteur $\frac{1}{r^n}$ et on fait tendre s vers $1+0$ au lieu de faire tendre r vers l'infini.

Revenons au domaine fondamental X d'un corps K de nombres algébriques. Puisque la fonction $F(x) = |N(x)|$ satisfait aux conditions (1) et (2), on peut appliquer le théorème 3 à la série (8), ce qui montre que cette série est convergente pour $s > 1$ et que la relation (9) est satisfaite.

Ceci termine la démonstration de tous les résultats que nous avons utilisés dans le point 1) pour démontrer le théorème 2.

5) Identité d'Euler

Pour utiliser la formule (2) pour calculer le nombre h de classes de diviseurs, il faut être capable de calculer la limite $\lim_{s \to 1+0} (s-1)\zeta_K(s)$ par un autre procédé. Dans certains cas, cela pourra se faire en utilisant la représentation de $\zeta_K(s)$ sous forme d'un produit infini, connu sous le nom d'identité d'Euler.

THÉORÈME 4. — *Pour $s > 1$, la fonction $\zeta_K(s)$ peut se représenter sous forme du produit infini convergent*

$$\zeta_k(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}},$$

où $\mathfrak{p}$ parcourt tous les diviseurs premiers du corps K.

DÉMONSTRATION. — Pour tout diviseur premier $\mathfrak{p}$, nous avons

$$\frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} = 1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s}} + \cdots \tag{24}$$

Soit N un nombre naturel quelconque et soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ tous les diviseurs premiers dont la norme ne dépasse pas N. Multipliant les séries absolument convergentes (24) pour $\mathfrak{p} = \mathfrak{p}_1, \ldots, \mathfrak{p}_r$, nous obtenons

$$\prod_{N(\mathfrak{p}) \leqslant N} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{k_1, \ldots, k_r = 0}^{\infty} \frac{1}{N\left(\mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_r^{k_r}\right)^s} = \sum_{\mathfrak{a}}{}' \frac{1}{N(\mathfrak{a})^s},$$

où, dans la somme Σ', a parcourt tous les diviseurs entiers du corps $\mathbf{K}$ dont la décomposition en produit de puissances de diviseurs premiers contient seulement des diviseurs premiers dont la norme ne dépasse pas N. Comparons la somme Σ' à la série $\zeta_{\mathbf{K}}(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$. Puisque dans la série Σ' on rencontre tous les diviseurs premiers dont la norme est $\leqslant$ N, on a

$$\left| \prod_{N(\mathfrak{p}) \leqslant N} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} - \zeta_{\mathbf{K}}(s) \right| < \sum_{N(\mathfrak{a}) > N} \frac{1}{N(\mathfrak{a})^s}.$$

Puisque pour $s > 1$ la série (1) est convergente, alors

$$\sum_{N(\mathfrak{a}) > N} \frac{1}{N(\mathfrak{a})^s} \to 0$$

pour $N \to \infty$ et cela démontre le théorème.

L'importance du théorème 4 réside dans le fait que, réuni au théorème 2, il établit un lien entre le nombre h et les diviseurs premiers du corps K. Comme on l'a déjà remarqué dans le point 1), si nous connaissons tous les diviseurs premiers du corps K, alors, en utilisant le théorème 4, on peut calculer par un autre procédé la partie gauche de la relation (2) et cela nous donne une formule explicite pour h. D'autre part, le fait que $\varkappa h \neq 0$ permet d'obtenir d'importants résultats sur les diviseurs premiers du corps K; par exemple, prenant pour $\mathbf{K}$ un corps cyclotomique, nous obtiendrons, dans le § 3 de ce chapitre, le théorème de Dirichlet sur l'infinité des nombres premiers rationnels dans une progression arithmétique.

EXERCICES

1. En utilisant la convergence de la série $\sum_{n=1}^{\infty} \frac{1}{n^s}$ $(s>1)$, démontrer que, pour $s>1$, la série

$$\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s},$$

où $\mathfrak{p}$ parcourt tous les diviseurs premiers du corps K, est aussi convergente.

2. En utilisant les résultats de l'exercice 1, démontrer la convergence du produit

$$\prod_{\mathfrak{p}} \frac{1}{1-\frac{1}{N(\mathfrak{p})}} \qquad (s>1).$$

En déduire la convergence de la série $\sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$.

3. Soient a_k et b_k $(k \geqslant 1)$ des nombres réels positifs tels que $\lim_{k\to\infty} \frac{b_k}{a_k} = c$. Démontrer que si la série $\sum_{k=1}^{\infty} a_k^s$ est convergente pour $s>1$ et

$$\lim_{s\to 1+0} (s-1)\sum_{k=1}^{\infty} a_k^s = A,$$

alors la série $\sum_{k=1}^{\infty} b_k^s$ converge aussi (pour $s>1$) et on a

$$\lim_{s\to 1+0} (s-1)\sum_{k=1}^{\infty} b_k^s = cA.$$

4. Soit C une classe quelconque de diviseurs d'un corps K de nombres algébriques. Désignons par $Z(\xi, C)$ le nombre de diviseurs entiers a de la classe C tels que $N(a) \leqslant \xi$. Démontrer que

$$\lim_{\xi\to\infty} \frac{Z(\xi, C)}{\xi} = \kappa = \frac{2^{s+t}\pi^t R}{m\sqrt{|D|}}.$$

5. Désignons par $\psi(a)$ le nombre des diviseurs entiers d'un corps K de nombres algébriques dont la norme est égale à a. Démontrer que

$$\frac{\zeta_K(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

avec

$$c_n = \sum_{d|n} \mu(d)\psi\left(\frac{n}{d}\right)$$

($\mu(a)$ est la fonction de Moëbius).

§ 2. — LE NOMBRE DE CLASSES DE DIVISEURS D'UN CORPS CYCLOTOMIQUE

Soient m un entier naturel et ζ une racine primitive $m^{\text{ième}}$ de l'unité. Puisque toutes les racines $m^{\text{ième}}$ de 1 divisent le cercle unité du plan complexe en m parties égales, le corps $\mathbf{Q}(\zeta)$ est appelé ***le corps de division du cercle en m parties égales*** ou plus simplement $m^{\text{ième}}$ ***corps cyclotomique.*** Dans ce paragraphe, nous calculerons le nombre h des classes de diviseurs des corps cyclotomiques en utilisant les théorème 2 et 4 du § 1. Dans ce but, il faut d'abord étudier la décomposition de tout nombre premier rationnel en produit de diviseurs premiers dans ce corps. Nous calculerons tout d'abord le degré du corps $\mathbf{Q}(\zeta)$.

1) Irréductibilité des polynômes cyclotomiques

Comme on le sait, le degré du corps $\mathbf{Q}(\zeta)$ est égal au degré du polynôme minimal du nombre ζ sur le corps Q des nombres rationnels. Nous démontrerons ici que le polynôme minimal du nombre ζ est le polynôme

$$\Phi_m = \Phi_m(t) = \prod_{(k,m)=1} (t - \zeta^k)$$

(le produit est étendu à un système réduit de résidus modulo m), dont les racines sont toutes les racines primitives $m^{\text{ièmes}}$ de 1. Puisque le degré de Φ_m est égal à la valeur $\varphi(m)$ de la fonction d'Euler, il en résulte que

$$(\mathbf{Q}(\zeta) : \mathbf{Q}) = \varphi(m).$$

Le polynôme $\Phi_m(t)$ est appelé ***polynôme de division du cercle en m parties égales ou*** $m^{\text{ième}}$ ***polynôme cyclotomique.***

Démontrons tout d'abord que les coefficients de Φ_m sont des entiers rationnels. C'est évident pour $m = 1$ ($\Phi_1 = t - 1$). La démonstration dans le cas général s'effectue par récurrence sur m. Puisque toute racine $m^{\text{ième}}$ de 1 est une racine primitive de degré $d \mid m$, alors

$$t^m - 1 = \prod_d \Phi_d,$$

où d parcourt tous les diviseurs du nombre m. Par hypothèse de récurrence, le polynôme $F = \prod_{d \neq m} \Phi_d$ a des coefficients entiers rationnels et son

coefficient dominant est égal à 1. Par suite, $\Phi_m = \frac{t^m - 1}{F}$ a aussi des coefficients entiers rationnels.

Désignons comme toujours par Z l'anneau des entiers rationnels, par $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ le corps résiduel modulo un nombre premier p et par $\bar{a}$ la classe résiduelle de a dans $\mathbf{Z}/p\mathbf{Z}$. Si dans le polynôme $f(t)$ à coefficients entiers rationnels, nous remplaçons tous les coefficients par leurs classes résiduelles modulo p, nous obtenons un polynôme $\bar{f}(t)$ à coefficients dans le corps $\mathbf{F}_p$. Il est clair que l'application $f \to \bar{f}$ est un homomorphisme de l'anneau $Z[t]$ sur l'anneau $\mathbf{F}_p[t]$. Puisque $(\bar{f} + \bar{g})^p = \bar{f}^p + g^p$ et, d'après le petit théorème de Fermat, $\bar{a}^p = \bar{a}$ (a $\in$ Z), on a identiquement dans l'anneau $\mathbf{F}_p[t]$

$$(\bar{f}(t))^p = \bar{f}(t^p). \tag{1}$$

Posons $h = t^m - 1$. Si le nombre premier p ne figure pas dans m, alors le polynôme $\bar{h}$ de $\mathbf{F}_p[t]$ est premier avec son polynôme dérivé et par suite ne contient] pas de facteurs multiples. Remarquant maintenant que $\bar{\Phi}_m$ est un diviseur de $\bar{h}$, nous avons obtenu le résultat suivant.

LEMME 1. — *Si le nombre premier rationnel p ne divise pas m, alors le polynôme Φ_m de l'anneau $\mathbf{F}_p[t]$ ne contient pas de facteurs multiples.*

Si $f(t)$ est le polynôme minimal du nombre ζ, alors $\Phi_m = f$ G où G appartient, comme f, à l'anneau $Z[t]$. Pour tout nombre premier p premier avec m, le nombre ζ^p est aussi une racine primitive $m^{\text{ième}}$ de 1, i. e. $\Phi_m(\xi^p) = 0$. Démontrons que ζ^p est une racine de f. Dans le cas contraire, $G(\zeta^p) = 0$. Considérons alors le polynôme H(t) = $G(t^p)$. Puisque $H(\zeta) = G(\zeta^p) = 0$, alors H est divisible par f, i. e. H = f Q, où Q $\in$ $Z[t]$. Passons au corps résiduel $\mathbf{F}_p$ dans l'égalité H = fQ. Nous obtenons H = f Q. Mais, d'après (1), $\bar{H}(t) = \bar{G}(t^p) = (G(t))^p$, d'où

$$G^p = \bar{f}\bar{Q}.$$

Soit $\bar{\psi}$ un certain facteur irréductible du polynôme $\bar{f}$ (dans l'anneau $\mathbf{F}^p[t]$). Il résulte de la dernière égalité que G est divisible par $\bar{\psi}$. Mais alors, il résulte de l'égalité $\bar{\Phi}_m = f$ G que Φ_m est divisible par $\bar{\psi}^2$, en contradiction avec le lemme 1. Ainsi, ζ^p n'est pas une racine de $G(t)$ et par suite c'est une racine de $f(t)$.

Si maintenant ζ' est une racine quelconque de Φ_m, alors $\zeta' = \zeta^k$, où k est premier avec m. Posons $k = p_1 p_2 \ldots p_s$. D'après ce qui précède, ζ^{p_1} est une racine de $f(t)$. Remplaçant la racine ζ par ζ^{p_1}, nous obtiendrons de même que $\zeta^{p_1 p_2}$ est une racine de $f(t)$. De proche en proche, nous obtenons finalement que ζ^k est également une racine de $f(t)$.

Ainsi, chaque racine du polynôme Φ_m est aussi une racine du polynôme f, d'où $\Phi_m = f$. Nous formulerons ce résultat comme suit.

THÉORÈME 1. — ***Pour tout entier naturel m, le polynôme cyclotomique*** Φ_m ***est irréductible sur le corps des nombres rationnels.***

COROLLAIRE. — ***Le degré du*** $m^{\text{ième}}$ ***corps cyclotomique*** $\mathbf{Q}(\zeta)$, $\zeta^m = 1$, ***est égal à*** $\varphi(m)$ ***(où*** $\varphi(m)$ ***est la fonction d'Euler).***

2) Loi de décomposition dans un corps cyclotomique

Puisque le degré du $m^{\text{ième}}$ corps cyclotomique $\mathbf{Q}(\zeta)$ est égal à $\varphi(m)$, alors les nombres

$$1, \zeta, \ldots, \zeta^{\varphi(m)-1} \tag{2}$$

forment une base de $\boldsymbol{Q(C)}$ sur $\boldsymbol{Q}$.

LEMME *2.* — ***Si le nombre premier p ne figure pas dans m, alors il ne figure pas non plus dans le discriminant*** $\mathrm{D} = \mathrm{D}(1, \zeta, \ldots, \zeta^{\varphi(m)-1})$ ***de la base (2).***

DÉMONSTRATION. — Comme nous le savons, le discriminant D est égal au discriminant $\mathrm{D}(\Phi_m)$ du polynôme cyclotomique Φ_m. La classe résiduelle $\overline{\mathrm{D}(\Phi_m)} \in \mathbf{F}_p$ du nombre $\mathrm{D}(\Phi_m)$ modulo p est égale évidemment au discriminant $\mathrm{D}(\overline{\Phi}_m)$ du polynôme $\overline{\Phi}_m \in \mathbf{Z}_p[t]$. Puisque $\overline{\Phi}_m(t)$ n'a pas de facteurs multiples (lemme 1), on a $\mathrm{D}(\overline{\Phi}_m) \neq 0$ et par suite $\mathrm{D} = \mathrm{D}(\overline{\Phi}_m)$ n'est pas divisible par p.

LEMME *3.* — ***Si un corps*** K ***de nombres algébriques contient une racine primitive*** $m^{\text{ième}}$ ***de*** 1, ***alors, pour tout diviseur premier*** $\mathfrak{p}$ ***du corps*** K, ***premier avec m, on a***

$$\mathrm{N}(\mathfrak{p}) \equiv 1 \pmod{m}.$$

DÉMONSTRATION. — Soient $\mathfrak{D}$ l'anneau des nombres entiers du corps K, p un nombre rationnel divisible par $\mathfrak{p}$ et ζ une racine primitive $m^{\text{ième}}$ de 1 ($\zeta \in \mathfrak{D}$). Dans le point 1), nous avons vu que le polynôme $t^m - 1$ n'a pas de racines multiples dans le corps résiduel $\mathfrak{D}/\mathfrak{p}$ qui est une extension du corps $\mathbf{F}_p$ (puisque $p \nmid m$). Par suite, les classes résiduelles $1, \zeta, \ldots, \overline{\zeta}^{m-1}$ de $\mathfrak{D}/\mathfrak{p}$ sont deux à deux distinctes. Il est clair que ces classes forment un groupe multiplicatif d'ordre m qui est un sous-groupe du groupe multiplicatif du corps résiduel $\mathfrak{D}/\mathfrak{p}$. L'ordre de ce dernier groupe est égal à $\mathrm{N}(\mathfrak{p}) - 1$. Mais l'ordre de tout groupe fini est divisible par l'ordre de chacun de ses sous-groupes et par suite $\mathrm{N}(\mathfrak{p}) - 1$ est divisible par m.

THÉORÈME 2. — *p* étant un ***nombre premier ne figurant pas dans m, désignonsparf lepluspetit entier naturel tel quepf*** $\equiv 1 \pmod{m}$ ***et soit*** $g = \frac{\varphi(m)}{f}$. ***Alors, dans le corps cyclotomique*** $\mathbf{Q}(\zeta)$, ***p admet la décomposition***

$$P = \mathfrak{p}_1 \dots \mathfrak{p}_g, \tag{3}$$

où les diviseurs premiers $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ ***sont deux à deux distincts et*** $N(\mathfrak{p}_i) = p^f$.

DÉMONSTRATION. — Puisque $(p, m) = 1$, alors, d'après le lemme 2, *p ne* figure pas dans le discriminant de la base (2); par suite, d'après le théorème 8 du chapitre III, § 5, *p* admet une décomposition de la forme (3). Il nous reste seulement à trouver le degré de chaque diviseur $\mathfrak{p}_i$ et à démontrer que le nombre des $\mathfrak{p}_i$ est égal à $\frac{\varphi(m)}{f}$.

Soient $\mathfrak{p}$ un quelconque des diviseurs premiers $\mathfrak{p}_i$, s son degré, i. e. $N(\mathfrak{p}) = p^s$. D'après le lemme 3, $p^s \equiv 1 \pmod{m}$ d'où $s \geqslant f$. Pour démontrer l'inégalité contraire, considérons le corps résiduel $\mathfrak{D}/\mathfrak{p}$ de l'anneau $\mathfrak{D}$ des nombres entiers du corps $\mathbf{Q}(\zeta)$ modulo p. D'après le corollaire du lemme du chapitre III, § 7-4), toute classe résiduelle de $\mathfrak{D}/\mathfrak{p}$ contient un représentant de la forme

$$\xi = \sum_{j=0}^{\varphi(m)-1} a_j \zeta^j, \tag{4}$$

où les a_j sont des nombres entiers rationnels. Élevons (4) à la puissance p^f. Puisque $p^f \equiv 1 \pmod{m}$, alors $\zeta^{p^f} = \zeta$. Tenant compte du fait que

$$(\alpha + \beta)^{p^f} \equiv \alpha^{p^f} + \beta^{p^f} \pmod{\mathfrak{p}}$$

pour tout α et β dans $\mathfrak{D}$ et du fait que $a^{p^f} \equiv a \pmod{\mathfrak{p}}$ pour tout entier rationnel a, nous obtenons, à partir de (4), la congruence :

$$\xi^{p^f} \equiv \xi \pmod{\mathfrak{p}}.$$

Ainsi, toute classe résiduelle $\xi \in \mathfrak{D}/\mathfrak{p}$ est une racine du polynôme $t^{p^f} - t$. Mais le nombre de racines d'un polynôme dans un corps ne dépasse pas son degré, d'où $p^s \leqslant p^f$, ce qui signifie $s \leqslant f$. Réunissant cette inégalité à celle obtenue ci-dessus, nous obtenons $s = f$.

Nous avons ainsi démontré que tous les diviseurs premiers $\mathfrak{p}_i$ dans la décomposition (3) ont le même degré f, égal à l'exposant de p modulo m. Appliquant maintenant le théorème 8 du chapitre III, § 5, nous obtenons que le nombre g des diviseurs premiers $\mathfrak{p}_i$ est égal à $\frac{\varphi(m)}{f}$. Le théorème 2 est démontré.

3) Expression de h au moyen des séries L

Revenons sur la fonction $\zeta_K(s)$ du $m^{\text{ième}}$ corps cyclotomique $K = \mathbf{Q}(\zeta)$, $\zeta^m = 1$. Utilisant l'identité d'Euler (§ 1, théorème 4) et réunissant dans celle-ci tous les facteurs p qui divisent un même nombre premier rationnel, on peut écrire

$$\zeta_K(s) = \prod_p \prod_{\mathfrak{p}|p} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}, \tag{5}$$

le produit extérieur étant étendu à tous les nombres premiers rationnels p. Les facteurs correspondant à des diviseurs premiers $\mathfrak{p}$ qui divisent m forment un produit fini que nous désignerons par

$$G(s) = \prod_{\mathfrak{p}|m} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}. \tag{6}$$

Si $(p, m) = 1$, alors, pour tout diviseur premier $\mathfrak{p}$ qui divise p, nous avons $N(\mathfrak{p}) = p^{f_p}$, où f_p est l'exposant du nombre p modulo m. Puisque le nombre des diviseurs $\mathfrak{p}$ distincts qui divisent p est égal à $\frac{\varphi(m)}{f_p}$ (théorème 2), nous obtenons

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} \left(1 - \frac{1}{p^{f_p s}}\right)^{\frac{\varphi(m)}{f_p}}. \tag{7}$$

Transformons chaque facteur de ce produit. Pour cela, nous utiliserons la décomposition

$$1 - \left(\frac{1}{p^s}\right)^{f_p} = \prod_{k=0}^{f_p - 1} \left(1 - \frac{\varepsilon^k}{p^s}\right), \tag{8}$$

où $\varepsilon = \varepsilon_p = \cos \frac{2\pi}{f_p} + i \sin \frac{2\pi}{f_p}$. Maintenant le produit

$$\prod_{k=0}^{f_p - 1} \left(1 - \frac{\varepsilon_p^k}{p^s}\right)^{-\frac{\varphi(m)}{f_p}}$$

contient $\varphi(m)$ facteurs et ce nombre de facteurs est le même pour tout p. Montrons que, pour des p différents, on peut associer les facteurs ci-dessus de telle sorte que le produit infini qui figure dans la partie droite de l'égalité (7) se décompose en un produit de $\varphi(m)$ facteurs de forme assez simple. Cette décomposition repose sur la notion de caractère modulo m. Nous

aurons besoin maintenant des résultats sur les caractères exposés dans le § 5 de l'appendice.

Désignons par G_m le groupe des classes résiduelles de l'anneau des entiers rationnels modulo m qui sont constitués de nombres premiers avec m. La classe $\bar{p}$, de représentant p qui appartient à G_m, est d'ordre f_p; par suite, pour tout caractère χ du groupe G_m, la valeur $\chi(\bar{p})$ qui est une racine de 1 d'ordre f_p, est égale à un certain ε^k. Réciproquement, choisissant arbitrairement une des racines ε^k, il existe sur le sous-groupe cyclique $\{\bar{p}\}$ du groupe G_m un caractère χ_1 et un seul tel que $\chi_1(\bar{p}) = \varepsilon^k$. D'après le théorème du § 5 de l'appendice, on peut prolonger ce caractère χ_1 en un caractère du groupe G_m. Ainsi, si χ parcourt tous les caractères du groupe G_m, $\chi(\bar{p})$ parcourt **toutes** les racines ε^k ($k = 0, 1, \ldots, f_p - 1$); chacune des racines ε^k est obtenue exactement $\frac{\varphi(m)}{f_p}$ fois. Substituant l'expression (8) dans la formule (7), nous obtenons donc

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} \prod_{\chi} \left(1 - \frac{\chi(\bar{p})}{p^s}\right)^{-1} \tag{9}$$

(le produit intérieur est étendu à tous les caractères χ du groupe G_m).

A la place des caractères du groupe G_m, nous considérerons maintenant des caractères modulaires modulo m (cf. appendice, § 5-3)). Puisque $\chi(p) = 0$ pour tout p figurant dans m (pour tout caractère modulaire χ modulo m), on peut écrire l'égalité (9) sous la forme

$$\zeta_K(s) = G(s) \prod_{p} \prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

(où p parcourt tous les nombres premiers et χ tous les caractères modulaires modulo m). Intervertissant l'ordre des multiplications, nous obtenons

$$\zeta_K(s) = G(s) \prod_{\chi} L(s, \chi), \tag{10}$$

en utilisant la notation suivante :

$$L(s, \chi) = \prod_{p} \frac{1}{1 - \frac{\chi(p)}{p^s}}. \tag{11}$$

Remarquons que dans tout ce qui précède, on a supposé $s > 1$ (sous cette hypothèse, on peut effectuer toutes les opérations ci-dessus sur les produits infinis).

Remarque. — Dans la formule (10), on peut omettre le facteur G(s) en prenant pour χ les caractères primitifs modulo tout diviseur d de m; cf. à ce sujet les exercices 13 à 16.

Le facteur $L(s, \chi_0)$ du produit (10) qui correspond au caractère unité χ_0 ne diffère que par un facteur simple de la fonction $\zeta(s)$ de Riemann. En effet, puisque $\chi_0(p) = 1$ pour $(p, m) = 1$ et $\chi_0(p) = 0$ pour $(p, m) > 1$, alors

$$L(s, \chi_0) = \prod_{(p,m)=1} \frac{1}{1 - \frac{1}{p^s}} \qquad (s > 1).$$

D'autre part, appliquant le théorème 4 du § 1 au corps Q des nombres rationnels, nous obtenons

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Ainsi,

$$L(s, \chi_0) = \left(\prod_{p|m} \frac{1}{1 - \frac{1}{p^s}}\right)^{-1} \zeta(s).$$

Substituant cette expression dans (10), nous obtenons pour $\zeta_K(s)$ la formule définitive suivante :

$$\zeta_K(s) = F(s)\zeta(s)\prod_{\chi \neq \chi_0} L(s, \chi) \qquad (s > 1), \tag{12}$$

où nous avons posé (cf. (6))

$$F(s) = \prod_{\mathfrak{p}|m} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \cdot \prod_{p|m} \left(1 - \frac{1}{p^s}\right).$$

Étudions plus en détail les fonctions $L(s, \chi)$. Considérons la série

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

absolument convergente pour $s > 1$. Remplaçant la décomposition (24) du § 1 par l'égalité

$$\frac{1}{1 - \frac{\chi(p)}{p^s}} = \sum_{k=0}^{\infty} \left(\frac{\chi(p)}{p^s}\right)^k,$$

nous obtiendrons facilement, en répétant presque mot à mot la démonstration du théorème 4 du § 1 (en utilisant la propriété multiplicative du caractère χ), l'égalité

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \qquad (s > 1) \tag{13}$$

La série qui figure dans la partie droite de l'égalité (13) est appelée la ***série*** L ***ou série de Dirichlet,*** du caractère modulaire χ. Notre but immédiat sera de démontrer que la série L d'un caractère χ différent du caractère unité est convergente, non seulement pour $s > 1$ mais également pour $s > 0$ (bien sûr, la convergence n'est pas absolue dans l'intervalle $0 < s \leqslant 1$). Démontrons à cet effet le lemme suivant.

LEMME 4. — ***Soit*** $\{a_n\}$ $(n = 1, 2, \ldots)$ ***une suite de nombres complexes telle que les sommes*** $A_n = \sum_{k=1}^{n} a_k$ ***soient bornées,*** i. e. $|A_n| \leqslant c$ ***pour tout*** $n \geqslant 1$. ***Alors la série***

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

est convergente pour tout nombre réel $s > 0$. ***Pour tout*** $\sigma > 0$, ***la convergence est uniforme dans l'intervalle*** $[\sigma, \infty)$; ***par suite*** $f(s)$ ***est une fonction continue de*** s ***(dans le domaine de convergence*** $(0, \infty)$***).***

DÉMONSTRATION. — Fixons arbitrairement $\sigma > 0$. Pour $\varepsilon > 0$ donné, soit n_0 tel que $\frac{1}{n^\sigma} < \varepsilon$ pour tout $n > n_0$. Pour ces entiers $n > n_0$, on a également $\frac{1}{n^s} < \varepsilon$ pour tout $s \geqslant \sigma$. Soit maintenant $M > N > n_0$. *Alors*

$$\sum_{k=N}^{M} \frac{a_k}{k^s} = \sum_{k=N}^{M} \frac{A_k - A_{k-1}}{k^s} = \sum_{k=N}^{M} \frac{A_k}{k^s} - \sum_{k=N-1}^{M-1} \frac{A_k}{(k+1)^s}$$

$$= -\frac{A_{N-1}}{N^s} + \sum_{k=N}^{M-1} A_k \left(\frac{1}{k^s} - \frac{1}{(k+1)^s} \right) + \frac{A_M}{M^s},$$

d'où

$$\left| \sum_{k=N}^{M} \frac{a_k}{k^s} \right| \leqslant \frac{C}{N^s} + C \sum_{k=N}^{M-1} \left(\frac{1}{k^s} - \frac{1}{(k+1)^s} \right) + \frac{C}{M^s} = \frac{2c}{N^s} < 2C\varepsilon$$

pour tout s appartenant à l'intervalle $[\sigma, \infty)$. Le lemme 4 est démontré.

COROLLAIRE. — ***Pour tout caractère*** χ ***différent du caractère unité, la série de Dirichlet*** $L(s, \chi)$ ***est convergente pour*** $s > 0$ ***et est une fonction continue de*** s ***dans l'intervalle*** $(0, \infty)$.

En effet, si $\chi \neq \chi_0$, alors $\Sigma\chi(k) = 0$ quand k parcourt un système complet de résidus modulo m. Représentant tout entier naturel n sous la forme $n = mq + r$, $0 \leqslant r < m$, alors

$$A_n = \sum_{k=1}^{n} \chi(k) = \sum_{k=1}^{r} \chi(k), \text{ d ' o ù } |A_n| \leqslant r < m.$$

Revenons à la fonction $\zeta_K(s)$. Multipliant l'égalité (12) par $s - 1$ et passant à la limite pour $s \to 1 + 0$, nous obtenons, d'après la relation (19) du § 1,

$$\lim_{s \to 1+0} (s-1)\zeta_K(s) = F(1) \prod_{\chi \neq \chi_0} L(1, \chi), \tag{14}$$

avec

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}. \tag{15}$$

Remarquons que quand la série (15) n'est pas absolument convergente, on ne peut pas modifier l'ordre de ses termes. Rapprochant la formule (14) du théorème 2 du § 1, nous obtenons l'expression suivante de h

$$h = \frac{w\sqrt{|D|}}{2^{s+t}\pi^t R} F(1) \prod_{\chi \neq \chi_0} L(1, \chi) \tag{16}$$

(ici w désigne le nombre de racines de l'unité contenues dans K). On ne peut pas se limiter à l'expression (16) pour étudier le nombre de classes de diviseurs d'un corps cyclotomique puisqu'elle contient des séries infinies $L(1, \chi)$. Dans le point suivant, nous calculerons la somme de ces séries.

4) Sommation des séries $L(1, \chi)$

Supposant que χ est un caractère modulo m différent du caractère unité, revenons à la série (13). Omettant dans celle-ci les termes de la somme qui sont nuls et remarquant que $\chi(n_1) = \chi(n_2)$ pour $n_1 \equiv n_2 \pmod m$, nous pouvons l'écrire sous la forme suivante (on suppose ici de manière essentielle que $s > 1$) :

$$L(s, \chi) = \sum_{(x,m)=1} \chi(x) \sum_{n \equiv x \pmod m} \frac{1}{n^s}$$

(la sommation extérieure est étendue à un système réduit de résidus modulo m). Nous écrirons la série intérieure sous la forme

$$\sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

où

$$c_n = \begin{cases} 1 & \text{pour } n \equiv x \pmod m, \\ 0 & \text{pour } n \not\equiv x \pmod m. \end{cases}$$

Pour écrire les coefficients c_n sous forme plus convenable, nous utiliserons la formule évidente suivante :

$$\sum_{k=0}^{m-1} \zeta^{rk} = \begin{cases} m & \text{pour } r \equiv 0 \pmod m, \\ 0 & \text{pour } r \not\equiv 0 \pmod m \end{cases}$$

o ù

$$\zeta = \cos\frac{2\pi}{m} + i \sin\frac{2\pi}{m}$$

est une racine primitive $m^{\text{ième}}$ de 1. Remarquons que si dans l'étude algébrique d'un corps cyclotomique on peut prendre pour ζ une racine primitive $m^{\text{ième}}$ de 1 quelconque, ici, il nous faut fixer une de ces racines sans ambiguïté pour les calculs qui vont suivre. Nous avons donc

$$c_n = \frac{1}{m} \sum_{k=0}^{m-1} \zeta^{(x-n)k}.$$

Ainsi

$$L(s, \chi) = \sum_{(x,m)=1} \chi(x) \sum_{n=1}^{\infty} \frac{1}{m} \sum_{k=0}^{m-1} \zeta^{(x-n)k} \frac{1}{n^s} = \frac{1}{m} \sum_{k=0}^{m-1} \left(\sum_{(x,m)=1} \chi(x) \zeta^{xk} \right) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s}.$$

Nous avons déjà rencontré l'expression entre parenthèses, pour $m = p$ premier, dans le chapitre premier § 2, et nous l'avons appelée somme de Gauss. Donnons la définition des sommes de Gauss pour des entiers m quelconques.

DÉFINITION. — ***Soit ζ une racine primitive $m^{\text{ième}}$ fixée de 1 et soit χ un caractère modulaire modulo m. L'expression***

$$\tau_a(\chi) = \sum_{x \bmod m} \chi(x) \zeta^{ax},$$

où x parcourt un système complet (ou réduit) ***de résidus modulo m s'appelle une somme de Gauss relative au caractère χ et au nombre entier rationnel a.***

Une somme de Gauss $\tau_a(\chi)$ dépend ainsi non seulement de χ et du résidu de a modulo m mais aussi du choix de la racine primitive ζ. Nous supposerons dans la suite que l'on prend pour ζ la racine $\cos\frac{2\pi}{m} + i \sin\frac{2X}{m}$. La somme de Gauss qui correspond à cette valeur de ζ est dite ***normée.***

Nous désignerons aussi par $\tau(\chi)$ la somme $\tau_1(\chi)$.

Si le caractère χ n'est pas le caractère unité, alors

$$\tau_0(\chi) = \sum_{(x,m)=1} \chi(x) = 0.$$

Nous pouvons donc écrire l'expression obtenue ci-dessus pour $L(s, \chi)$ sous la forme

$$L(s, \chi) = \frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s}.$$

Nous pouvons maintenant appliquer le lemme 4 à la série $\sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n^s}$ ($\zeta^{-k} \neq 1$ pour $k \neq 0$, d'où $\sum_{n=1}^{m} \zeta^{-nk} = 0$). D'après ce lemme, notre série converge pour $0 < s < \infty$ et représente dans cet intervalle une fonction continue de s. Nous pouvons donc faire $s = 1$ dans la dernière égalité; nous obtenons ainsi

$$L(1, \chi) = \frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n}.$$

Pour trouver la somme de la série intérieure, considérons la série entière $\sum \frac{z^n}{n}$. On sait qu'elle converge dans le cercle $|z| < 1$ et y représente la branche de la fonction $-\operatorname{Log}(1 - z)$ dont la partie imaginaire (i. e. le coefficient de i) appartient à l'intervalle $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$. Puisque cette série entière converge au point $z = \zeta^{-k}$ (situé sur la circonférence unité), alors, d'après le théorème d'Abel,

$$\sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n} = -\operatorname{Log}(1 - \zeta^{-k}),$$

ce qui entraîne

$$L(1, \chi) = -\frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \operatorname{Log}(1 - \zeta^{-k}). \tag{17}$$

Nous avons ainsi obtenu une expression finie pour la série $L(1, \chi)$. La substituant dans (16), nous trouvons une formule, ne contenant plus de séries infinies, pour le nombre de classes de diviseurs d'un corps cyclotomique.

On peut encore simplifier la formule (17). Dans le point suivant, nous le ferons, non dans le cas général, mais pour des caractères χ primitifs. Nous

appliquerons ces résultats dans le § 5 au calcul de h pour un corps cyclotomique de division du cercle en un nombre premier de parties égales. Dans ce cas, la formule donnant h a de très nombreuses applications.

5) Les séries $L(1, \chi)$ dans le cas des caractères primitifs

Démontrons que si χ est un caractère primitif modulo m et $(a, m) = r > 1$, alors

$$\tau_a(\chi) = 0.$$

Posons $m = rd$. Il est clair que ζ^a est une racine primitive $d^{\text{ième}}$ de a et par suite $\zeta^{az} = \zeta^a$ si et seulement si $z \equiv 1 \pmod d$. Prenons pour z un nombre tel que $(z, m) = 1$, $z \equiv 1 \pmod d$ et $\chi(z) \neq 1$ (l'existence d'un tel z résulte du théorème 4 du § 5 de l'appendice). Puisque, en même temps que x, le produit zx parcourt un système complet de résidus modulo m, alors

$$\tau_a(\chi) = \sum_{x \bmod m} \chi(zx)\zeta^{azx} = \chi(z) \sum_{x \bmod m} \chi(x)\zeta^{ax} = \chi(z)\tau_a(\chi).$$

Puisque $\chi(z) \neq 1$, il en résulte que $\tau_a(\chi) = 0$.

De plus, si $(a, m) = 1$, alors

$$\tau_a(\chi) = \chi(a)^{-1}\tau(\chi).$$

En effet, puisque le produit ax parcourt, simultanément avec x, un système complet de résidus modulo m, alors

$$\chi(a)\tau_a(\chi) = \sum_{x \bmod m} \chi(ax)\zeta^{ax} = \tau_1(\chi) = \tau(\chi).$$

La formule (17) peut s'écrire, dans le cas d'un caractère χ primitif, sous la forme

$$L(1, \chi) = -\frac{\tau(\chi)}{m} \sum_{(k,m)=1} \overline{\chi}(k) \operatorname{Log}(1 - \zeta^{-k}). \tag{18}$$

Revenons à l'étude de la somme

$$S_\chi = \sum_{(k,m)=1} \overline{\chi}(k) \operatorname{Log}(1 - \zeta^{-k}) \tag{19}$$

(k parcourt un système réduit de résidus modulo m). L'étude de la somme S_χ nécessite la distinction de deux cas de nature tout à fait différente. Pour différencier ces deux cas, nous aurons besoin de la définition suivante.

DÉFINITION, — ***Un caractère modulaire*** χ ***est dit pair si*** $\chi(-1) = 1$ ***(d'où*** $\chi(-x) = \chi(x)$ ***pour tout entier*** x***) et dit impair si*** $\chi(-1) = -1$ ***(dans ce cas,*** $\chi(-x) = -\chi(x)$***).***

Puisque

$$(\chi(-1))^2 = \chi((-1)^2) = \chi(1) = 1,$$

alors $\chi(-1) = \pm 1$ et par suite tout caractère χ est pair ou impair.

Le nombre $1 - \zeta^{-k}$ pour $0 < k < m$ peut s'écrire sous la forme trigonométrique suivante

$$1 - \zeta^{-k} = 2 \sin \frac{\pi k}{m} \left(\cos \left(\frac{\pi}{2} - \frac{\pi k}{m} \right) + i \sin \left(\frac{\pi}{2} - \frac{\pi k}{m} \right) \right),$$

avec $-\frac{\pi}{2} < \frac{\pi}{2} - \frac{\pi k}{m} < \frac{\pi}{2}$; par suite,

$$\operatorname{Log}(1 - \zeta^{-k}) = \operatorname{Log} | 1 - \zeta^{-k} | + i\pi \left(\frac{1}{2} - \frac{k}{m} \right).$$

De plus, puisque $1 - \zeta^{-k}$ et $1 - \zeta^{k}$ sont conjugués, alors

$$\operatorname{Log}(1 - \zeta^{k}) = \operatorname{Log} | 1 - \zeta^{k} | - i\pi \left(\frac{1}{2} - \frac{k}{m} \right)$$

(soulignons, cette fois encore, que ces deux dernières formules ne sont valables que si k est pris parmi les plus petits résidus positifs modulo m).

Supposons maintenant que le caractère χ (et par suite aussi le caractère $\bar{\chi}$) est pair. Remplaçant k par $-k$ dans la somme (19), nous obtenons

$$S_\chi = \sum_{(k,m)=1} \bar{\chi}(k) \operatorname{Log}(1 - \zeta^{k}),$$

ce qui, ajouté à (19), donne

$$2S_\chi = \sum_{(k,m)=1} \bar{\chi}(k) [\operatorname{Log}(1 - \zeta^{-k}) + \operatorname{Log}(1 - \zeta^{k})]$$

$$= 2 \sum_{(k,m)=1} \bar{\chi}(k) \operatorname{Log} | 1 - \zeta^{k} | = 2 \sum_{\substack{(k,m)=1 \\ 0<k<m}} \bar{\chi}(k) \operatorname{Log} 2 \sin \frac{\pi k}{m}.$$

Si maintenant le caractère χ est impair, alors, remplaçant de nouveau k par $-k$ dans (19), nous obtenons

$$S_\chi = -\sum_{(k,m)=1} \bar{\chi}(k) \operatorname{Log}(1 - \zeta^{k}),$$

d'où

$$2S_\chi = \sum_{(k,m)=1} \bar{\chi}(k) [\text{Log } (1 - \zeta^{-k}) - \text{Log } (1 - \zeta^k)] = 2 \sum_{\substack{(k,m)=1 \\ 0<k<m}} \bar{\chi}(k) \pi i \left(\frac{1}{2} - \frac{k}{m}\right).$$

Tenant compte du fait que $\sum_{(k,m)=1} \bar{\chi}(k) = 0$ (car le caractère χ est distinct du caractère unité), nous obtenons, en utilisant (18), le résultat suivant.

THÉORÈME 3. — *Soit χ un caractère primitif modulo $m > 1$. Si χ est pair, alors*

$$L(1, \chi) = -\frac{\tau(\chi)}{m} \sum_{(k,m)=1} \bar{\chi}(k) \text{ Log } |1 - \zeta^k|$$

$$= -\frac{\tau(\chi)}{m} \sum_{\substack{(k,m)=1 \\ 0<k<m}} \bar{\chi}(k) \text{ Log sin } \frac{\pi k}{m} \qquad (20)$$

Si maintenant χ est impair, alors

$$L(1, \chi) = \frac{\pi i \tau(\chi)}{m^2} \sum_{\substack{(k,m)=1 \\ 0<k<m}} \bar{\chi}(k) k. \qquad (21)$$

EXERCICES

1. Montrer que si χ est un caractère primitif modulo m, alors

$$|\tau(\chi)| = \sqrt{m}.$$

2. Soit p un nombre premier impair et posons $p^* = (-1)^{\frac{p-1}{2}} p$. Démontrer que le corps quadratique $\mathbf{Q}(\sqrt{p^*})$ est contenu dans le $p^{\text{ième}}$ corps cyclotomique. (Utiliser l'exercice 5 du chapitre premier § 2, pour a = b = 1).

3. Démontrer que tout corps quadratique est contenu dans un certain corps cyclotomique.

4. Les notations étant celles de l'exercice 6 du § 5 de l'appendice, démontrer l'égalité

$$\tau_a(\chi) = \tau_a(\chi_1) \cdots \tau_a(\chi_k) \chi_1\left(\frac{m}{m_1}\right) \cdots \chi_k\left(\frac{m}{m_k}\right)$$

(on suppose que pour définir les sommes de Gauss $\tau_a(\chi_i)$ on prend comme racine primitive d'ordre m_i de 1 le nombre $\zeta^{\frac{m}{m_i}}$, où ζ est la racine primitive $m^{\text{ième}}$ de 1 qui intervient dans la somme $\tau_a(\chi)$).

5. Soit p un nombre premier ne figurant pas dans m et soit f le plus petit entier naturel tel que $pf \equiv 1 \pmod m$. Démontrer que le polynôme $\Phi_m(t)$, à coefficients

dans $\mathbf{F}_p$ (cf. 1)) se décompose dans l'anneau $\mathbf{F}_p[t]$ en un produit de $\frac{\varphi(m)}{f}$ facteurs irréductibles de même degré f (D'après le théorème 8 du chapitre III, § 5, cela donne une seconde démonstration du théoréme 2).

6. Soit p un nombre premier impair. Considérant le corps $\mathbf{Q}(\sqrt{-1})$ et rapprochant pour ce corps le théorème 1 du chapitre III, § 8, du théorème 2 de ce paragraphe, démontrer l'égalité

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

(premier complément à la loi de réciprocité quadratique).

7. Soient p et $q \neq 2$ deux nombres premiers distincts, K le $q^{\text{ième}}$ corps cyclotomique et g le nombre de diviseurs premiers distincts du corps K qui figurent dans la décomposition du nombre p. Utilisant le critère d'Euler $\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \pmod{q}$, démontrer que

$$\left(\frac{p}{q}\right) = (-1)^g$$

8. Conservant les mêmes notations, considérons le sous-corps quadratique $k = \mathbf{Q}(\sqrt{q^*})$ du corps K, $q^* = (-1)^{\frac{q-1}{2}} q$. Posons $f = \frac{q-1}{g}$. Démontrer que si p se décompose dans le corps k en un produit de deux diviseurs premiers, alors g est pair, et si p reste premier dans k, alors f est pair. En s'appuyant sur le théorème 1 du chapitre III, § 8, montrer de plus que

$$\left(\frac{q^*}{p}\right) = (-1)^g.$$

Ainsi p se décompose dans k si et seulement si g est pair.

Indication. — Dans le cas où $q \equiv 1 \pmod 4$, utiliser l'exercice 7 et montrer que $\left(\frac{p}{q}\right) = (5) = 1$ entraîne $\left(\frac{q}{p}\right) = \left(\frac{q^*}{p}\right) = 1$.

9. Déduire des deux exercices précédents la loi de réciprocité quadratique

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

10. Démontrer que si un nombre premier $q \neq 2$ se décompose en un produit de deux diviseurs premiers dans le corps $\mathbf{Q}(\sqrt{2})$ et $q \equiv 1 \pmod 4$, alors $q \equiv 1 \pmod 8$ (Considérer la décomposition de q dans le corps $\mathbf{Q}(\sqrt{2}, \sqrt{-1})$ de division du cercle en 8 parties).

11. Les notations étant celles des exercices 7 et 8, démontrer que le nombre $p = 2$ se décompose en un produit de deux diviseurs premiers dans le corps k si et seulement si g est pair.

12. Rapprochant le résultat de l'exercice précédent du théorème 1, chapitre III, § 8, démontrer que l'égalité $\left(\frac{2}{q}\right) = +1$ est équivalente à la congruence $q^* \equiv 1 \pmod 8$, i. e. que

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^*-1}{8}}$$

deuxième complément à la loi de réciprocité quadratique).

13. Démontrer que dans le corps de décomposition du cercle en p^k parties le nombre p admet la décomposition

$$P = \mathfrak{p}^g, \qquad g = \varphi(p^k) = p^k(p-1), \qquad N(\mathfrak{p}) = p.$$

14. Soit $m = p^k m'$ $(p, m') = 1$ et soit f le plus petit entier naturel tel que $p^f \equiv 1 \pmod{m'}$. Démontrer que dans le corps de division du cercle en m parties le nombre p a une décomposition de la forme

$$P = (\mathfrak{p}_1 \ldots \mathfrak{p}_g)^e, \qquad N(\mathfrak{p}_i) = p^f,$$

où $e = \varphi(p^k)$, $fg = \varphi(m')$ (φ fonction d'Euler).

15. Démontrer que la fonction G(s) définie par l'égalité (6) vérifie la formule

$$G(s) = \prod_{p|m} \prod_{\chi \bmod m'} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

où p parcourt tous les diviseurs premiers du nombre m et χ, pour p donné, parcourt tous les caractères modulaires modulo m', $m = p^k m'$, $p \nmid m'$.

16. Utilisant l'exercice 9 du § 5 de l'appendice, l'égalité (10) et la formule de l'exercice précédent, démontrer que la fonction $\zeta_K(s)$ du corps de division du cercle en m parties admet la décomposition

$$\zeta_K(s) = \prod_{d|m} \prod_{\substack{\chi \bmod d \\ \chi \text{ primitif}}} L(s,\chi)$$

où d parcourt tous les diviseurs du nombre m (y compris 1 et m) et χ (pour d donné) parcourt tous les caractères primitifs modulo d. En déduire que

$$\lim_{s \to 1+} (s-1)\zeta_K(s) = \prod_{\substack{d|m \\ d \neq 1}} \prod_{\substack{\chi \bmod d \\ \chi \text{ primitif}}} L(1,\chi).$$

§ 3. — LE THÉORÈME DE DIRICHLET SUR LES NOMBRES PREMIERS DANS UNE PROGRESSION ARITHMÉTIQUE

Dans le § 2, nous avons utilisé les théorèmes 2 et 4 du § 1 pour calculer le nombre h de classes de diviseurs des corps cyclotomiques. Dans ce paragraphe, nous montrerons que la formule (2) du § 1 dont la partie droite est différente de zéro permet d'obtenir d'importants résultats sur les diviseurs premiers de degré 1 et sur les nombres premiers dans les progressions arithmétiques.

1) Sur les diviseurs premiers de degré un

THÉORÈME 1. — *Dans tout corps* K *de nombres algébriques il existe une infinité de diviseurs premiers de degré un.*

DÉMONSTRATION. — D'après le théorème 4 du § 1, la fonction $\zeta_K(s)$ admet la décomposition

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{N(p)^s}\right)^{-1}. \tag{1}$$

Puisque le produit infini est convergent et non nul, alors $\zeta_K(s) \neq 0$ pour tout $s > 1$. Prenant les logarithmes des deux membres de l'égalité (1), nous obtenons

$$\operatorname{Log} \zeta_K(s) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mN(p)^{ms}}. \tag{2}$$

Isolons dans cette égalité la somme

$$P(s) = \sum_{p_1} \frac{1}{N(p_1)^s}, \tag{3}$$

dans laquelle la sommation est étendue à tous les diviseurs premiers p_1 de degré un du corps K. Si on désigne par G(s) la somme de tous les termes restants, l'égalité (2) s'écrit

$$\operatorname{Log} \zeta_K(s) = P(s) + G(s). \tag{4}$$

Soit f le degré d'un diviseur premier p, i. e. $N(p) = p^f$. Si $f \geqslant 2$, alors

$$\sum_{m=1} \frac{1}{mN(p)^{ms}} < \sum_{m=1} \frac{1}{p^{2sm}} < \frac{1}{p^{2s} - 1} < \frac{2}{p^{2s}}.$$

Si maintenant $f = 1$, alors

$$\sum_{m=2}^{\infty} \frac{1}{mN(p)^{ms}} < \sum_{m=2}^{\infty} \frac{1}{p^{sm}} = \frac{1}{p^s(p^s - 1)} < \frac{2}{p^{2s}}.$$

Puisque pour tout nombre premier rationnel p il existe au plus $n = (K : Q)$ diviseurs premiers du corps K qui divisent p, nous obtenons l'estimation suivante pour G(s) :

$$G(s) < \sum_P \frac{2n}{p^{2s}} < 2n \sum_{m=1}^{\infty} \frac{1}{m^{2s}};$$

il en résulte que G(s) est bornée pour $s \to 1 + 0$. D'autre part, il résulte de la relation (2) du § 1, dans laquelle $\varkappa h \neq 0$, que $\operatorname{Log} \zeta_K(s)$ de même que $\zeta_K(s)$ tend vers l'infini pour $s \to 1 + 0$. Par suite, d'après (4), P(s) vérifie

cette même propriété; ainsi la somme (3) contient une infinité de termes. Le nombre de diviseurs premiers p_1 de degré 1 est donc infini et le théorème 1 est démontré.

2) Théorème de Dirichlet

THÉORÈME 2 (théorème de Dirichlet). — ***Toute classe résiduelle modulo m, formée de nombres premiers avec m, contient une infinité de nombres premiers.***

DÉMONSTRATION. — Nous utiliserons ici encore le fait que la limite (2) du § 1 n'est pas nulle. La démonstration repose sur le fait que $L(1, \chi) \neq 0$ pour tout caractère χ modulo ***m*** différent du caractère unité, ce qui résulte de manière évidente de la formule (16), § 2.

Considérons la décomposition suivante de la série $L(s, \chi)$ en produit infini :

$$L(s, \chi) = \prod_P \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{5}$$

De la convergence de ce produit infini résulte que pour tout caractère numérique χ modulo ***m*** (y compris le caractère unité χ_0), $L(s, \chi)$ est différent de zéro pour tout $s > 1$. On peut donc considérer dans l'intervalle $(1, \infty)$ la fonction à valeurs complexes Log $L(s, \chi)$. Puisque la fonction logarithme n'est pas uniforme il faut faire choix d'une branche de cette fonction; nous procéderons ainsi. Prenons le logarithme de chaque facteur du produit infini (5), en choisissant sa valeur de telle sorte que

$$-\operatorname{Log}\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{sn}}. \tag{6}$$

Faisant la somme des séries (6) pour **tout *p***, nous obtenons

$$\sum_P -\operatorname{Log}\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_P \frac{\chi(p)}{p^s} + R(s, \chi),$$

avec

$$R(s, \chi) = \sum_P \left(\frac{1}{2}\frac{\chi(p)^2}{p^{2s}} + \frac{1}{3}\frac{\chi(p)^3}{p^{3s}} + \ldots\right)$$

(la convergence absolue, pour $s > 1$, de toutes les séries qui figurent ci est évidente). Nous choisirons la valeur de Log $L(s, \chi)$ de telle sorte que l'on ait l'égalité

$$\operatorname{Log} L(s, \chi) = \sum_P \frac{\chi(p)}{p^s} + R(s, \chi) \tag{7}$$

pour tout $s > 1$. Remarquons que, dans le cas du caractère unité χ_0, la valeur de Log $L(s, \chi_0)$ ainsi déterminée est réelle.

Évaluons la quantité $R(s, \chi)$:

$$|R(s, \chi)| < \sum_p \sum_{n=2}^{\infty} \frac{1}{p^{sn}} < \sum_p \frac{1}{p(p-1)} < \sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1,$$

Ainsi $|R(s, \chi)| < 1$ pour tout $s > 1$.

En dehors des caractères modulaires χ, on considérera aussi, en les désignant par la même lettre χ, les caractères correspondants du groupe G_m des classes résiduelles modulo m premières avec m. Supposons que C parcourt toutes les classes du groupe G_m. Puisque $\chi(p) = \chi(C)$ pour $p \in C$, alors

$$\sum_p \frac{\chi(p)}{p^s} = \sum_C \chi(C) \sum_{p \in C} \frac{1}{p^s}$$

(rappelons que $\chi(p) = 0$ si $p \mid m$). Posant

$$f(s, C) = \sum_{p \in C} \frac{1}{p^s},$$

on peut écrire l'égalité (7) sous la forme suivante :

$$\text{Log } L(s, \chi) = \sum_C \chi(C) f(s, C) + R(s, \chi). \tag{8}$$

Puisque le nombre de tous les caractères modulo m est égal à $\varphi(m)$, on peut considérer les égalités (8) pour tout χ comme un système de $\varphi(m)$ équations linéaires à $\varphi(m)$ inconnues $f(s, C)$ (dont les termes constants sont égaux aux différences Log $L(s, \chi) - R(s, \chi)$). Pour obtenir $f(s, A)$ à partir de ce système ($A \in G_m$), multiplions (8) par $\chi(A^{-1})$ et faisons la somme pour tous les caractères χ. Nous obtenons

$$\sum_\chi \chi(A^{-1}) \text{ Log } L(s, \chi) = \sum_C \sum_\chi \chi(CA^{-1}) f(s, C) + R_A(s), \tag{9}$$

où la quantité

$$R_A(s) = \sum_\chi \chi(A^{-1}) R(s, \chi)$$

admet l'estimation $|R_A(s)| < \varphi(m)$ pour tout $s > 1$. D'après la formule (6) du § 5 de l'appendice, la somme $\sum_\chi \chi(CA^{-1})$ est égale à $q(m)$ pour C = A

et à zéro pour C ≠ A; l'égalité (9) peut donc s'écrire sous la forme

$$\operatorname{Log} L(s, \chi_0) + \sum_{\chi \neq \chi_0} \chi(A^{-1}) \operatorname{Log} L(s, \chi) = \varphi(m) f(s, A) + R_A(s). \quad (10)$$

Par ailleurs, la valeur de $f(s, A)$ est connue d'après le système (8).

Faisons maintenant tendre s vers 1 à droite. Si $\chi \neq \chi_0$, alors

$$L(s, \chi) \to L(1, \chi)$$

et L(l, χ) est différent de zéro, comme on l'a remarqué au début de la démonstration. Par suite, la somme qui figure dans la partie gauche de l'égalité (10) (étendue à tous les caractères non unité) a une limite finie. Faisant passer cette somme dans la partie droite de (10) et la réunissant à R_A (s), nous obtenons l'égalité

$$\operatorname{Log} L(s, \chi_0) = \varphi(m) f(s, A) + T_A(s), \quad (11)$$

où T_A est borné pour $s \to 1 + 0$.

Si nous supposons maintenant qu'il n'existe qu'une quantité finie de nombres premiers dans la classe A, alors la fonction

$$f(s, A) = \sum_{p \in A} \frac{1}{p^s}$$

aura une limite finie pour $s \to 1$ et toute la partie droite de (11) sera bornée pour $s \to 1 + 0$. Pourtant, c'est impossible puisque

$$\lim_{s \to 1+0} L(s, \chi_0) = +\infty,$$

ce qui résulte de l'égalité

$$L(s, \chi_0) = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right).$$

La contradiction obtenue démontre le théorème 2.

On peut préciser le théorème de Dirichlet sous la forme suivante. Posons

$$f(s) = \sum_A f(s, A) = \sum_{(p,m)=1} \frac{1}{p^s}.$$

Divisons l'égalité (11) par $\varphi(m)$ et sommons selon toutes les classes $A \in G_m$. Nous obtenons

$$\operatorname{Log} L(s, \chi_0) = f(s) + T(s), \quad (12)$$

où T(s) est borné pour $s \to 1 + 0$. Égalons les parties droites de (11) et (12) et divisons l'égalité obtenue par $\varphi(m) f(s)$; passant à la limite pour $s \to 1 + 0$, nous obtenons l'égalité

$$\lim_{s \to 1+0} \frac{\sum_{p \in A} \frac{1}{p^s}}{\sum_{(p,m)=1} \frac{1}{p^s}} = \frac{1}{\varphi(m)}.$$

La formule obtenue s'exprime en disant que les nombres premiers, premiers avec m, sont répartis uniformément dans les classes résiduelles mod m.

EXERCICES

1. Démontrer que la différence entre les fonctions

$$\text{Log } \zeta(s) \text{ et } g(s) = \sum_p \frac{1}{p^s}$$

(p parcourt tous les nombres premiers rationnels) est bornée pour $s \to 1 + 0$.

2. Soit P(s) la fonction définie par l'égalité (3). Démontrer que la différence

$$P(s) - \text{Log } \frac{1}{s-1}$$

est bornée pour s $\to$ 1 + 0.

3. Un nombre entier rationnel a est appelé un résidu de degré n modulo un nombre p premier si la congruence $x^n \equiv a \pmod p$ est résoluble. Démontrer que pour tout a et n donnés il existe une infinité de p premiers tels que a soit un résidu de degré n modulo p.

4. Soient $a_1, \ldots,$ a, des nombres entiers tels que $a_1^{x_1} \ldots a_n^{x_n}$ soit un carré si et seulement si tous les x_i sont pairs. Démontrer que, pour tout choix des signes $\varepsilon_1, \ldots, \varepsilon_n$ ($\varepsilon = \pm 1$), il existe une infinité de nombres premiers $p \neq 2$ (qui ne divisent pas a,, . . . , a_n) tels que

$$\left(\frac{a_1}{p}\right) = \varepsilon_1, \ldots, \left(\frac{a_n}{p}\right) = \varepsilon_n.$$

Indication. — Considérer la somme

$$\sum_P \left(\prod_i \left(1 + \varepsilon_i \left(\frac{a_i}{p}\right)\right)\right) \frac{1}{p^s}.$$

§ 4. — NOMBRE DE CLASSES DE DIVISEURS D'UN CORPS QUADRATIQUE

1) Formule donnant le nombre de classes de diviseurs

Soit K = $\mathbf{Q}(\sqrt{d})$ un corps quadratique (d est un entier rationnel sans carrés). D'après le théorème 2 du chapitre III, § 8, la décomposition d'un nombre premier p en un produit de diviseurs premiers dans le corps K est la suivante :

1° $p = \mathfrak{p}\mathfrak{p}', \mathfrak{p} \neq \mathfrak{p}', N(\mathfrak{p}) = N(\mathfrak{p}') = p$ si $\chi(p) = 1$;

2° $p = \mathfrak{p}, N(\mathfrak{p}) = p^2,$ si $\chi(p) = -1$;

3° $p = \mathfrak{p}^2, N(\mathfrak{p}) = p,$ si $\chi(p) = 0$:

où χ est le caractère du corps quadratique K (cf. définition du chapitre III, § 8, 2)). Par suite, dans le produit

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

les facteurs qui correspondent au nombre p sont égaux respectivement à

1) $$\left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{-1};$$

2) $$\left(1 - \frac{1}{p^{2s}}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1};$$

3) $$\left(1 - \frac{1}{p^s}\right)^{-1}.$$

Dans ces trois cas, le facteur qui correspond au nombre p peut s'écrire sous la forme

$$\left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Puisque

$$\prod_{P} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s)$$

(théorème 4, § 1, appliqué au corps des nombres rationnels), alors $\zeta_K(s)$ admet la représentation

$$\zeta_K(s) = \zeta(s) \prod_{P} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \qquad (1)$$

Le produit infini qui constitue la partie droite de cette égalité est la **série** $L(s, \chi)$ qui correspond au caractère χ (modulo | D |, où D est le discriminant du corps K); puisque ce caractère n'est pas unité, alors $L(s, \chi)$ est une fonction continue dans l'intervalle $0 < s < \infty$ (corollaire du lemme 4 du § 2). Multiplions (1) par $s - 1$ et passons à la limite pour $s \to 1 + 0$. Tenant compte de l'égalité (19) du § 1, nous obtenons

$$\lim_{s \to 1+0} (s - 1)\zeta_K(s) = L(1, \chi).$$

Utilisons maintenant le théorème 2 du § 1. Puisque pour un corps quadratique réel, on a $s = 2$, $t = 0$, $m = 2$, $r = \operatorname{Log} \varepsilon$ ($\varepsilon > 1$ est une unité fondamentale du corps) et pour un corps imaginaire $s = 0$, $t = 1$, $r = 1$,

alors on a les formules suivantes pour le nombre de classes de diviseurs du corps K :

$$h = \begin{cases} \dfrac{\sqrt{D}}{2 \operatorname{Log} \varepsilon} L(1, \chi) & \text{pour} \quad d > 0, \\ \dfrac{m\sqrt{|D|}}{2x} L(1, \chi) & \text{pour} \quad d < 0. \end{cases}$$

(remarquons que le nombre m, i. e. le nombre de racines de 1 contenues dans K est égal à 4 pour K = $\mathbf{Q}(\sqrt{-1})$, égal à 6 pour K = $\mathbf{Q}(\sqrt{-3})$ et égal à 2 pour tous les autres corps quadratiques imaginaires; cf. chap. II, § 7-3)).

Nous démontrerons dans le point suivant que le caractère d'un corps quadratique de discriminant D est un caractère primitif modulo | D | (cf. définition, § 5-3) de l'appendice) et qu'il est pair pour des corps réels et impair pour des corps imaginaires. Nous pouvons donc utiliser les formules (20) et (22) du § 2 donnant les valeurs de L(1, χ). Pour obtenir des formules définitives pour h, il faut calculer explicitement les sommes normées de Gauss $\tau(\chi) = \tau_1(\chi)$. Dans le numéro 3) de ce paragraphe, nous verrons que la somme $\tau(\chi)$ est égale à $\sqrt{D}$ pour des corps réels et à $i\sqrt{|D|}$ pour des corps imaginaires. Utilisant ce résultat et remarquant que, dans le cas d'un corps réel, $\chi(D - x) = \chi(x)$, nous pouvons formuler le théorème suivant (pour simplifier les formules donnant h, nous avons écarté les corps $Q(\sqrt{-1})$ et $\mathbf{Q}(\sqrt{-3})$ de discriminants respectifs -4 et -3 pour lesquels m est égal respectivement à 4 et 6; pour ces corps, $h = 1$).

THÉORÈME 1. — *Le nombre des classes de diviseurs d'un corps quadratique réel de discriminant* D *est donné par la formule*

$$h = -\frac{1}{\operatorname{Log} \varepsilon} \sum_{\substack{(x,D)=1 \\ 0<x<\frac{D}{2}}} \chi(x) \operatorname{Log} \sin \frac{\pi x}{D}, \tag{2}$$

où $\varepsilon > 1$ *est une unité fondamentale du corps ; dans le cas d'un corps quadratique imaginaire de discriminant* $D < -4$, *ce nombre est donné par la formule*

$$h = -\frac{1}{|D|} \sum_{\substack{(x,D)=1 \\ 0<x<|D|}} \chi(x) x. \tag{3}$$

Dans ces deux cas, χ désigne le caractère du corps correspondant défini dans le chapitre III, § 8, 2) (formule (5)).

Mettons en évidence quelques conséquences du théorème 1. Commençons par la formule (2). Si nous introduisons le nombre

$$\eta = \frac{\prod_b \sin \frac{\pi b}{D}}{\prod_a \sin \frac{\pi a}{D}}, \qquad (4)$$

où a et b parcourent les nombres naturels de l'intervalle $\left(0, \frac{D}{2}\right)$ premiers avec D, qui satisfont respectivement aux conditions $\chi(a) = +1$ et $\chi(b) = -1$, cette formule peut s'écrire $\varepsilon^h = \eta$. Il en résulte que η est une unité de notre corps quadratique et $\eta > 1$ (puisque $\varepsilon > 1$). Nous avons obtenu le théorème suivant.

THÉORÈME *2. — Pour un corps quadratique réel* K *de discriminant* D *et de caractère* χ, *le nombre* η *de la forme (4) appartient à ce corps* K, *est une unité de ce corps et est lié à une unité fondamentale* $\varepsilon > 1$ *par la relation*

$$Eh = \eta,$$

où h est le nombre de classes de diviseurs du corps K.

Malgré la simplicité de son énoncé, ce théorème, jusqu'à présent, est de démonstration assez délicate. De plus, les procédés purement arithmétiques ne permettent pas de montrer que $\eta > 1$ et cette inégalité $\eta > 1$ a des conséquences pour la décomposition des résidus quadratiques modulo un nombre premier $p \equiv 1 \pmod 4$. En effet, le discriminant du corps quadratique $Q(\sqrt{p})$ est égal à p et le caractère $\chi(x)$ coïncide avec le caractère de Legendre $\left(\frac{x}{p}\right)$. Nous avons donc l'inégalité

$$\prod_b \sin \frac{\pi b}{p} > \prod_a \sin \frac{\pi a}{p},$$

dans laquelle a et b parcourent respectivement tous les résidus et non-résidus quadratiques modulo p de l'intervalle $\left(0, \frac{p}{2}\right)$. Du fait que la fonction sin x est monotone sur l'intervalle $\left(0, \frac{\pi}{2}\right)$, cette inégalité entraîne que toutes les valeurs $\frac{\pi b}{p}$ sont « en moyenne » plus grandes que les valeurs $\frac{\pi a}{p}$, i. e. que les résidus quadratiques modulo p « se concentrent » au début de

l'intervalle $\left(0, \frac{p}{2}\right)$ et les non-résidus à la fin (le nombre de résidus et de non-résidus modulo $p \equiv 1 \pmod 4$ contenus dans l'intervalle $\left(0, \frac{p}{2}\right)$ est, bien entendu, le même).

De plus, on peut obtenir des résultats sur la décomposition des résidus quadratiques pour des nombres premiers $p \equiv 3 \pmod 4$ en appliquant la formule (3) au corps $\mathbf{Q}(\sqrt{-p})$.

Simplifions tout d'abord la formule (3) dans le cas général. Nous poserons $|D| = m$ dans ce qui suit.

Supposons tout d'abord m pair. Un raisonnement simple (exercice 9) montre que, dans ce cas, $\chi\left(x + \frac{m}{2}\right) = -\chi(x)$; la formule (3) donne alors

$$hm = -\sum_{0<x<\frac{m}{2}} \chi(x)x - \sum_{0<x<\frac{m}{2}} \chi\left(x+\frac{m}{2}\right)\left(x+\frac{m}{2}\right)$$

$$= -\sum_{0<x<\frac{m}{2}} \chi(x)x + \sum_{0<x<\frac{m}{2}} \chi(x)\left(x+\frac{m}{2}\right) = \frac{m}{2}\sum_{0<x<\frac{m}{2}} \chi(x),$$

d'où

$$h = \frac{1}{2}\sum_{0<x<\frac{m}{2}} \chi(x).$$

Remarquons que la parité de m équivaut à $\chi(2) = 0$.

Supposons maintenant m impair. Puisque le caractère χ d'un corps quadratique imaginaire est impair, i. e. $\chi(-1) = -1$ (ce qui sera démontré dans le théorème 6 du point suivant), alors (3) entraîne

$$hm = -\sum_{0<x<\frac{m}{2}} \chi(x)x - \sum_{0<x<\frac{m}{2}} \chi(m-x)(m-x)$$

$$= -2\sum_{0<x<\frac{m}{2}} \chi(x)x + m\sum_{0<x<\frac{m}{2}} \chi(x). \qquad (5)$$

D'autre part

$$hm = -\sum_{\substack{0<x<m \\ x \text{ pair}}} \chi(x)x - \sum_{\substack{0<x<m \\ x \text{ pair}}} \chi(m-x)(m-\chi)$$

$$= -4\sum_{0<x<\frac{m}{2}} \chi(2x)x + m\sum_{0<x<\frac{m}{2}} \chi(2x),$$

d'où

$$hm\chi(2) = -4\sum_{0<x<\frac{m}{2}}\chi(x)x + m\sum_{0<x<\frac{m}{2}}\chi(x). \tag{6}$$

Éilminons $\sum\chi(x)x$ entre (5) et (6); nous obtenons l'égalité

$$h(2 - \chi(2)) = \sum_{0<x<\frac{m}{2}}\chi(x).$$

Puisque cette égalité est vraie aussi pour m pair, comme on l'a vu plus haut (puisque $\chi(2) = 0$ pour $2 \mid m$), nous avons obtenu le théorème suivant.

THÉORÈME *3. — Le nombre h de classes de diviseurs d'un corps quadratique imaginaire de discriminant* $D < -4$ *et de caractère* χ *est donné par la formule*

$$h = \frac{1}{2 - \chi(2)}\sum_{\substack{0<x<\frac{|D|}{2}\\(x,D)=1}}\chi(x). \tag{7}$$

Appliquons le théorème 3 au corps $\mathbf{Q}(\sqrt{-p})$ où p est un nombre premier de la forme $4n + 3$. Puisque $-p \equiv 1 \pmod 4$, alors, dans ce cas, $D = -p$ et le caractère $\chi(x)$ coïncide avec le symbole de Legendre $\left(\frac{x}{p}\right)$. Remarquant que le nombre de termes de la somme $\sum_{0<x<\frac{p}{2}}\left(\frac{x}{p}\right)$ est impair $\left(\frac{p-1}{2} = 2n + 1\right)$ et que cette somme est impaire puisque $\chi(2) = 1$ si $p \equiv 7 \pmod 8$ et $\chi(2) = -1$ si $p \equiv 3 \pmod 8$, le théorème 3 entraîne le résultat suivant :

THÉORÈME *4. — Pour un nombre premier p de la forme* $4n + 3$, *le nombre de classes de diviseurs du corps* $\mathbf{Q}(\sqrt{-p})$ *est impair et égal à*

$$h = V - N \qquad \text{si} \quad p \equiv 7 \pmod 8,$$

$$h = \frac{1}{3}(V - N) \quad \text{si} \quad p \equiv 3 \pmod 8, \ p \neq 3,$$

où V *est le nombre de résidus quadratiques modulo p qui appartiennent à l'intervalle* $\left(0, \frac{p}{2}\right)$ *et N le nombre de non-résidus de ce même intervalle.*

Le théorème 4 entraîne trivialement que $V > N$. Ainsi, pour un modulo

premier p de la forme $4n + 3$, le nombre de résidus quadratiques est supérieur au nombre de non-résidus dans l'intervalle $\left(0, \frac{p}{2}\right)$ et la différence de ces nombres est divisible par 3 si $p \equiv 3 \pmod 8$, $p \neq 3$).

La propriété ci-dessus, malgré sa simplicité, est un résultat profond de la théorie des nombres. Nous l'avons obtenu comme un simple corollaire du fait que h est, par nature même, un nombre positif et que, par suite, l'expression de droite de la formule (7) est aussi positive. Le signe de cette expression est défini par le signe de la *somme* de Gauss $\tau_1(\chi)$ et nous verrons dans le point 3), que la détermination du signe du $\tau_1(\chi)$ est un problème très difficile.

La formule donnant h pour les corps quadratiques imaginaires dans le cas où $D \neq 1 \pmod 8$ peut s'obtenir par des procédés purement arithmétiques, comme l'a montré B. A. Venkov. Cette démonstration repose sur la représentation d'une forme binaire comme somme de trois carrés de formes linéaires et sur des propriétés des fractions continues (B. A. Venkov, Sur le nombre des classes de formes quadratiques binaires de déterminants négatifs. I et II. *Izv.* A. *N. URSS,* série VII, Dép. Sciences Phys. et Math., 1928, n° 4-5, 375392; 1928, n° 6-7, 455-480). Dans le cas des corps imaginaires tels que $D \equiv 1 \pmod 8$ (comme dans le cas des corps réels), il n'existe pas jusqu'à présent de raisonnement purement arithmétique donnant la valeur de h. Par ailleurs, il n'existe pas de démonstration élémentaire du fait que, pour un module premier p de la forme $8n + 7$, l'intervalle $\left(0, \frac{p}{2}\right)$ contient plus de résidus quadratiques que de non-résidus.

Remarque. — On peut montrer élémentairement (exercice 7) que pour p premier de la forme $8n + 7$ il existe dans l'intervalle $\left(0, \frac{p}{2}\right)$ le même nombre de résidus et de non-résidus impairs. Par suite, le nombre h pour le corps $Q(\sqrt{-p})$, $p \equiv 7 \pmod 8$ est donné par la formule

$$h = V^* - N^*,$$

où V^* et N^* sont respectivement les nombres de résidus et non-résidus pairs mod p contenus dans $\left(0, \frac{p}{2}\right)$.

2) Caractère d'un corps quadratique

NOUS démontrerons ici toutes les propriétés du caractère d'un corps quadratique que nous avons utilisées dans le point 1).

THÉORÈME 5. — *Le caractère* χ (modulo $|D|$) *d'un corps quadratique de discriminant* D *est primitif.*

DÉMONSTRATION. — D'après le théorème 4 du § 5 de l'appendice, il suffit de démontrer que pour tout nombre premier p figurant dans D, il existe x tel que (x, D) = 1, $x \equiv 1 \left(\mathrm{mod}\ \frac{|D|}{p}\right)$ et $\chi(x) = -1$. Considérons tout d'abord le cas $p \neq 2$. Choisissons un certain non-résidu quadratique s modulo p et soit x un entier satisfaisant au système de congruences

$$x \equiv s \pmod{p}$$

$$x \equiv 1 \left(\mathrm{mod}\ \frac{2|D|}{p}\right).$$

Utilisant la formule (5) du chapitre III § 8, on voit facilement que, dans tous les cas

$$\chi(x) = \left(\frac{x}{p}\right) = \left(\frac{s}{p}\right) = -1.$$

Soit maintenant $p = 2$. Si $d \equiv 3 \pmod 4$, D = $4d$, alors, pour x satisfaisant aux congruences

$$x \equiv 3 \pmod 4$$

$$x \equiv 1 \pmod{2|d|},$$

nous aurons $\chi(x) = (-1)^{\frac{x-1}{2}}$. Si maintenant $d = 2d'$, D = $4d = 8d'$, alors, pour x satisfaisant aux congruences

$$x \equiv 5 \pmod 8$$

$$x \equiv 1 \pmod{4|d'|},$$

nous aurons $\chi(x) = (-1)^{\frac{x^2-1}{8}} = -1$.

Ceci démontre que le caractère χ est primitif.

THÉORÈME 6. — *Tous les caractères des corps quadratiques réels sont pairs et tous ceux des corps quadratiques imaginaires sont impairs.*

DÉMONSTRATION. — Soit χ un caractère d'un corps quadratique $\mathbf{Q}(\sqrt{d})$. Calculons $\chi(-1)$ en utilisant les formules (5) du chapitre III § 8. Si $d \equiv 1 \pmod 4$, alors

$$\chi(-1) = \left(\frac{-1}{|d|}\right) = (-1)^{\frac{|d|-1}{2}} = (-1)^{\frac{d}{2}+\frac{|d|-1}{2}}.$$

Si $d \equiv 3 \pmod 4$, alors

$$\chi(-1) = -\left(\frac{-1}{|d|}\right) = -(-1)^{\frac{|d|-1}{2}} = (-1)^{\frac{d-1}{2}+\frac{|d|-1}{2}}.$$

Si enfin $d = 2d'$, alors

$$\chi(-1) = (-1)^{\frac{d'-1}{2}} \left(\frac{-1}{|d'|}\right) = (-1)^{\frac{d'-1}{2} + \frac{|d'|-1}{2}}.$$

Pour a impair, nous avons donc

$$\frac{a-1}{2} + \frac{|a|-1}{2} = \begin{cases} a-1 \equiv 0 \pmod 2 \text{ pour } a > 0, \\ -1 \text{ pour } a < 0. \end{cases}$$

Par suite, dans tous les cas

$$\chi(-1) = \begin{cases} 1 \text{ pour } d > 0, \\ -1 \text{ pour } d < 0. \end{cases}$$

Le théorème 6 est démontré.

3) Sommes de Gauss pour des caractères quadratiques

Pour obtenir la formule donnant le nombre de classes de diviseurs d'un corps quadratique, nous avons utilisé la valeur de la somme de Gauss normée $\tau(\chi)$. Rappelons qu'une somme de Gauss $\tau_a(\chi)$ du caractère χ modulo m est dite normée si, pour la définir (cf. § 2-4) de ce chapitre), on a pris pour racine primitive $m^{\text{ième}}$ de 1 le nombre $\zeta = \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m}$. Calculons la valeur $\tau(\chi)$.

D'après le théorème 5, le caractère χ d'un corps quadratique $\mathbf{Q}(\sqrt{d})$ de discriminant D est un caractère numérique primitif modulo $|D|$. De plus, il satisfait à la condition $\chi^2 = \chi_0$, où χ_0 est le caractère unité. Ce dernier résultat équivaut au fait que les valeurs du caractère χ sont les nombres ± 1 (et bien sûr aussi zéro).

DÉFINITION. — ***Un caractère modulaire χ différent du caractère unité est dit quadratique si $\chi^2 = \chi_0$.***

Les caractères des corps quadratiques épuisent tous les caractères modulaires quadratiques primitifs (selon tous les modules possibles). En effet, d'après l'exercice 8, il existe des caractères quadratiques primitifs seulement pour des modules de la forme r et $4r$ (un seul caractère) et pour des modules de la forme $8r$ (deux caractères), où r est un nombre entier naturel impair sans carré (dans le cas d'un module impair, $r > 1$). L'ensemble de ces modules coïncide avec l'ensemble des modules de la forme $|D|$ où D parcourt les discriminants de tous les corps quadratiques. Remarquant que pour $|D| = 8r$ il existe deux corps quadratiques $\mathbf{Q}(\sqrt{2r})$ et $\mathbf{Q}(\sqrt{-2r})$ et que modulo $8r$ l'un des caractères quadratiques primitifs est pair et l'autre

impair, nous obtenons que l'ensemble des corps quadratiques est en correspondance biunivoque avec l'ensemble des caractères quadratiques primitifs.

Les valeurs des sommes de Gauss pour des caractères quadratiques primitifs sont données par le théorème suivant.

THÉORÈME 7. — ***Soit χ un caractère quadratique primitif modulo m. Alors la somme de Gauss normée $\tau(\chi) = \tau_1(\chi)$ est égale à***

$$\tau(\chi) = \begin{cases} \sqrt{m} & \text{si} \quad \chi(-1) = 1 ; \\ i\sqrt{m} & \text{si} \quad \chi(-1) = -1. \end{cases}$$

DÉMONSTRATION. — Nous nous bornerons ici à la démonstration complète du théorème 7 pour un module ***p*** premier impair, puisque ce cas contient les difficultés essentielles. Le passage d'un module premier impair à un module quelconque s'effectue relativement facilement; à la fin de la démonstration nous indiquerons les étapes essentielles de ce passage.

Soient donc ***p*** premier impair et $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$. Puisque le caractère quadratique non unité χ modulo ***p*** coïncide avec le symbole de Legendre $\left(\frac{x}{p}\right)$ (cf. exercice 4, chap. Ier, § 2), la somme de Gauss normée $\tau(\chi)$ peut s'écrire

$$\tau(\chi) = \sum_x{}' \left(\frac{x}{p}\right)\zeta^x$$

(où le prime dans la somme indique que x parcourt un système réduit de résidus modulo ***p***). Trouvons le nombre complexe conjugué $\overline{\tau(\chi)}$. Puisque $\overline{\zeta} = \zeta^{-1}$, alors

$$\overline{\tau(\chi)} = \sum_x{}' \left(\frac{x}{p}\right)\zeta^{-x} = \sum_x{}' \left(\frac{-x}{p}\right)\zeta^x = \left(\frac{-1}{p}\right)\tau(\chi). \tag{8}$$

D'autre part, d'après le théorème 4 du chapitre premier § 2,

$$\tau(\chi)\,\overline{\tau(\chi)} = p. \tag{9}$$

Des égalités (8) et (9) résulte maintenant que

$$\tau(\chi)^2 = \left(\frac{-1}{p}\right)p = (-1)^{\frac{p-1}{2}}p,$$

d'où

$$\tau(\chi) = \begin{cases} \pm\sqrt{p} & \text{si} \quad p \equiv 1 \pmod 4, \\ \pm i\sqrt{p} & \text{si} \quad p \equiv 3 \pmod 4. \end{cases} \tag{10}$$

Pour démontrer le théorème 7 (dans le cas $m = p$) il semble qu'il reste peu à faire : il faut seulement déterminer le signe devant $\sqrt{p}$ et $i\sqrt{p}$. En fait, c'est dans la détermination de ce signe que réside toute la difficulté de la démonstration.

Transformons la somme $\tau(\chi)$. Supposons que a parcourt tous les résidus quadratiques modulo p et b tous les non-résidus. Alors, il est clair que

$$\tau(\chi) = \sum_a \zeta^a - \sum_b \zeta^b. \tag{11}$$

Mais

$$1 + \sum_a \zeta^a + \sum_b \zeta^b = 0,$$

d'où

$$\tau(\zeta) = 1 + 2\sum_a \zeta^a.$$

Si x parcourt les valeurs 0, 1, . . . , $p - 1$, alors x^2 parcourt modulo p la valeur 0 et tous les résidus quadratiques chacun deux fois. Par la suite, nous pouvons écrire la somme de Gauss $\tau(\chi)$ sous la forme

$$\tau(\zeta) = \sum_{x=0}^{p-1} \zeta^{x^2}.$$

Introduisons la matrice

$$A = (\zeta^{xy})_{0 \leqslant x, y \leqslant p-1} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots & \zeta^{p-1} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-1)^2} \end{pmatrix}$$

D'après la formule (1 1), la somme de Gauss $\tau(\chi)$ est égale à la trace de cette matrice A. C'est pourquoi, si nous désignons par $\lambda_1, \ldots, \lambda_p$ les valeurs caractéristiques (en tenant compte des ordres de multiplicité), nous aurons

$$\tau(\chi) = A, + \ldots + \lambda_p. \tag{12}$$

Le calcul de $\tau(\chi)$ est ainsi ramené à la recherche des valeurs caractéristiques de la matrice A. Élevons A au carré. Puisque

$$\sum_{t=0}^{p-1} \zeta^{xt}\zeta^{ty} = \sum_{t=0}^{p-1} \zeta^{t(x+y)} = \begin{cases} p \text{ pour } x + y \equiv 0 \pmod p, \\ 0 \text{ pour } x + y \not\equiv 0 \pmod p. \end{cases}$$

alors

$$A^2 = \begin{pmatrix} p & 0 & \dots & 0 \\ 0 & 0 & \dots & p \\ \cdot & \cdot & \cdot & \cdot \\ 0 & p & \dots & 0 \end{pmatrix}$$

Comme on le sait, les valeurs caractéristiques de la matrice A^2 coïncident avec les carrés

$$\lambda_1^2, \dots, \lambda_p^2 \tag{13}$$

des valeurs caractéristiques de A. Mais on peut calculer facilement le polynôme caractéristique de A^2 : il est égal à

$$(t-p)^{\frac{p+1}{2}}(t+p)^{\frac{p-1}{2}}.$$

Donc $\frac{p+1}{2}$ des nombres de la suite (13) sont égaux à p et $\frac{p-1}{2}$ sont égaux à $-p$. Nous en déduisons facilement que chacun des λ_k est égal à l'un des nombres $\pm\sqrt{p}$, $\pm i\sqrt{p}$; par suite, si a, *b*, c, *d* désignent respectivement les multiplicités des valeurs caractéristiques $\sqrt{p}$, $\sqrt{-p}$, $i\sqrt{p}$, $-i\sqrt{p}$, alors

$$a+b=\frac{p}{2} \qquad c+d=\frac{p}{2} \tag{14}$$

La somme (12) s'écrit maintenant

$$\tau(\chi) = (a-b+(c-d)i)\sqrt{p}. \tag{15}$$

Rapprochant cette expression de (10), nous obtenons

$$\left.\begin{array}{ll} a-b=\pm 1,\ c=d & \text{pour} \quad p\equiv 1 \pmod 4, \\ a=b,\quad c-d=\pm 1 & \text{pour} \quad p\equiv 3 \pmod 4. \end{array}\right\} \tag{16}$$

Pour déterminer les multiplicités *a*, *b*, c, *d* il nous faut trouver encore une relation entre elles. Pour obtenir cette relation, calculons le déterminant de la matrice A. Puisque

$$\det(A^2) = p^p(-1)^{\frac{p(p-1)}{2}},$$

alors

$$\det A = f i^{\frac{p(p-1)}{2}} p^2. \tag{17}$$

Le déterminant det A est un déterminant de Vandermonde; c'est pourquoi, en posant

$$\eta = \cos\frac{\pi}{p} + i\sin\frac{\pi}{p},$$

nous aurons

$$\det A = \prod_{p-1 \geqslant r > s \geqslant 0} (\zeta^r - \zeta^s) = \prod_{r>s} \eta^{r+s}(\eta^{r-s} - \eta^{-(r-s)})$$
$$= \prod_{r>s} \eta^{r+s} \prod_{r>s} \left(2i \sin \frac{(r-s)\pi}{p}\right) = i^{\frac{p(p-1)}{2}} 2^{\frac{p(p-1)}{2}} \prod_{r>s} \sin \frac{(r-s)\pi}{p},$$

puisque

$$\sum_{r>s}(r+s) = \sum_{r=1}^{p-1}\sum_{s=0}^{r-1}(r+s) = \sum_{r=1}^{p-1}\left(r^2 + \frac{r(r-1)}{2}\right) = 2p\left(\frac{p-1}{2}\right)^2$$

est divisible par $2p$. Comparons avec l'expression (17) de det A. Puisque $\sin \frac{(r-s)\pi}{p} > 0$ pour $0 \leqslant s < r < p-1$, alors dans (17) il faut prendre le signe plus. Ainsi

$$\det A = i^{\frac{p(p-1)}{2}} p^{\frac{p}{2}}.$$

D'autre part, nous avons

$$\det A = \prod_{k=1}^{p} \lambda_k = (-1)^b i^c (-i)^d p^{\frac{p}{2}} = i^{2b+c-d} p^{\frac{p}{2}}.$$

La réunion de ces deux résultats nous donne

$$2b + c - d \equiv p\frac{p-1}{2} \pmod 4,$$

d'où, en tenant compte de (14) et (16),

$$a-b = \frac{p+1}{2} - 2b \equiv \frac{p+1}{2} - \frac{p-1}{2} = 1 \pmod 4 \quad \text{pour} \quad p \equiv 1 \pmod 4,$$

$$c-d \equiv -\frac{p-1}{2} + 2b = -\frac{p-1}{2} + \frac{p+1}{2} = 1 \pmod 4 \quad \text{pour} \quad p \equiv 3 \pmod 4.$$

Les congruences obtenues montrent que, dans les égalités (16), les différences $a - b$ et $c - d$ sont égales à + 1. D'après (10), nous obtenons donc finalement

$$\tau(\chi) = \begin{cases} \sqrt{p} & \text{pour} \quad p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{pour} \quad p \equiv 3 \pmod 4. \end{cases}$$

La démonstration du théorème 7 dans le cas d'un module p premier est terminée.

Pour passer au cas général, nous utiliserons l'argument de l'exercice 4

du § 2. Cet exercice montre que la somme de Gauss normée $\tau(\chi)$ pour un caractère quadratique primitif χ modulo m s'exprime simplement au moyen des sommes de Gauss normées du caractère non unité modulo 4, des deux caractères primitifs modulo 8 et des caractères quadratiques modulo p premier impair. Puisque toutes ces sommes de Gauss sont connues (pour les modules 4 et 8, cf. exercices 10 et 11 de ce paragraphe), la formule de l'exercice 4 du § 2 permet de calculer explicitement $\tau(\chi)$. Considérons par exemple le caractère

$$\chi(x) = (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}}\frac{x}{0r}, \qquad (x, 2r) = 1$$

modulo $m = 8r$ oh r est un nombre naturel impair sans carrés. Si $r = p_1 \ldots p_s$ alors χ admet la décomposition

$$\chi(x) = (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}}\left(\frac{x}{p_1}\right)\cdots\left(\frac{x}{p_s}\right).$$

Désignons par α le nombre des nombres premiers $p_1, \ldots, p_s$ qui sont congrus à 3 (mod 4). Alors

$$\begin{aligned}\tau(\chi) &= 2i\sqrt{2}\,i^{\alpha}\sqrt{r}(-1)^{\frac{r^2-1}{8}+\frac{r-1}{2}}\left(\frac{2}{r}\right)\prod_{k<j}\left(\frac{p_k}{p_j}\right)\\ &= i^{\alpha+1}\sqrt{m}(-1)^{\frac{r-1}{2}+C_{\alpha}^{2}} = \sqrt{m}\,i^{\alpha+1+2\alpha+\alpha(\alpha-1)}\\ &= i^{(\alpha+1)^2}\sqrt{m} \begin{cases} = \sqrt{m} & \text{si} \quad \chi(-1) = (-1)^{\alpha+1} = 1,\\ = i\sqrt{m} & \text{si} \quad \chi(-1) = (-1)^{\alpha+1} = -1.\end{cases}\end{aligned}$$

De manière analogue, on calculerait les sommes $\tau(\chi)$ pour les autres caractères quadratiques primitifs.

La démonstration ci-dessus (pour un module premier) est due à Schur. Une autre démonstration, due à Kronecker, est contenue dans les exercices 13 à 16.

EXERCICES

1. Sachant qu'une unité fondamentale du corps $\mathbf{Q}(\sqrt{5})$ est égale à

$$\frac{1+\sqrt{5}}{2} = 2\cos\frac{\pi}{5},$$

calculer le nombre h pour ce corps, en utilisant la formule (2).

2. Calculer le nombre h pour les corps $\mathbf{Q}(\sqrt{-5})$ et $\mathbf{Q}(\sqrt{-23})$.

3. Démontrer que tout corps quadratique de discriminant D est un sous-corps du corps de division du cercle en $m = |D|$ parties.

4. Soient p un nombre premier impair et ζ une racine primitive $p^{\text{ième}}$ de 1. Démontrer que le corps cyclotomique $\mathbf{Q}(\zeta)$ contient un sous-corps quadratique et un seul. Ce sous-corps est $\mathbf{Q}(\sqrt{p})$ si $p \equiv 1 \pmod 4$ et $\mathbf{Q}(\sqrt{-p})$ si $p \equiv 3 \pmod 4$ (Pour résoudre cet exercice et le suivant, utiliser le théorème fondamental de la théorie de Galois).

5. Démontrer, indépendamment du théorème 2, que pourp $\equiv 1 \pmod 4$ premier le nombre

$$\frac{\prod_b \sin \frac{\pi b}{p}}{\prod_a \sin \frac{\pi a}{p}},$$

où a et b parcourent respectivement tous les résidus et non-résidus quadratiques modulo p de l'intervalle $\left(0, \frac{p}{2}\right)$ est une unité du corps quadratique $\mathbf{Q}(\sqrt{p})$. Démontrer de plus que la norme de cette unité est égale à -1.

6. Utilisant la deuxième partie de l'exercice 5, montrer que le nombre des classes de diviseurs du corps $\mathbf{Q}(\sqrt{p})$, $p \equiv 1 \pmod 4$ premier, est impair et que la norme d'une unité fondamentale de ce corps est égale à -1.

7. Démontrer que, pour tout module premier p de la forme $8n + 7$, il existe le même nombre de résidus et non-résidus quadratiques impairs dans l'intervalle $\left(0, \frac{p}{2}\right)$.

8. Démontrer que les caractères quadratiques primitifs n'existent que pour des modules m de la forme r, 4r et $8r$, r étant un entier naturel impair sans carrés (dans le cas d'un module impair $r > 1$). Montrer de plus que tous les caractères quadratiques primitifs sont épuisés par les caractères :

$$\chi(x) = \left(\frac{x}{r}\right), \quad (x, r) = 1, \quad \text{modulo r ;}$$

$$\chi(x) = (-1)^{\frac{x-1}{2}} \left(\frac{x}{r}\right), \quad (x, 2r) = 1, \quad \text{modulo } 4r ;$$

$$\left.\begin{aligned} \chi(x) &= (-1)^{\frac{x^2-1}{8}} \left(\frac{x}{r}\right), \\ \chi(x) &= (-1)^{\frac{x^2-1}{8} + \frac{x-1}{2}} \left(\frac{x}{r}\right), \end{aligned}\right\} (x, 2r) = 1, \text{ modulo } 8r.$$

9. Démontrer que tout caractère quadratique primitif χ modulo m pair (m = $4r$ ou $8r$, avec r impair) vérifie la formule

$$\chi\left(x + \frac{n}{2}\right) = -\chi(x).$$

10. Vérifier que la somme de Gauss normée pour le caractère

$$\chi(x) = (-1)^{\frac{X-1}{2}}, \quad (x,2)=1, \quad \text{modulo4}$$

est égale à $\tau_1(\chi) = 2i$.

11. Vérifier que pour les caractères primitifs

$$\chi'(x) = (-1)^{\frac{x^2-1}{8}} \quad \text{et} \quad \chi''(x) = (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}} \quad (2 \nmid x) \quad \text{modulo } 8,$$

les sommes de Gauss normées sont égales à

$$\tau_1(\chi') = 2\sqrt{2} \quad \text{et} \quad \tau_1(\chi'') = 2i\sqrt{2}.$$

12. Démontrer le théorème 7 pour un module quelconque.

13. Soient p un nombre premier impair et

$$\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}.$$

Posons

$$\delta = \prod_{x=1}^{\frac{p-1}{2}}(\zeta^x - \zeta^{-x}).$$

Démontrer que

$$\delta^2 = (-1)^{\frac{p-1}{2}}p.$$

Ainsi δ^2 coïncide avec le carré τ^2 de la somme de Gauss

$$\tau = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\zeta^x.$$

14. Avec les mêmes notations, montrer que

$$\left(\frac{-2}{p}\right)\delta = \begin{cases} \sqrt{p} & \text{pour} \quad p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{pour} \quad p \equiv 3 \pmod 4. \end{cases}$$

De plus, posant $A = 1 - \zeta$, montrer que dans l'ordre $\mathbf{Z}[\zeta]$ on a la congruence

$$\left(\frac{-2}{p}\right)\delta \equiv \left(\frac{p-1}{2}\right)!\,\lambda^{\frac{p-1}{2}} \pmod{\lambda^{\frac{p+1}{2}}}.$$

15. Démontrer que dans l'anneau $\mathbf{Z}[\zeta]$ on a la congruence

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\zeta^x = \tau \equiv \left(\frac{p-1}{2}\right)!\,\lambda^{\frac{p-1}{2}} \pmod{\lambda^{\frac{p+1}{2}}}.$$

Indication. — Développer la somme

$$\sum_{x=1}^{p-1} x^{\frac{p-1}{2}}(1-\lambda)^x$$

suivant les puissances de λ et utiliser le fait que

$$\sum_{x=1}^{p-1} x^m \equiv \begin{cases} 0 \pmod p \text{ pour } 0 < m < p-1, \\ -1 \pmod p \text{ pour } m = p-1. \end{cases}$$

16. Utilisant les deux exercices précédents, montrer que

$$\tau = \begin{cases} \sqrt{p} \text{ pour } p \equiv 1 \pmod 4, \\ i\sqrt{p} \text{ pour } p \equiv 3 \pmod 4. \end{cases}$$

§ 5. — NOMBRE DE CLASSES DE DIVISEURS DU CORPS DE DIVISION DU CERCLE EN UN NOMBRE PREMIER DE PARTIES ÉGALES

1) Décomposition du nombre h en deux facteurs

Les égalités (16) et (17) que nous avons obtenues dans le § 2 de ce chapitre donnent une formule finie (i. e. ne contenant ni séries ni produits infinis) pour le nombre h de classes de diviseurs du $m^{\text{ième}}$ corps cyclotomique). Cette formule cependant ne nous satisfait pas totalement car elle exprime le nombre h qui est par nature même un entier naturel, au moyen de quantités complexes et irrationnelles. Dans ce paragraphe, nous transformerons l'expression de h, en nous limitant cependant au cas d'un corps de division du cercle en un nombre premier de parties égales.

Soient donc $l = 2n + 1$ un nombre premier et $K = \mathbf{Q}(\zeta)$ le $l^{\text{ième}}$ corps cyclotomique. Pour faciliter cette étude, nous considérerons ici que K est un sous-corps du corps de tous les nombres complexes et nous conviendrons que ζ désigne la racine $\zeta = \cos \frac{2\pi}{l} + i \sin \frac{2\pi}{l}$ (il est nécessaire de fixer avec exactitude la racine ζ, pour des raisons analytiques). Calculons pour le corps K les quantités qui figurent devant le produit dans la formule (16) du § 2. Puisque le degré (K : Q) est égal à $l - 1$ (corollaire du théorème 1, § 2) et puisque tous les isomorphismes du K dans le corps des nombres complexes sont complexes (ici, ce sont en effet des automorphismes du corps K), alors $s = 0$, $t = \frac{l - 1}{2} = m$. Le nombre ω des racines de 1 qui appartiennent à K est égal à 21 d'après le lemme 3 du chapitre III, § 1. La norme du diviseur principal $\mathfrak{L} = (1 - \zeta)$ est égale à $N(B) = N(1 - \zeta) = l$ (cf. égalité (5) du chapitre III § 1). Par suite, le diviseur $\mathfrak{L}$ est premier et le nombre l admet, d'après le lemme 1 du chapitre III, § 1, la décomposi-

tion $l = \mathfrak{L}^{l-1}$. Il en résulte que le facteur F(s) dans la formule (12) du § 2 est égal à

$$F(s) = \left(1 - \frac{1}{N(\mathfrak{L})^s}\right)^{-1}\left(1 - \frac{1}{l^s}\right) = 1,$$

Calculons maintenant le discriminant du corps K.

THÉORÈME 1. — *Les nombres*

$$1, \zeta, \ldots) \ \zeta^{l-2}$$

forment une basé fondamentale du $l^{\text{ième}}$ ***corps*** *cyclotomique* $K = \mathbf{Q}(\zeta)$.

DÉMONSTRATION. — Puisque pour $s \not\equiv 0 \pmod{l}$ le polynôme caractéristique du nombre ζ^s est égal à $X^{l-1} + X^{l-2} + \ldots + X + 1$, alors

$$\operatorname{Tr} \zeta^s = \begin{cases} -1, & \text{si} \quad s \not\equiv 0 \pmod{l} \\ l - 1, & \text{si} \quad s \equiv 0 \pmod{E}. \end{cases} \tag{1}$$

Soit

$$a = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2} \qquad (a_i \in \mathbf{Q})$$

un nombre entier de K. Il nous faut démontrer que tous les coefficients a_i sont des nombres entiers rationnels. Puisque $\alpha\zeta^{-k} - \alpha\zeta$ est entier, alors la trace

$$\operatorname{Tr}(\alpha\zeta^{-k} - \alpha\zeta) = la_k - \sum_{i=0}^{I-2} a_i + \sum_{i=0}^{1-2} a_i = la_k$$

est un nombre entier rationnel ($0 \leqslant k \leqslant l - 2$). Posons $la_k = b_k$, $1 - \zeta = A$ et considérons le nombre

$$l\alpha = b_0 + b_1\zeta + \ldots + b_{l-2}\zeta^{l-2} = c_0 + c_1\lambda + \ldots + c_{l-2}\lambda^{l-2},$$

où les nombres b_k, de même que les c_k, sont des entiers rationnels. Montrons que les coefficients c_k sont tous divisibles par l. Si cette propriété a été établie pour $c_0, \ldots, c_{k-1}$ ($0 \leqslant k < l - 2$), alors nous considérerons cette dernière égalité comme une congruence modulo λ^{k+1} (dans l'anneau des nombres entiers du corps K). Puisque $l \equiv 0 \pmod{\lambda^{k+1}}$ (lemme 1 du chapitre III, § 1), alors cette congruence s'écrit

$$c_k\lambda^k \equiv 0 \pmod{\lambda^{k+1}} ;$$

il en résulte facilement que c_k est divisible par A, et cela entraîne, d'après le lemme 2 du chapitre III § 1, que c_k est divisible aussi par l. Ainsi, tous les coefficients c_k sont divisibles par l; mais alors tous les coefficients b_k sont également divisibles par l, i. e. tous les a_k sont des entiers. Le théorème 1 est démontré.

COROLLAIRE. — *Le discriminant du $l^{\text{ième}}$ corps cyclotomique, pour $l > 2$ premier, est égal à $(-1)^{\frac{l-1}{2}} l^{l-2}$.*

En effet, d'après la formule (1), le discriminant du corps K est égal au déterminant

$$\det (\operatorname{Tr} \zeta^{i+j})_{1 \leqslant i,j \leqslant l-1} = \begin{vmatrix} -1 & -1 & \dots & -1 \\ -1 & -1 & \dots & l-1 \\ \dots & \dots & \dots & \dots \\ -1 & l-1 & \dots & 1 \end{vmatrix}$$

d'ordre $l - 1$ (on remplace ici la base du théorème 1 par la base $\zeta, \zeta^2, \dots, \zeta^{l-1}$).

La formule (16) du § 2 s'écrit donc, dans le cas du $l^{\text{ième}}$ corps cyclotomique K, sous la forme

$$h = \frac{l^{\frac{l}{2}}}{2^{m-1}\pi^m R} \prod_{\chi \neq \chi_0} L(1, \chi), \tag{2}$$

où R est le régulateur du corps K, $m = \frac{l-1}{2}$; χ parcourt ici tous les caractères modulaires modulo l différents du caractère unité χ_0.

Puisque toutes les grandeurs qui sont à l'extérieur du produit dans la formule (2) sont réelles et positives, cette formule reste vraie en remplaçant chacun des facteurs $L(1, \chi)$ du produit par son module $|L(1, \chi)|$.

Tous les caractères $\chi \neq \chi_0$ modulo un nombre premier l sont primitifs; pour transformer l'expression de h, nous pourrons donc utiliser ultérieurement le théorème 3 du § 2. Dans ce but, séparons les caractères pairs et impairs. Soient g une certaine racine primitive fixée modulo l et θ une racine primitive de degré $l - 1$ de 1. Si nous désignons par χ le caractère modulo l tel que

$$\chi(g) = \theta^{-1},$$

toutes les puissances $\chi, \chi^2, \dots, \chi^{l-1} = \chi_0$ épuisent tout le groupe des caractères modulo l; par suite, tous les caractères χ^{2k} sont pairs et χ^{2k-1} impairs, puisque

$$\chi^s(-1) = \chi\left(g^{\frac{l-1}{2}}\right)^s = \theta^{-\frac{l-1}{2}s} = (-1)^s.$$

D'après la formule (20) du § 2 et le théorème 4 du chapitre premier § 2, pour les caractères pairs χ^{2k} $\left(1 \leqslant k \frac{l-3}{2}\right)$, nous avons

$$|L(1, \chi^{2k})| = \frac{|\tau(\chi^{2k})|}{l} \left| \sum_{r=0}^{l-2} \bar{\chi}^{-2k}(g^r) \operatorname{Log} |1 - \zeta^{g^r}| \right|$$

$$= \frac{1}{\sqrt{l}} \left| \sum_{r=0}^{l-2} \theta^{2kr} \operatorname{Log} |1 - \zeta^{g^r}| \right|.$$

Si nous prenons $r = \frac{l-1}{2} + s$, avec $0 \leqslant s < \frac{l-1}{2} = m$, alors, d'après la relation

$$1 - \zeta^{g^{m+s}} = 1 - \zeta^{-g^s}, \tag{3}$$

nous aurons l'égalité

$$\theta^{2k(m+s)} \operatorname{Log} \left| 1 - \zeta^{g^{m+s}} \right| = \theta^{2ks} \operatorname{Log} \left| 1 - \zeta^{g^s} \right|,$$

d'où

$$| L(1, \chi^{2k}) | = \frac{2}{\sqrt{l}} \left| \sum_{r=0}^{m-1} \theta^{2kr} \operatorname{Log} | 1 - \zeta^{g^r} | \right|.$$

De manière analogue, nous pouvons appliquer la formule (21) du § 2 aux caractères impairs χ^{2k-1}. Désignons par g_s le plus petit résidu positif du nombre g^s modulo l. Alors

$$\sum_{r=1}^{l-1} \bar{\chi}^{2k-1}(r) r = \sum_{s=0}^{l-2} \chi^{2k-1}(g^s)^{-1} g_s = \sum_{s=0}^{l-2} g_s \theta^{(2k-1)s} = F(\theta^{2k-1}),$$

où F désigne le polynôme

$$F(X) = \sum_{s=0}^{l-2} g_s X^s.$$

Par suite

$$| L(1, \chi^{2k-1}) | = \frac{\pi \sqrt{l}}{l^2} | F(\theta^{2k-1}) |.$$

Substituant dans l'égalité (2) les valeurs ainsi obtenues pour $| L(1, \chi^{2k}) |$, $1 \leqslant k \leqslant m - 1$ et $L | (1, \chi^{2k-1}) |$, $1 \leqslant k \leqslant m$, nous obtenons

$$h = h_0 h^* \tag{4}$$

après avoir posé

$$h_0 = \frac{2^{m-1}}{R} \prod_{k=1}^{m-1} \left| \sum_{r=0}^{m-1} \theta^{2kr} \operatorname{Log} | 1 - \zeta^{g^r} | \right|, \tag{5}$$

$$h^* = \frac{1}{(2l)^{m-1}} | F(\theta) F(\theta^3) \ldots F(\theta^{l-2}) |. \tag{6}$$

Dans les points suivants, nous démontrerons que chacun des nombres h_0 et h^* est un entier naturel. La formule (4) donne donc une représentation du nombre h comme produit de deux entiers naturels.

Remarque 1. — Parfois, on désigne h^* par h_1 et h_0 par h_2 et on les appelle respectivement ***premier et deuxième facteurs du nombre h.***

Remarque 2. — Le facteur h_0 est égal au nombre de classes de diviseurs du sous-corps $\mathbf{Q}(\zeta + \zeta^{-1})$ de degré $\frac{l-1}{2}$ formé de tous les nombres réels du corps $\mathbf{Q}(\zeta)$ (cf. exercices 1 à 4).

2) Le facteur h_0

Pour simplifier l'écriture, introduisons la notation

$$a_r = \operatorname{Log} |1 - \zeta^{g^r}|, \qquad r \geqslant 0.$$

D'après l'égalité (3), pour tout $r \geqslant 0$ nous avons l'égalité $a_{r+} = a_r$. Cela signifie que les valeurs a_r dépendent seulement du résidu du nombre r modulo $m = \frac{l-1}{2}$. Si nous posons

$$A = \prod_{k=1}^{m-1} \left(\sum_{r=0}^{m-1} \theta^{2kr} a_r \right),$$

la formule (5) s'écrit sous la forme

$$h_0 = \frac{2^{m-1}}{R} |A|. \tag{7}$$

Montrons que le produit

$$(a_0 + a_1 + \ldots + a_{m-1})A$$

est égal, au signe près, au déterminant

$$\Delta = \det (a_{i+j})_{0 \leqslant i,\, j \leqslant m-1} = \begin{vmatrix} a_1 & a_2 & \ldots & a_0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{m-1} & a_m & \ldots & a_{m-2} \end{vmatrix}$$

Considérons le groupe cyclique G d'ordre m engendré par la racine primitive θ^2 de degré m de 1. Les fonctions χ_k, $0 \leqslant k \leqslant m-1$, $\chi_k(\theta^{2r}) = \theta^{2kr}$, sont, c'est clair, les caractères du groupe G. Définissons sur le groupe G la fonction f en posant $f(\theta^{2r}) = a_r$. D'après l'exercice 13 du § 5 de l'appendice, notre produit s'écrit alors

$$\prod_{k=0}^{m-1} \left(\sum_{r=0}^{m-1} \theta^{2kr} a_r \right) = \prod_{k=0}^{m-1} \left(\sum_{r=0}^{m-1} \chi_k(\theta^{2r}) f(\theta^{2r}) \right)$$

$$= \det (f(\theta^{2(i-j)})) = \det (a_{i-j})_{0 \leqslant i,\, j \leqslant m-1}.$$

Remarquant que les matrices (a_{i-j}) et (a_{i+j}) diffèrent l'une de l'autre seulement par l'ordre des colonnes, nous obtenons le résultat désiré.

La somme a, + a, + . . . + a_{m-1} est différente de zéro puisque

$$a_0 + a_1 + \ldots + a_{m-1} = \operatorname{Log} \left| \prod_{r=0}^{m-1} (1 - \zeta^{g^r}) \right| = \operatorname{Log} \sqrt{l}, \qquad (8)$$

d'après la relation (5) du chapitre III, § 1 et la formule (3). C'est pourquoi, si nous mettons en facteur le nombre (8) dans le déterminant A, nous obtenons une nouvelle expression pour A. Ajoutant dans A toutes les colonnes à l'une d'entre elles, nous obtenons une colonne dont tous les éléments sont égaux à la somme (8). Ainsi, au signe près, A est égal au déterminant A' obtenu à partir de A en remplaçant tous les nombres d'une colonne par 1. Si maintenant nous soustrayons la première ligne des autres, nous obtenons que le nombre | A | est égal à la valeur absolue de l'un des mineurs d'ordre $m - 1$ de la matrice

$$(a_{i+j} - a_j)_{\substack{1 \leqslant i \leqslant m-1 \\ 0 \leqslant j \leqslant m-1}}. \qquad (9)$$

Considérons la racine primitive

$$\eta = -\zeta^{\frac{l+1}{2}} = \cos \frac{\pi}{l} + i \sin \frac{\pi}{l}$$

de degré 21 de 1. Puisque $\eta^2 = \zeta$, alors

$$\frac{1 - \zeta^k}{1 - \zeta} = \eta^{k-1} \frac{\eta^k - \eta^{-k}}{\eta - \eta^{-1}} = \eta^{k-1} \frac{\sin \frac{k\pi}{l}}{\sin \frac{\pi}{l}}.$$

Pour $k \not\equiv 0 \pmod{l}$, le rapport de gauche est une unité du corps K (cf. démonstration du lemme 1 du chapitre III, § 1); par suite, les nombres

$$\theta_k = \frac{\sin \frac{k\pi}{l}}{\sin \frac{\pi}{l}} \qquad (10)$$

sont aussi des unités du corps K pour tout $k \not\equiv 0 \pmod{l}$. Il est clair que ces unités, réelles pour $1 \leqslant k < 1$, sont positives.

Il existe $m = \dfrac{l-1}{2}$ paires d'isomorphismes complexes du corps K dans le corps des nombres complexes. Puisque les nombres $\zeta, \zeta^g, \ldots, \zeta^{g^{m-1}}$ ne sont pas conjugués, les isomorphismes

$$\sigma_j : \zeta \to \zeta^{g^j} \qquad (j = 0, 1, \ldots m\text{-}1)$$

ne sont pas deux à deux conjugués (pour tout σ_j, l'isomorphisme conjugué est l'isomorphisme $\zeta \to \zeta^{-g^j} = \zeta^{g^{m+j}}$). Désignons par $\bar{r}$ la valeur absolue du plus petit résidu (en valeur absolue) du nombre g^r (modulo l). Alors

$$\frac{1-\zeta^{g^r}}{1-\zeta} = \pm \eta_1^{g^r-1}\theta_{\bar{r}}.$$

Transformant cette égalité par l'automorphisme σ_j, nous obtenons

$$\frac{1-\zeta^{g^{r+j}}}{1-\zeta^{g^j}} = \pm (\sigma_j\eta_1)^{g^r-1}\sigma_j(\theta_{\bar{r}}),$$

d'où, en prenant les logarithmes des modules,

$$a_{r+j} - a_j = \operatorname{Log} |\sigma_j(\theta_{\bar{r}})|. \tag{11}$$

Montrons que si r prend les valeurs $1, \ldots, m-1$ alors $\bar{r}$ parcourt les nombres $2, \ldots, m$. En effet, si $g^i \equiv \pm g^j \pmod{l}$, $1 \leqslant i \leqslant m-1$, alors $g^{j-i} \equiv \pm 1 \pmod{l}$ et $0 \leqslant j - i \leqslant \frac{l-3}{2}$ et cela n'est possible que pour $j - i = 0$. Il en résulte que les valeurs $\bar{r}$ sont deux à deux distinctes et, puisqu'elles satisfont à l'inégalité $2 \leqslant \bar{r} \leqslant m = \frac{l-1}{2}$, en nombre égal à $m-1$, alors chacun des nombres $2, \ldots, m$ est un $\bar{r}$.

D'après l'égalité (11), nous obtenons ainsi que la matrice (9) ne se distingue de la matrice

$$(\operatorname{Log} |\sigma_j(\theta_k)|)_{\substack{2 \leqslant k \leqslant m \\ 0 \leqslant j \leqslant m-1}} \tag{12}$$

que par l'ordre des lignes; par suite le module $|A|$ est égal à la valeur absolue de l'un des mineurs d'ordre $m-1$ de la matrice (12).

Revenons maintenant au système d'unités fondamentales du corps K. D'après le lemme 4 du chapitre III, § 1, toute unité du corps K est le produit d'une puissance de ζ par une unité réelle. D'après cela, on peut choisir les unités fondamentales $\varepsilon_1, \ldots, \varepsilon_{m-1}$ réelles positives. Il est clair que toute unité réelle positive s'écrit alors sous la forme $\varepsilon_1^{c_1} \ldots \varepsilon_{m-1}^{c_{m-1}}$, les c_i étant des entiers rationnels. Dans notre cas, les fonctions $l_j(\alpha)$, $a \in K$, introduites dans le chapitre II, § 3-3) s'écrivent

$$l_j(\alpha) = \operatorname{Log} |\sigma_j(\alpha)|^2 = 2 \operatorname{Log} |\sigma_j(\alpha)|, \qquad 0 \leqslant j \leqslant m-1.$$

Pour les unités fondamentales $\varepsilon_1, \ldots, \varepsilon_{m-1}$, formons la matrice

$$(\operatorname{Log} |\sigma_j(\varepsilon_i)|)_{\substack{1 \leqslant i \leqslant m-1 \\ 0 \leqslant j \leqslant m-1}}. \tag{13}$$

Puisque la matrice (6) du chapitre II § 4 s'obtient en multipliant par 2 toutes les lignes de (13), alors, par définition du régulateur R, la valeur absolue d'un des mineurs d'ordre $m - 1$ de la matrice (13) est égale à $\frac{R}{2^{m-1}}$.

Toutes les unités θ_k de la forme (10) pour $k = 2, \ldots, m$ sont réelles positives et par suite elles s'écrivent au moyen des unités fondamentales sous la forme

$$\theta_k = \prod_{i=1}^{m-1} \varepsilon_i^{c_{ki}} \qquad (k = 2, \ldots, m)$$

pour des entiers rationnels c_{ki}. D'après les égalités

$$\operatorname{Log} | \sigma_j(\theta_k) | = \sum_{i=1}^{m-1} c_{ki} \operatorname{Log} | \sigma_j(\varepsilon_i) |,$$

la matrice (12) est le produit de la matrice (c_{ki}) par la matrice (13). Il en résulte que tout mineur d'ordre $m - 1$ de la matrice (12) est égal au produit de $\det (c_{ki})$ par le mineur correspondant de la matrice (13), i. e.

$$| A | = | \det (c_{ki}) | \frac{R}{2^{m-1}}.$$

Comparant cette égalité avec l'égalité (7), nous obtenons finalement

$$h_0 = | \det (c_{kj}) |.$$

Puisque tous les c_{kj} sont des entiers rationnels et $h_0 \neq 0$, on a bien démontré ainsi que h_0 est un entier naturel. De plus, d'après le lemme 1 du chapitre II § 6, nous avons aussi obtenu le résultat suivant.

THÉORÈME 2. — *Le facteur h_0 du nombre de classes de diviseurs du $l^{\text{ième}}$ corps cyclotomique* K *est égal à l'indice* (E : E,) *du groupe* E_0 *engendré par les unités*

$$\theta_k = \frac{\sin \frac{k\pi}{l}}{\sin \frac{\pi}{l}} \qquad \left(k = 2, \ldots, \frac{l-1}{2}\right)$$

du corps K *dans le groupe* E *de toutes les unités réelles positives du corps K.*

En liaison avec la remarque 2 de la fin du point 1), on comparera ce résultat au théorème 2 du paragraphe précédent.

3) Le facteur h^*

Démontrons que le nombre h^*, défini par l'égalité (6), est aussi un entier naturel.

Le produit

$$B = F(8)\, F(\theta^3) \ldots F(\theta^{l-2})$$

est tout d'abord un entier algébrique du corps Q(0) où θ est une racine primitive d'ordre $l - 1$ de 1. D'autre part, il est rationnel, puisque, d'après (4) et (6), $|B| = \frac{h}{h_0}(2l)^{m-1}$. Par suite, B est un entier rationnel et il nous reste à vérifier que B est divisible par 2^{m-1} et par l^{m-1} (par hypothèse, $l \neq 2$). Vérifions la première condition.

Comme dans le point 1), nous désignerons par g_s le plus petit résidu positif du nombre g^s modulo l, g étant une racine primitive fixée modulo l. Puisque

$$g_{m+s} + g_s \equiv g^{m+s} + g^s = g^s\left(g^{\frac{l-1}{2}} + 1\right) \equiv 0 \pmod{l},$$

alors

$$g_{m+s} + g_s = l.$$

Il en résulte que les nombres g_{m+s} et g_s sont de parités différentes. Considérons des congruences modulo 2 dans l'anneau des nombres entiers du corps Q(0). D'après l'égalité $\theta^m = -1$, nous aurons, pour k impair,

$$F(\theta^k) = \sum_{s=0}^{m-1}(g_s\theta^{ks} + g_{m+s}\theta^{k(m+s)}) = \sum_{s=0}^{m-1}(g_s - g_{m+s})\theta^{ks} \equiv \sum_{s=0}^{m-1}\theta^{ks} \pmod{2},$$

d'où

$$F(\theta^k)(1 - \theta^k) \equiv 0 \pmod{2}.$$

Cela montre que le produit

$$B(1 - e)(1 - \theta^3)\ldots(1 - \theta^{l-2})$$

est divisible par 2^m. D'autre part, puisque θ et θ^2 sont respectivement des racines primitives d'ordre $l - 1$ et $\frac{l-1}{2}$ de 1, alors

$$l - 1 = \prod_{k=1}^{I-2}(1 - \theta^k), \qquad \frac{l-1}{2} = \prod_{s=1}^{m-1}(1 - \theta^{2s}),$$

d'où

$$(1 - \theta)(1 - \theta^3)\ldots(1 \quad \theta^{l-2}) = 2.$$

On a ainsi démontré que B est divisible par 2^{m-1}.

Pour démontrer que B est divisible par l^{m-1}, trouvons tout d'abord la décomposition du nombre l comme produit de diviseurs premiers du corps $\mathbf{Q}(\theta)$. Puisque l est premier avec $l - 1$ et $l \equiv 1 \pmod{l - 1}$ alors, d'après le théorème 2 du § 2, le nombre l se décompose en un produit de $\varphi(l - 1)$ diviseurs premiers distincts, la norme de chacun d'eux étant égale à l. Soit q un de ces diviseurs premiers. Les nombres 0, 1, θ, . . . , θ^{l-2} sont

non congrus deux à deux modulo q (cf. démonstration du lemme 3 du § 2) et forment donc un système complet de résidus modulo q. D'après la congruence

$$1 - g^{l-1} = \prod_{k=0}^{l-2}(1 - \theta^k g) \equiv 0 \pmod{l}, \tag{14}$$

q divise une des différences $1 - \theta^k g$. Si $1 - \theta^k g \equiv 0 \pmod{q}$ et

$$1 - \theta^s g \equiv 0 \pmod{q}$$

alors $\theta^k \equiv \theta^s \pmod{q}$, d'où $\theta^k = \theta^s$. Ainsi q divise une et une seule des différences $1 - \theta^k g$ de la décomposition (14). Montrons que ce k est premier avec $l - 1$. Si $(k, l - 1) = d$, alors, élevant la congruence $1 \equiv \theta^k g \pmod{q}$ à la puissance $\frac{l-1}{d}$, nous obtenons que $g^{\frac{l-1}{d}} - 1$ est divisible par q et par suite aussi par l et cela n'est possible que pour $d = 1$.

Si un entier $a \in \mathbf{Q}(\theta)$ est divisible par $\mathfrak{q}|l$, alors N(a) est divisible par $N(\mathfrak{q}) = l$. Réciproquement, si $N(a)$ est divisible par l, alors a est divisible par l'un au moins des diviseurs premiers qui figurent dans l. Toutes les $\varphi(l - 1)$ différences $1 - \theta^k g$ telles que k soit premier avec $l - 1$ ont la même norme et cette norme est divisible par 1. C'est pourquoi chacune de ces différences est divisible par un des diviseurs premiers figurant dans l.

Nous avons ainsi montré que pour tout k premier avec $l - 1$, il existe un diviseur premier divisant l et un seul (que nous désignerons par $\mathfrak{q}_k$) tel que

$$1 - \theta^k g \equiv 0 \pmod{\mathfrak{q}_k} \tag{15}$$

et que pour tout s qui n'est pas premier avec $l - 1$ la différence $1 - \theta^s g$ n'est divisible par aucun des diviseurs premiers $\mathfrak{q}_k$. La décomposition du nombre l dans le corps $\mathbf{Q}(\theta)$ peut s'écrire sous la forme

$$l = \prod_{(k,l-1)=1} \mathfrak{q}_k,$$

où k parcourt un système réduit de résidus modulo $l - 1$.

Revenons à la question de la divisibilité du nombre B par l^{m-1}. Puisque dans l'anneau des nombres entiers du corps Q(0) on a la congruence

$$F\theta^{(k)}(1 - g\theta^k) \equiv \sum_{s=0}^{l-2} g(\theta^k)^s(1 - g\theta^k) = 1 - (g\theta^k)^{l-1} = 1 - g^{l-1} \equiv 0 \pmod{l},$$

alors F(W) $(1 - g\theta^k)$ est divisible par l. Il résulte donc de ce qui précède que $F(\theta^k)$ est divisible par l pour $(k, l - 1) > 1$ et divisible par $l\mathfrak{q}_k^{-1}$ pour

(k, $l-1$) = 1. Convenons que, pour (k, $l-1$) > 1, q_k désigne le diviseur unité; on pourra dire ainsi que $F(\theta^k)$ est divisible par lq_k^{-1} pour tout k. Le produit B = F(8) $F(\theta^3)$ . . . $F(\theta^{l-2})$ est donc divisible par

$$l^m \prod_{k=1,3,\ldots,l-2} q_k^{-1} = l^m \prod_{(k,l-1)=1} q_k^{-1} = l^{m-1}.$$

Ainsi, nous avons démontré que h^* est un nombre entier.

4) Critère pour que h^* et l soient premiers entre eux

Dans le chapitre III, § 7-3) nous avons vu l'importance d'un critère permettant d'affirmer si h et l sont premiers entre eux ou pas, i. e. si le nombre premier l est régulier ou irrégulier. Puisque $h = h_0 h^*$, le nombre l sera régulier si et seulement si aucun des deux facteurs h_0 et h^* n'est divisible par l. Nous donnerons dans ce point une condition nécessaire et suffisante pour que le facteur h^* ne soit pas divisible par l. Puisque nous verrons dans le paragraphe suivant que si $(h^*, l) = 1$, alors h_0 n'est pas non plus divisible par l, cette condition est également un critère de régularité de l.

Conservant les notations du point précédent, considérons la relation

$$\frac{B}{p-1} = \prod_{k=1,3,\ldots,l-2} \frac{F(\theta^k)q_k}{l} \qquad (16)$$

(nous identifions ici le diviseur principal (α) et le nombre α). D'après la formule (6), le nombre h^* est divisible par l si et seulement le nombre entier rationnel (16) est divisible par un des diviseurs premiers q_s, $(s, l-1) = 1$, disons par $q_{l-2} = q_{-1}$, i. e. si l'un au moins des diviseurs entiers $F(\theta^k)q_k l^{-1}$ (k = 1, 3, . . ., $l-2$) est divisible par q_{-1}. Pour cela, de nouveau, il faut et il suffit que l'un au moins des entiers k = 1, 3, . . . , $l-2$, le diviseur $F(\theta^k)q_k$ soit divisible par q_{-1}^2. Montrons que, pour $k = l-2 \equiv -1 \pmod{l-1}$ cette dernière condition est impossible. En effet, d'après (15), $\theta_g^{-1} \equiv 1 \pmod{q_{-1}}$, d'où

$$F(\theta^{-1}) = \sum_{r=0}^{l-a} (\theta^{-1}g)^r \equiv l-1 \equiv -1 \pmod{q_{-1}},$$

i. e. $F(\theta^{-1})$ n'est pas divisible par q_{-1}; par suite $F(\theta^{-1})q_{-1}$ n'est pas divisible par q_1^2. Ainsi, pour que h^* soit divisible par l, il faut et il suffit que pour un des entiers k = 1, 3, . . . , $l-4$ le nombre $F(\theta^k)$ soit divisible par q_{-1}^2.

Jusqu'à présent, nous n'avons pas précisé le choix de la racine primitive g modulo 1. Nous supposerons maintenant que g satisfait à la congruence

$$g^{l-1} \equiv 1 \pmod{l^2}$$

(si g ne satisfait pas à cette condition, on le remplacera par g + xl pour un x convenable). Puisque la congruence (14) est maintenant satisfaite modulo l^2, alors 1 — $\theta^k g$ est divisible par q_k^2 pour tout k premier avec l 1. En particulier

$$\theta \equiv g \pmod{q_{l-1}^2}.$$

Pour un tel choix de g, on peut trouver très simplement la condition de divisibilité de $F(\theta^k)$ par q_{l-1}^2. En effet, d'après la congruence

$$F(\theta^k) = \sum_{s=0}^{l-2} g_s \theta^{sk} \equiv \sum_{s=0}^{l-2} g_s g^{sb} \pmod{q_{l-1}^2},$$

le nombre $F(\theta^k)$ est divisible par q_{l-1}^2 si et seulement si

$$\sum_{s=0}^{l-2} g_s g^{sk} \equiv 0 \pmod{l^2}. \tag{17}$$

Pour transformer la condition (17) en une condition plus maniable, considérons les congruences

$$g_s \equiv g^s + l a_s \pmod{l^2}, \qquad 0 \leqslant s \leqslant l-2, \tag{18}$$

où les a_s sont des nombres entiers. Si nous élevons à la puissance $k+1$ ($k = 1, 3, \ldots, l-4$) la congruence (18), nous obtenons

$$g_s^{k+1} \equiv g^{s(k+1)} + (k+1) g^{sk} l a_s \equiv g^{s(k+1)} + (k+1) g^{sk} (g_s - g^s) \pmod{l^2},$$

i. e.

$$g_s^{k+1} \equiv (k+1) g_s g^{sk} - k g^{s(k+1)} \pmod{l^2}. \tag{19}$$

Sommons les congruences (19) pour $s = 0, 1, \ldots, l-2$. Pour $g^{k+1} \not\equiv 1 \pmod{l}$ pour $k+1 \leqslant l-3$ et $g^{l-1} \equiv 1 \pmod{l^2}$, alors

$$\sum_{s=0}^{l-2} g^{s(k+1)} = \frac{g^{(l-1)(k+1)} - 1}{g^{k+1} - 1} \equiv 0 \pmod{l^2}$$

et, par suite,

$$\sum_{s=0}^{l-2} g_s^{k+1} \equiv (k+1) \sum_{s=0}^{l-2} g_s g^{sk} \pmod{l^2}.$$

Mais $k+1 \not\equiv 0 \pmod{l}$; la condition (17) équivaut donc à la congruence

$$S_{k+1} = \sum_{s=0}^{l-2} g_s^{k+1} = \sum_{n=1}^{l-1} n^{k+1} \equiv 0 \pmod{l^2}.$$

Nous avons ainsi démontré le théorème suivant.

THÉORÈME 3. — ***Pour que le nombre h* ne soit pas divisible par l, il faut et il suffit que l'un des nombres***

$$S_k = \sum_{n=1}^{l-1} n^k \qquad (k = 2, 4, \ldots, l-3) \tag{20}$$

ne soit pas divisible par l^2.

Remarquons que tous les nombres S_k pour $k \not\equiv 0 \pmod{l-1}$ sont divisibles par l (cf. congruence (10) du § 8).

Exprimons le théorème 3 en utilisant les nombres de Bernoulli (la définition et certaines propriétés de ces nombres sont étudiées dans le § 8). Puisque les nombres 2, 4, . . . , $l-3$ ne sont pas divisibles par $l-1$, alors, d'après le théorème 4 du § 8, les nombres de Bernoulli $B_2, B_4, \ldots, B_{l-3}$ sont Z-entiers (i. e. leurs dénominateurs ne contiennent pas l). De plus, les sommes S_k satisfont aux congruences

$$S_k \equiv B_k l \pmod{l^2} \qquad (k = 2, 4, \ldots l-3) \tag{21}$$

(dans l'anneau des nombres I-entiers; cf. congruence (II) du § 8). On a donc le théorème suivant.

THÉORÈME *4.* — ***Le nombre h* n'est pas divisible par l si et seulement si les numérateurs des nombres de Bernoulli $B_2, B_4, \ldots, B_{l-3}$ ne sont pas divisibles par l.***

Par exemple, puisque les numérateurs des nombres $B_2, B_4, B_6, B_8, B_{10}, B_{12}, B_{14}$ ne sont pas divisibles par 17, alors $l = 17$ est régulier.

Remarque. — Pour démontrer que le nombre h^* est premier avec l, il n'est pas indispensable de déterminer les valeurs précises des nombres de Bernoulli. Il suffit de considérer les relations récurrentes (2) du § 8 comme des congruences modulo l et de déterminer à partir de ces congruences des nombres $B_2, B_4, \ldots, B_{l-3}$. h^* sera alors premier avec l si et seulement si aucun de ces nombres n'est divisible par 1.

EXERCICES

1. Soit K_0 le sous-corps de tous les nombres réels du $l^{\text{ième}}$ corps cyclotomique $Q(\zeta)$, $\zeta^l = 1$. Montrer que K_0 coïncide avec $Q(\zeta + \zeta^{-1})$ et est de degré $\frac{l-1}{2}$.

Démontrer de plus que le discriminant du corps K_0 est égal à $l^{\frac{l-3}{2}}$ et que son régulateur R_0 est lié au régulateur R du corps $Q(\zeta)$ par la relation $R = 2^{\frac{l-3}{2}} R_0$.

2. Soient p premier différent de l et f le plus petit entier naturel tel que $pf \equiv 1 \pmod{l}$. Démontrer que le nombre p se décompose dans le corps $\mathbf{K}_0$ en un produit de $\frac{l-1}{2f}$ diviseurs premiers de degrés f pour f impair et en un produit de $\frac{l-1}{f}$ diviseurs premiers de degré $\frac{f}{2}$ pour f pair.

3. Démontrer que la fonction zêta $\zeta_{\mathbf{K}_0}(s)$ du corps $\mathbf{K}_0$ vérifie la relation

$$\lim_{s \to 1+0} (s-1)\zeta_{\mathbf{K}_0}(s) = \prod_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} L(1, \chi),$$

où χ parcourt tous les caractères numériques pairs modulo l distincts du caractère unité χ_0.

4. Démontrer que le nombre de classes de diviseurs du sous-corps réel $\mathbf{Q}(\zeta + \zeta^{-1})$ du $l^{\text{ième}}$ corps cyclotomique est égal au facteur h_0 du nombre de classes du corps $\mathbf{Q}(\zeta)$.

5. Démontrer pour le facteur h^* la formule

$$h^* = \frac{1}{(2l)^{m-1}} \left| \det \left(g_{m+i+j} - g_{i+j}\right)_{0 \leqslant i,j \leqslant m-1} \right|,$$

où g_s est le plus petit résidu positif du nombre g^s modulo $l = 2m + 1$ (g est une racine primitive modulo l).

6. Calculer le facteur h^* pour $l = 7$.

7. Montrer que le nombre premier 37 est irrégulier.

§ 6. — CONDITION DE RÉGULARITÉ

Le but de ce paragraphe est d'établir que si le facteur h^* du nombre de classes de diviseurs du $l^{\text{ième}}$ corps cyclotomique n'est pas divisible par l, le facteur h_0 n'est pas non plus divisible par l et par suite le nombre premier l est régulier. Nous démontrerons de plus ici que si l est régulier toute unité du corps K = Q(T) est congrue modulo l à la puissance $l^{\text{ième}}$ d'un nombre entier rationnel. C'est sur cet argument, appelé lemme de Kummer, que repose la démonstration du deuxième cas du théorème de Fermat pour des exposants réguliers. Comme autre conséquence de la régularité, comme nous l'avons vu, si $l \nmid h^*$, dans le complété Sadique $\mathbf{K}_\mathfrak{L}$ du corps $K = \mathbf{Q}(\zeta)$, $\mathfrak{L} = (1 - \zeta)$, les valeurs $\operatorname{Log} \theta_k^{l-1}$, $k = 2, 3, \ldots, \frac{l-1}{2}$ forment une base de l'ensemble des nombres entiers « réels » Sadiques dont la trace est nulle (les unités θ_k sont définies par les égalités (10) du § 5).

1) **Le corps des nombres Sadiques**

Comme nous le savons, le corps cyclotomique K = **Q(C),**

$$\zeta = \cos\frac{2x}{l} + i\sin\frac{2\pi}{l}$$

pour l premier $\geqslant 3$ est de degré $l - 1$ et la décomposition de l en facteurs premiers dans ce corps s'écrit $l = \mathfrak{L}^{l-1}$, où $\mathfrak{L} = (1 - \zeta)$ est un diviseur premier de degré 1.

Considérons le complété $\mathfrak{L}$-adique $K_{\mathfrak{L}}$ du corps K; nous appellerons nombres Sadiques les éléments de ce complété. Le corps complet $K_{\mathfrak{L}}$ contient un sous-corps isomorphe de manière naturelle au corps $\mathbf{Q}_l$ des nombres l-adiques (ce sous-corps est l'adhérence du corps Q dans $K_{\mathfrak{L}}$. D'après cet isomorphisme naturel, on peut considérer que $\mathbf{Q}_l \subset K_{\mathfrak{L}}$.

Puisque $\mathfrak{L}$ est l'unique diviseur premier qui divise l, alors, d'après le théorème 1 du chapitre IV, § 2, le degré de l'extension $K_{\mathfrak{L}}/\mathbf{Q}_l$ est égal à $l - 1 = (K : \mathbf{Q})$. Il en résulte (cf. (6), chap. IV, § 2) que pour tout $\alpha \in K$ on a l'égalité

$$N_{K/R}(\alpha) = N_{K_{\mathfrak{L}}/\mathbf{Q}_l}(\alpha). \qquad (1)$$

LEMME 1. — *Dans l'anneau des nombres entiers !Sadiques il existe un élément premier* λ *tel que* :

1° $\qquad A'^{-1} + l = 0$

2° $\qquad \lambda \equiv \zeta - 1 \pmod{A''}$.

Les conditions 1° *et* 2° *définissent de manière unique l'élément* λ.

D'après l'égalité (5) du chapitre III, § 1, nous avons

$$\frac{1}{(1-\zeta)^{l-1}} = (1+\zeta)(1+\zeta+\zeta^2)\ldots(1+\zeta+\ldots+\zeta^{l-2}).$$

Passons ici à la congruence correspondante modulo l'élément premier $1 - \zeta$ du corps $K_{\mathfrak{L}}$ (rappelons que $v_{\mathfrak{L}}(1 - \zeta) = 1$). Puisque $\zeta \equiv 1 \pmod{1 - \zeta}$ et $(l - 1)! + 1 \equiv 0 \pmod{l}$ (théorème de Wilson), alors

$$\frac{l}{(1-\zeta)^{l-1}} \equiv 2.3.\ldots.(l-1) \equiv 1 \pmod{(1-\zeta)}.$$

Montrons que l'unité $\mathfrak{L}$-adique

$$\alpha = \frac{-l}{(1-\zeta)^{l-1}},$$

congrue à 1 modulo $1 - \zeta$, peut s'écrire sous la forme $a = \gamma^{l-1}$. Considérons pour cela le polynôme $F(X) = X^{l-1} - a$. Puisque $F(1) \equiv 0 \pmod{1 - \zeta}$

et F'(1) $\not\equiv 0 \pmod{1-\zeta}$, alors il existe une unité y de $\mathbf{K}_{\mathfrak{L}}$ telle que F(y) $= 0$ (cf. fin du point 2) du chapitre IV, § 1). Ainsi a = γ^{l-1} convient. Posant maintenant A = $(\zeta - 1)\gamma$, nous obtenons un élément premier λ possédant les propriétés demandées. Tout autre λ_1 satisfaisant à la première condition du lemme s'écrit $\lambda\theta$ où θ est une racine d'ordre l 1 de 1. Mais de la congruence $\lambda\theta \equiv$ A (mod λ^2) résulte que $\theta \equiv 1 \pmod{A}$. Si la racine θ était différente de 1, alors l 1 serait divisible par A, ce qui est impossible. Ainsi θ = 1, d'où A, = A. Le lemme 1 est complètement démontré.

Dans la suite, sauf mention expresse du contraire, nous désignerons par A l'élément du corps $\mathbf{K}_{\mathfrak{L}}$ défini de manière unique par les conditions du lemme 1.

Pour tout k premier avec l, la correspondance $\zeta \to \zeta^k$ définit l'automorphisme σ_k de l'extension $\mathbf{K}/\mathbf{Q}$. Si σ est l'un de ces automorphismes, alors la fonction $v'(a) = v_{\mathfrak{L}}(\sigma(\alpha))$, a $\in$ K est une valuation du corps K qui prolonge la valuation l-adique v_l du corps Q. Mais v_l n'admet qu'un seul prolongement au corps K, qui est donc vs. Par suite, $v' = v_{\mathfrak{L}}$ et cela signifie que $v_{\mathfrak{L}}(\sigma(\alpha)) = v_a(a)$ pour tout a $\in$ K. Ainsi, la suite de l'image par l'automorphisme σ d'une suite de Cauchy d'éléments de K (pour la métrique qui correspond au diviseur premier 0) est une suite de Cauchy. Cela permet de prolonger au corps $\mathbf{K}_{\mathfrak{L}}$ l'automorphisme $\sigma = \sigma_k$ du corps K : si

$$\xi = \lim_{n \to +\infty} (\alpha_n), \qquad \alpha_n \in \mathbf{K},$$

alors on peut poser

$$\sigma(\xi) = \lim_{n \to \infty} \sigma(\alpha_n)$$

(on vérifie facilement que $\sigma(\xi)$ ne dépend pas du choix de la suite { a, } et que l'application $\xi \to \sigma(\xi)$ est un automorphisme de l'extension $\mathbf{K}_{\mathfrak{L}}/\mathbf{Q}_l$).

Puisque le degré résiduel de l'extension $\mathbf{K}_{\mathfrak{L}}/\mathbf{Q}_l$ est égal à 1 et son indice de ramification à l — 1, alors, d'après le théorème 4 du chapitre IV, § 1, tout nombre entier $\mathfrak{L}$-adique s'écrit de manière unique sous la forme

$$a_0 + a_1\lambda + \ldots + a_{l-2}\lambda^{l-2}, \tag{2}$$

pour des a_i entiers I-adiques.

Le sous-corps des nombres réels du corps K est formé des $a \in$ K qui sont invariants par l'automorphisme $\sigma_{-1} : \zeta \to \zeta^{-1}$. Cherchons les nombres $\mathfrak{L}$-adiques qui sont invariants par σ_{-1}. Puisque $\lambda^{l-1} = -l$, alors

$$(\sigma_{-1}(\lambda))^{l-1} = -l,$$

ce qui exprime que $\sigma_{-1}(\lambda) = \lambda\theta$, où θ est une racine d'ordre l — 1 de 1.

D'après l'exercice 4 du chapitre premier, § 3, la racine θ appartient à $\mathbf{Q}_l$, d'où

$$\sigma_{-1}^2(\lambda) = \sigma_{-1}(\sigma_{-1}(\lambda)) = \sigma_{-1}(\theta\lambda) = \theta\sigma_{-1}(\lambda) = \theta^2\lambda,$$

et puisque, par ailleurs $\sigma_{-1}^2(\lambda) = \lambda$, alors $\theta = \pm 1$. Si $\theta = 1$, tout nombre $\mathfrak{L}$-adique qui se représente sous la forme (2) par des coefficients a_i l-adiques serait invariant par l'automorphisme σ_{-1}, ce qui n'est pas. Ainsi $\theta = -1$ et $\sigma_{-1}(\lambda) = -\lambda$ et par suite les seuls éléments du corps $\mathbf{K}_\mathfrak{L}$ invariants par σ_{-1} sont les nombres $\mathfrak{L}$-adiques de la forme

$$\sum_{i=0}^{m-1} b_i\lambda^{2i} \qquad \left(b_i \in \mathbf{Q}_l, \quad m = \frac{l-1}{2}\right). \tag{3}$$

Tous ces nombres forment un sous-corps du corps $\mathbf{K}_\mathfrak{L}$, de degré $m = \dfrac{l-1}{2}$ sur $\mathbf{Q}_l$. Il sera commode d'appeler ces nombres $\mathfrak{L}$-adiques « réels ».

Calculons la trace du nombre $\mathfrak{L}$-adique (2) (pour l'extension $\mathbf{K}_\mathfrak{L}/\mathbf{Q}_l$). Pour tout $i = 1, \ldots, l-2$, la matrice de la transformation linéaire $\xi \to \lambda^i\xi$ ($\xi \in \mathbf{K}_\mathfrak{L}$) dans la base $1, \lambda, \ldots, \lambda^{l-2}$ a des éléments diagonaux nuls (puisque $\lambda^{l-1} = -l$), d'où $\mathrm{Tr}_{\mathbf{K}_\mathfrak{L}/\mathbf{Q}_l}(\lambda^i) = 0$ (pour $i = 1, \ldots, l-2$). Il en résulte que la trace du nombre (2) est égale à $a_0(l-1)$. Ainsi, les nombres $\mathfrak{L}$-adiques de trace nulle sont caractérisés par le fait que le coefficient a_0 dans la décomposition a, correspondante est nul.

Dans la suite, nous nous intéresserons à l'ensemble $\mathfrak{M}$ de tous les nombres entiers $\mathfrak{L}$-adiques « réels » de trace nulle. D'après ce qui précède, $\mathfrak{M}$ est l'ensemble de toutes les combinaisons linéaires

$$\sum_{i=1}^{m} b_i\lambda^{2i} \tag{4}$$

avec des coefficients b_i entiers 1-adiques.

Nous pouvons considérer sur le corps $\mathbf{K}_\mathfrak{L}$ les fonctions Log ε et exp α définies par des séries entières (cf. chap. IV, § 5-2)). Puisque l'indice de ramification e de l'extension $\mathbf{K}_\mathfrak{L}$ sur $\mathbf{Q}_l$ est égal à $l-1$, alors, pour cette extension, le nombre $\left[\dfrac{e}{l-1}\right] + 1$ est égal à 2 et par suite la série exp a est convergente pour tous les entiers $a \in \mathbf{K}_\mathfrak{L}$ divisibles par λ^2. La fonction Log ε est définie, elle, comme nous le savons, pour toutes les unités principales du corps $\mathbf{K}_\mathfrak{L}$.

Si ε est une unité principale du corps $\mathbf{K}_\mathfrak{L}$, i. e. $\varepsilon \equiv 1 \pmod{A}$, alors pour chacun des automorphismes σ_k nous aurons encore $\sigma_k(\varepsilon) \equiv 1 \pmod{\lambda}$ et

par suite Log $\sigma_k(\varepsilon)$ a un sens. Mais alors (corollaire 1 du théorème 11, § 2 de l'appendice)

$$\mathrm{Tr}_{K_\lambda/Q_l} \mathrm{Log}\ \varepsilon = \sum_{k=1}^{l-1} \sigma_k\ (\mathrm{Log}\ \varepsilon) = \sum_k \mathrm{Log}\ (\sigma_k(\varepsilon))$$
$$= \mathrm{Log}\left(\prod_k \sigma_k(\varepsilon)\right) = \mathrm{Log}\ (N_{K_\lambda/Q_l}\varepsilon),$$

Supposons maintenant que ε est une unité du corps K. Il est clair que ε est encore une unité du corps K_λ cependant Log ε peut ne pas avoir de sens puisque ε n'est pas, en général, une unité principale de K_λ. Pourtant nous aurons une congruence $\varepsilon \equiv a \pmod{A}$ pour un certain nombre entier rationnel a non divisible par 1. Mais $a^{l-1} \equiv 1 \pmod{l}$, d'où $\varepsilon^{l-1} \equiv 1 \pmod{A}$, i. e. ε^{l-1} est une unité principale dans K_λ. Le logarithme Log ε^{l-1} a donc un sens et, d'après la formule (1),

$$\mathrm{Tr}_{K_\lambda/Q_l}(\mathrm{Log}\,\varepsilon^{l-1}) = \mathrm{Log}\,(N_{K_\lambda/Q_l}\varepsilon^{l-1}) = \mathrm{Log}\ (N_{K/Q}\varepsilon^{l-1}) = 0,$$

i. e. la trace du nombre entier f-adique Log ε^{l-1} est nulle. D'autre part, si ε est une unité réelle du corps K, alors Log ε^{l-1} est, bien entendu, « réel ».

Ainsi, pour toute unité réelle ε du corps K, le nombre λ-adique Log ε^{l-1} appartient à l'ensemble $\mathfrak{M}$, i. e. se représente sous la forme (4). En particulier, ce résultat est valable pour les unités θ_k $k = 2, 3, \ldots, m = \frac{l-1}{2}$), définie par les formules (10) du § 5. Nous avons donc

$$\mathrm{Log}\ \theta_k^{l-1} = \sum_{i=1}^{m-1} b_{ki}\lambda^{2i} \qquad (2 \leqslant k \leqslant m) \tag{5}$$

pour des coefficients b_{ki} entiers I-adiques.

Rappelons que nous voulons démontrer que si le facteur h^* du nombre de classes de diviseurs du corps K n'est pas divisible par l, alors les nombres λ-adiques Log θ_k^{l-1} forment une base de $\mathfrak{M}$ sur l'anneau des nombres entiers l-adiques au sens suivant : tout $\xi \in \mathfrak{M}$ s'écrit de manière unique comme combinaison linéaire à coefficients entiers I-adiques de ces éléments. Pour cela, il est clair qu'il suffit de montrer que det (b_{ki}) est une unité l-adique, i. e. que det $(b_{ki}) \not\equiv 0 \pmod{l}$.

2) Quelques congruences auxiliaires

Dans le corps K_λ, la série exp x ne converge que pour les entiers x divisibles par λ^2. En liaison avec ce fait, considérons le polynôme

$$E(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^{l-1}}{(l-1)!},$$

obtenu en ne conservant que les 1 premiers termes de la série exp x. Puisque les coefficients $\frac{1}{k!}$ pour $k \leqslant l-1$ sont des entiers I-adiques, alors E(x) est une unité principale du corps K pour tout entier $x \equiv 0 \pmod{\lambda}$.

Nous savons que le produit formel des séries exp x et exp y est égal à la série exp (x + y), Il en résulte facilement que

$$E(x)\,E(y) = E(x+y) + F(x, Y), \tag{6}$$

où $F(x, y)$ est un polynôme à coefficients entiers *l*-adiques dont tous les termes sont de degré $\geqslant l$.

LEMME 2. — *Dans l'anneau des nombres entiers S-adiques on a la congruence*

$$E(\lambda)^l \equiv 1 \pmod{\lambda^{2l-1}}.$$

Posons

$$E(x) = 1 + xg(x),$$

où

$$g(x) = 1 + \frac{x}{2!} + \ldots + \frac{x^{l-2}}{(l-1)!}$$

est un polynôme à coefficients entiers *l*-adiques. Alors

$$E(x)^l = 1 + C_l^1 xg(x) + \ldots + C_l^{l-1}(xg(x))^{l-1} + x\$(x)' = 1 + lh(x) + x^l g(x)^l$$

où h(x) est encore un polynôme à coefficients entiers *l*-adiques. D'autre part, d'après (6), nous avons

$$E(x)' = E(lx) + x^l M(x),$$

d'où

$$lh(x) = \frac{lx}{1!} + \frac{(lx)^2}{2!} + \ldots + \frac{(lx)^{l-1}}{(l-1)!} + x^l H(x), \tag{7}$$

avec $H(x) = M(x) - g(x)'$. Comparant dans cette égalité les coefficients des puissances correspondantes de x nous voyons que tous les coefficients de H(x) sont des nombres entiers *l*-adiques divisibles par *1*. Simplifiant l'égalité (7) par *l*, nous obtenons

$$h(x) = x + \frac{lx^2}{2!} + \ldots + \frac{l^{l-2}x^{l-1}}{(l-1)!} + x^l G(x),$$

où G(x) a des coefficients entiers *l*-adiques. Posant x = A, nous obtenons la congruence

$$h(A) \equiv \lambda \pmod{\lambda},$$

d'où

$$lh(\lambda) \equiv l\lambda \pmod{\lambda^{2l-1}}. \tag{8}$$

De plus, puisque $g(A) \equiv 1 \pmod{A}$, alors $g(h) \equiv 1 \pmod{\lambda^l}$, d'où

$$\lambda^l g(\lambda)^l \equiv \lambda^l \pmod{\lambda^{2l}}. \tag{9}$$

D'après (8) et (9) nous avons maintenant

$$E(\lambda)^l = 1 + lh(\lambda) + \lambda^l g(\lambda)^l \equiv 1 + l\lambda + \lambda^l = 1 \pmod{\lambda^{2l-1}}$$

(puisque $l\lambda + \lambda^l = 0$), ce qu'il fallait démontrer.

LEMME 3. — ***Pour tout entier naturel k, on a la congruence***

$$E(k\lambda) \equiv \zeta^k \pmod{\lambda^l}.$$

D'après la formule (6),

$$E(k\lambda) \equiv (E(\lambda))^k \pmod{\lambda^l},$$

et il suffit donc de démontrer le lemme pour $k = 1$.

D'après la définition de l'élément premier A, nous avons $\zeta \equiv 1 + A \pmod{\lambda^2}$. D'autre part, $E(A) = 1 + A \pmod{\lambda^2}$, d'où

$$\zeta^{-1}E(\lambda) \equiv 1 \pmod{\lambda^2}.$$

Posons

$$\zeta^{-1}E(\lambda) = 1 + \lambda^2\gamma,$$

où γ est un entier !Sadique. Élevant cette égalité à la puissance $l^{\text{ième}}$ et utilisant le lemme 2, nous obtenons la congruence

$$\gamma\left(l\lambda^2 + \frac{l(l-1)}{2}\gamma l^4 + \ldots + \gamma^{l-1}\lambda^{2l}\right) \equiv 0 \pmod{\lambda^{2l-1}}.$$

L'expression entre parenthèses est divisible exactement par λ^{l+1}, d'où $\gamma \equiv 0 \pmod{\lambda^{l-2}}$; il en résulte que

$$\zeta^{-1}E(\lambda) \equiv 1 \pmod{\lambda^l},$$

ce qui démontre le lemme.

Considérons également le polynôme

$$L(1 + x) = x - \frac{x^2}{2} + \ldots + (-1)^{l-2}\frac{x^{l-1}}{l-1}, \tag{9*}$$

obtenu en ne conservant que les l premiers termes de la série $\text{Log}(1 + x)$.

LEMME 4. — ***Si le nombre entier $\mathfrak{L}$-adique a est divisible par λ^2, alors***

$$L(1 + a) = \text{Log}(1 + a) \pmod{\lambda^l}.$$

En effet, pour $n \geqslant l$, nous avons

$$v_{\mathfrak{L}}\left(\frac{\alpha^n}{n}\right) \geqslant 2n - v_{\mathfrak{L}}(n) \geqslant 2n - (l-1)\frac{\text{Log } n}{\text{Log } l}$$
$$\geqslant l + (n-l) + \frac{(l-1)n}{\text{Log } l}\left(\frac{\text{Log } l}{l-1} - \frac{\text{Log } n}{n-1}\right) \geqslant l$$

(cf. chap. IV § 5-2)).

LEMME *5.* — *Si ε_1 et ε_2 sont des unités Sadiques principales, alors*

$$L(\varepsilon_1, \varepsilon_2) \equiv L(\varepsilon_1) + L(\varepsilon_2) \pmod{\lambda^l}.$$

Puisque la série Log $(1 + x + y + xy)$ est égale à la somme des séries Log $(1 + x)$ et Log $(1 + y)$, alors

$$L(1 + x + y + xy) = L(1 + x) + L(1 + y) + G(x, y),$$

où le polynôme $G(x, y)$, à coefficients entiers l-adiques, ne contient que des termes de degré $\geqslant 1$. Le lemme 5 résulte maintenant du fait que si x et y sont divisibles par λ, alors $G(x, y) \equiv 0 \pmod{\lambda^l}$.

LEMME *6.* — *Dans l'anneau des nombres entiers $\mathfrak{L}$-adiques, on a la congruence*

$$L(\zeta) \equiv \lambda \pmod{\lambda^l}.$$

Nous utiliserons, pour la démonstration, l'égalité formelle Log exp x = x. De cette égalité résulte facilement que

$$L(E(x)) = x + H(x),$$

où $H(x)$ est un polynôme à coefficients entiers l-adiques ne contenant que des termes de degré $\geqslant l$. Faisant x = A et utilisant le lemme 3 pour $k = 1$, nous obtenons la congruence demandée.

Remarque. — Soient $\mathfrak{U}$ le groupe multiplicatif des classes résiduelles du groupe des unités $\mathfrak{L}$-adiques modulo A et $\mathfrak{X}$ le groupe additif des classes résiduelles de nombres entiers $\mathfrak{L}$-adiques divisibles par A modulo A. Il est facile de montrer que l'application $\varepsilon \to L(\varepsilon)$ (pour les unités principales $\mathfrak{L}$-adiques ε) induit un isomorphisme du groupe $\mathfrak{U}$ sur le groupe $\mathfrak{X}$. L'isomorphisme inverse $\mathfrak{X} \to \mathfrak{U}$ est induit par l'application $a \to E(a)$ $(a \equiv 0 \pmod{A})$.

3) Base des entiers Sadiques réels dans le cas $(h^*, l) = 1$

Revenons à la question posée à la fin du point 1). Pour déterminer si $\det(b_{ki})$ est divisible par 1 ou non, il suffit de considérer les coefficients b_{ki} modulo 1. Il est clair que deux nombres entiers $\mathfrak{L}$-adiques du type (2) sont

congrus modulo l si et seulement si les coefficients des puissances correspondantes de A sont congrus modulo l (dans l'anneau des nombres entiers l-adiques). Il en résulte que pour calculer les coefficients b_{ki} modulo l on peut remplacer chacun des nombres Log θ_k^{l-1} par un nombre entier Sadique qui lui soit congru modulo 1 (i. e. modulo λ^{l-1}).

Conservons ici toutes les notations du § 5-2). L'unité principale θ_k^{l-1} est réelle et par suite elle est congrue à 1 modulo λ^2, d'où, d'après le lemme 4,

$$\operatorname{Log} \theta_k^{l-1} \equiv \mathrm{L}(\theta_k^{l-1}) \pmod{k}. \tag{10}$$

Calculons $\mathrm{L}(\theta_k^{l-1})$. Puisque

$$\theta_k = \frac{\zeta^k - 1}{\zeta - 1}\eta^{\cdot\, k},$$

alors

$$\theta_k^l = (1 + \zeta + \ldots + \zeta^{k-1})^l (-1)^{1-k}.$$

Mais $\zeta \equiv 1 \pmod{\mathrm{A}}$, c'est pourquoi

$$1 + \zeta + \ldots + \zeta^{k-1} \equiv k \pmod{\lambda},$$

d'ou

$$(1 + \zeta + \ldots + \zeta^{k-1})^l \equiv k^l \pmod{\lambda^l},$$

et, puisque $k^l \equiv k \pmod{\lambda^{k-1}}$, alors

$$(1 + \zeta + \ldots + \zeta^{k-1})^l \equiv k \pmod{\lambda^{l-1}}.$$

Ainsi,

$$\theta_k^{l-1} 3\, \theta_k^{-1} k(-1)^{1-k} \equiv k \frac{\zeta - 1}{\zeta^k - 1}(-\eta)^{k-1} \pmod{\lambda^{l-1}},$$

ou encore

$$\theta_k^{l-1} = \frac{\zeta - 1}{\mathrm{A}} \cdot \left(\frac{\zeta^k - 1}{k\lambda}\right)^{-1} \zeta^{(k-1)\frac{l+1}{2}} \pmod{\lambda^{l-1}}.$$

D'après le lemme 5, nous avons

$$\mathrm{L}(\theta_k^{l-1}) \equiv \mathrm{L}\left(\frac{\zeta - 1}{\lambda}\right) - \mathrm{L}\left(\frac{\zeta^k - 1}{k\lambda}\right) + (k-1)\frac{l+1}{2}\mathrm{L}(\zeta) \pmod{\lambda^{l-1}}.$$

Mais, d'après le lemme 3,

$$\frac{\zeta^k - 1}{kl} \equiv \frac{\mathrm{E}(k\lambda) - 1}{k\lambda} \pmod{\lambda^{l-1}};$$

nous obtenons donc, en utilisant le lemme 6,

$$\mathrm{L}(\theta_k^{l-1}) \equiv \mathrm{L}\left(\frac{\mathrm{E}(\lambda) - 1}{\lambda}\right) - \frac{\lambda}{2} - \mathrm{L}\left(\frac{\mathrm{E}(k\lambda) - 1}{k\lambda}\right) + \frac{k\lambda}{2} \pmod{\lambda^{l-1}}.$$

Démontrons maintenant que

$$L\left(\frac{E(x)-1}{x}\right)-\frac{x}{2}=\sum_{k=1}^{m-1}\frac{B_{2k}x^{2k}}{(2k)!\,2k}+x^{l-1}R(x), \tag{11}$$

où R(x) est un polynôme à coefficients entiers *l*-adiques et où les B_{2k} sont les nombres de Bernoulli (cf. § 8 de ce chapitre). Utilisons l'identité

$$\frac{x}{e^x-1}=\sum_{n=0}^{\infty}\frac{B_n}{n!}x^n.$$

Puisque $B_1 = -\frac{1}{2}$ et puisque tous les autres nombres de Bernoulli d'indices impairs sont nuls, cette identité peut aussi s'écrire sous la forme :

$$\frac{e^x}{e_x-1}-\frac{1}{2}-\frac{1}{x}=\sum_{k=1}^{\infty}\frac{B_{2k}}{(2k)!}x^{2k-1}.$$

Par intégration, nous obtenons

$$\mathrm{Log}\frac{e^x-1}{x}-\frac{x}{2}=\sum_{k=1}^{\infty}\frac{B_{2k}}{(2k)!\,2k}x^{2k} \tag{12}$$

(le terme constant de la série est nul puisque la fonction de gauche s'annule pour $x = 0$). L'égalité (11) résulte maintenant facilement de la formule (12). Substituant la valeur $k\lambda$ à l'inconnue x dans la formule (1 1), nous obtenons

$$L\left(\frac{E(k\lambda)-1}{k\lambda}\right)-\frac{k\lambda}{2}\equiv\sum_{i=1}^{m-1}\frac{B_{2i}k^{2i}\lambda^{2i}}{(2i)!\,2i}\pmod{\lambda^{l-1}}$$

d'où

$$L\left(\theta_k^{l-1}\right)\equiv\sum_{i=1}^{m-1}\frac{B_{2i}(1-k^{2i})\lambda^{2i}}{(2i)!\,2i}\pmod{\lambda^{l-1}}. \tag{12*}$$

Ceci démontre que les coefficients b_{ki} des égalités (5) satisfont aux congruences

$$b_{ki}\equiv\frac{B_{2i}(1-k^{2i})}{(2i)!\,2i}\pmod{l}\qquad\left(2\leqslant k\leqslant m=\frac{l-1}{2},\ 1\leqslant i\leqslant m-1\right).$$

Mais alors det (b_{ki}) est congru modulo l au déterminant

$$\prod_{i=1}^{m-1}\frac{(-1)^{m-1}B_{2i}}{(2i)!\,2i}\begin{vmatrix} 2^2-1 & 2^4-1 & \cdots & 2^{l-3}-1\\ 3^2-1 & 3^4-1 & \cdots & 3^{l-3}-1\\ \cdots & \cdots & \cdots & \cdots\\ m^2-1 & m^4-1 & \cdots & m^{l-3}-1\end{vmatrix}$$

Il est facile de ramener ce dernier déterminant à un déterminant de Vandermonde. Il est égal au produit

$$\prod_{1 \leqslant s < r \leqslant m} (r^2 - s^2) = \prod_{S<1} (r + s)(r - s),$$

dont aucun des facteurs n'est divisible par 1. Si maintenant $h^* \not\equiv 0 \pmod{l}$, alors les nombres de Bernoulli $B_2, \ldots, B_{l-3}$ ne sont pas divisibles par l et nous obtenons

$$\det b_{ki} \not\equiv 0 \pmod{l}.$$

Nous avons ainsi démontré le théorème suivant :

THÉORÈME 1. — ***Si*** $h^* \not\equiv 0 \pmod{l}$ ***tout nombre entier*** $\mathfrak{L}$***-adique « réel » de trace nulle s'écrit de manière unique comme une combinaison linéaire***

$$\sum_{k=2}^{m} a_k \operatorname{Log} \theta_k^{l-1} \tag{13}$$

à coefficients entiers l-adiques a_k.

4) Critère de régularité et lemme de Kummer

Le théorème 1 obtenu ci-dessus permet de démontrer facilement le théorème suivant.

THÉORÈME. — ***Si pour le*** $l^{\text{ième}}$ ***corps cyclotomique*** $\mathbf{Q}(\zeta)$ ***le facteur*** h^* ***du nombre de classes de diviseurs n'est pas divisible par*** l, ***alors le facteur*** h_0 ***n'est pas non plus divisible par 1.***

DÉMONSTRATION. — Supposant que $h_0 = (E : E_0)$ est divisible par l (cf. notations du théorème 2 du § 5), on peut trouver une unité réelle positive $\varepsilon \in E$ qui n'appartient pas à E_0 mais telle que $\varepsilon^l \in E_0$, i. e.

$$\varepsilon^l = \prod_{k=2}^{m} \theta_k^{c_k} \tag{14}$$

pour des entiers rationnels c_k non tous divisibles par l (car sinon l'unité c appartiendrait à E_0). Élevant l'égalité (14) à la puissance $l - 1$ et prenant les logarithmes (dans le corps $K_{\mathfrak{L}}$), nous obtenons

$$l \operatorname{Log} \varepsilon^{l-1} = \sum_{k=2}^{m} c_k \operatorname{Log} \theta_k^{l-1}. \tag{15}$$

D'autre part, puisque la valeur Log ε^{l-1} appartient à $\mathfrak{M}$, ce nombre admet une représentation de la forme (13) ; égalant à (15), nous obtenons que tous les quotients $\frac{c_k}{l}$ sont des entiers l-adiques, ce qui contredit le fait que tous les c_k ne sont pas divisibles par *1.* La contradiction obtenue démontre le théorème 2.

COROLLAIRE. — *Un nombre premier $1 \geqslant 3$ est régulier si et seulement si aucun des nombres de Bernoulli* B_2, $B_4, \ldots, B_{l-3}$ *n'est divisible par 1.*

THÉORÈME 3 (lemme de Kummer). — ***Soit 1 un nombre premier rationnel régulier. Si une unité du*** $l^{\text{ième}}$ ***corps cyclotomique Q(C) est congrue modulo*** l ***à un nombre rationnel, cette unité est la puissance*** $l^{\text{ième}}$ ***d'une autre unité.***

DÉMONSTRATION. — Supposons $\varepsilon \equiv a \pmod{l}$. Montrons tout d'abord que ε est une unité réelle. Si $\varepsilon = \zeta^k \varepsilon_1$, pour une unité réelle ε_1, alors $\varepsilon_1 \equiv b \pmod{\lambda^2}$ pour un entier rationnel b et $\zeta \equiv 1 + k\lambda \pmod{\lambda^2}$. De la congruence $a \equiv b\,(1 + k\lambda) \pmod{\lambda^2}$ résulte maintenant que $k \equiv 0 \pmod{A}$. Ceci démontre notre argument. Puisque $-1 = (-1)^l$, on peut supposer $\varepsilon > 0$, i. e. $\varepsilon \in E$. De la congruence $\varepsilon^{l-1} \equiv a^{l-1} \equiv 1 \pmod{l}$ résulte que Log $\varepsilon^{l-1} \equiv 0 \pmod{l}$, puisque, d'après le théorème 1,

$$\text{Log } \varepsilon^{l-1} = \sum_{k=2}^{m} l c_k \text{ Log } \theta_k^{l-1} \tag{16}$$

avec des entiers l-adiques c_k. D'autre part, puisque le sous-groupe E_0 est d'indice fini dans E, alors $\varepsilon^a \in E_0$ pour un certain entier naturel a; par suite,

$$\varepsilon^a = \prod_{k=2}^{m} \theta_k^{d_k} \tag{17}$$

pour des entiers rationnels d_k. Il est clair que nous pouvons supposer que les exposants $a, d_2, \ldots, d_m$ sont premiers dans leur ensemble (puisque le groupe E ne contient pas d'élément d'ordre fini, on peut simplifier dans (17) par tout diviseur commun). Élevant l'égalité (17) à la puissance $l - 1$ et prenant les logarithmes (dans le corps K_∞), nous obtenons

$$a \text{ Log } \varepsilon^{l-1} = \sum_{k=2}^{m} d_k \text{ Log } \theta_k^{l-1}.$$

Comparant ce résultat à l'égalité (16), nous obtenons

$$d_k = l a c_k \qquad (k = 2, \ldots m).$$

Puisque les nombres ac_k sont des entiers I-adiques, il en résulte que tous les d_k sont divisibles par l; ainsi ε^a est une puissance $l^{\text{ième}}$: $\varepsilon^a = \varepsilon_1^l$, avec $\varepsilon_1 \in E_0$. Mais, d'après la condition $(a, d_2, \ldots, d_m) = 1$, a est premier avec l, d'où $1 = au + lv$ pour certains entiers rationnels u et v; on a alors

$$\varepsilon = (\varepsilon^a)^u(\varepsilon^v)^l = (\varepsilon_1^u\varepsilon^v)^l,$$

ce qui démontre le théorème.

EXERCICES

1. Soient p un nombre premier de la forme $4n + 1$, $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$, $\lambda = \zeta - 1$, $m = \frac{p-1}{2}$. Posons

$$\xi = \prod_{k=1}^{p-1}\theta_k^{-\left(\frac{k}{p}\right)}$$

avec $\theta_k = \sin\frac{k\pi}{p}\left(\sin\frac{\pi}{p}\right)^{-1}$, $1 \leqslant k \leqslant p - 1$. Montrer que dans le $p^{\text{ième}}$ corps cyclotomique on a la congruence

$$L(\xi^{p-1}) \equiv \frac{2B_m}{m!}\lambda^m \equiv -2B_m\sqrt{p} \pmod{\lambda^{m+1}}.$$

Ici L désigne la fonction définie par l'égalité (9*) et B_m le $m^{\text{ième}}$ nombre de Bernoulli (Utiliser la congruence (12*) et la congruence de l'exercice 14 du § 4).

2. Soit $\varepsilon = T + U\sqrt{p} > 1$ une unité fondamentale et h le nombre de classes de diviseurs du corps quadratique $Q(\sqrt{p})$, où $p \equiv 1 \pmod 4$ est premier. En s'appuyant sur l'exercice précédent et sur le théorème 2 du § 4, démontrer la congruence

$$hU \equiv TB_m \pmod p, \qquad m = \frac{p-1}{2}$$

(dans l'anneau des nombres rationnels p-entiers).

§ 7. — DEUXIÈME CAS DU THÉORÈME DE FERMAT POUR DES EXPOSANTS RÉGULIERS

1) Théorème de Fermat

THÉORÈME 1. — *Soit $l \geqslant 3$ un nombre premier régulier. L'équation*

$$x^l + y^l = z^l \tag{1}$$

n'a pas de solution en nombres entiers rationnels x, y, z non nuls.

DÉMONSTRATION. — Supposons que les nombres entiers x, y et z (non nuls) premiers entre eux vérifient l'équation (1). Puisque le premier cas du théorème de Fermat a déjà été étudié dans le chapitre III, § 7-3), nous supposerons qu'un (et un seul) de ces nombres est divisible par l, soit z (si par exemple y est divisible par l, nous écrirons l'égalité (1) sous la forme $x^l + (-z)^l = (-y)^l$). Soit $z = l^k z_0$, avec $(z_0, l) = 1$, $k \geqslant 1$. Puisque dans le $l^{\text{ième}}$ corps cyclotomique $\mathbf{Q}(\zeta)$ le nombre l admet la décomposition $l = (1 - \zeta)^l \varepsilon$, où une unité du corps $\mathbf{Q}(\zeta)$ (lemme 1 du chapitre III, § 1), alors l'égalité (1) peut s'écrire, dans le corps $\mathbf{Q}(\zeta)$, sous la forme

$$x^l + y^l = \varepsilon(1 - \zeta)^{lm} z_0^l, \tag{2}$$

avec $m = k(l - 1) > 0$. Pour démontrer le théorème, il suffit de montrer que toute égalité du type (2) est impossible. Nous démontrerons un peu plus. En fait, on montrera que l'égalité (2) est impossible non seulement pour des entiers rationnels x, y, z_0 premiers avec l mais aussi pour des entiers x, y, z_0 du corps $\mathbf{Q}(\zeta)$ premiers avec $1 - \zeta$. Raisonnons par l'absurde, i. e. supposons qu'il existe des égalités du type (2) ; choisissons-en une pour laquelle le nombre $m \geqslant 1$ est le plus petit possible. Pour ne pas introduire de notations nouvelles, nous écrirons cette égalité sous la forme (2). Les nombres x, y et z_0 désignent donc maintenant certains nombres entiers du corps $\mathbf{Q}(\zeta)$ premiers avec $1 - \zeta$ et ε une unité du corps $\mathbf{Q}(\zeta)$.

Comme au § 6, nous désignerons par $\mathfrak{L}$ le diviseur premier $(1 - \zeta)$ du corps $\mathbf{Q}(\zeta)$. Décomposons la partie gauche de l'égalité (2) en facteurs linéaires et passons aux diviseurs. Nous obtenons

$$\prod_{k=0}^{l-1} (x + \zeta^k y) = \mathfrak{L}^{lm} \mathfrak{a}^l, \tag{3}$$

où le diviseur $\mathfrak{a} = (z_0)$ est premier avec $\mathfrak{L}$. Puisque $lm \geqslant l > 0$, il résulte de (3) que l'un au moins des facteurs de gauche est divisible par $\mathfrak{L}$. Mais

$$x + \xi^i y = x + \xi^k y - \xi^k (1 - \xi^{i-k}) y,$$

et par suite tous les nombres

$$x + \zeta^k y \quad (0 \leqslant k \leqslant l - 1) \tag{4}$$

sont divisibles par $\mathfrak{L}$. Si pour $0 \leqslant k < i \leqslant l - 1$ nous avions la congruence

$$x + \zeta^k y \equiv x + \zeta^i y \pmod{\mathfrak{L}^2},$$

alors nous aurions aussi $\zeta^k y(1-\zeta^{i-k}) \equiv 0 \pmod{\mathfrak{L}^2}$ et c'est impossible puisque $\zeta^k y$ est premier avec $\mathfrak{L}$ et $1-\zeta^{i-k}$ associé avec $1-\zeta$. Ainsi, les nombres (4) sont deux à deux non congrus modulo $\mathfrak{L}^2$; par suite, les rapports

$$\frac{x+\zeta^k y}{1-\zeta} \qquad (k = 0, 1, \ldots, l-1)$$

sont deux à deux non congrus modulo $\mathfrak{L}$. Mais N(2) = *1* et ces nombres forment donc un système complet de résidus modulo $\mathfrak{L}$ et l'un d'eux est divisible par $\mathfrak{L}$. Il en résulte que, parmi les nombres (4), un (et un seul) est divisible par $\mathfrak{L}^2$. Puisque nous pouvons remplacer y dans l'égalité (2) par l'un des nombres $\zeta^k y$, on peut considérer que x + y est divisible par $\mathfrak{L}^2$, ce qui signifie que tous les autres nombres $x + \zeta^k y$, divisibles par $\mathfrak{L}$, ne sont pas divisibles par $\mathfrak{L}^2$. Du fait que la partie gauche de l'égalité (3) est divisible exactement par $\mathfrak{L}^{l-1}\mathfrak{L}^2 = \mathfrak{L}^{l+1}$, il en résulte maintenant que $m > 1$.

Désignons par $\mathfrak{m}$ le plus grand commun diviseur des diviseurs (x) et (y) Puisque x et y ne sont pas divisibles par $\mathfrak{L}$, alors $\mathfrak{m}$ n'est pas non plus divisible par $\mathfrak{L}$. Il est clair par ailleurs que $(x + \zeta^k y)$ est divisible par $\mathfrak{L}\mathfrak{m}$ et x + y divisible par $\mathfrak{L}^{l(m+1)+1}$ m. Posons

$$(x + y) = \mathfrak{L}^{l(m-1)+1}\,\mathrm{mc},,$$
$$(x + \zeta^k y) = \mathfrak{L}\mathfrak{m}\mathfrak{c}_k \qquad (k = 1, \ldots \text{..r-1})$$

et démontrons que les diviseurs $\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{l-1}$ sont deux à deux premiers entre eux. En effet, si $\mathfrak{c}_i$ et $\mathfrak{c}_k$ $(0 \leqslant i < k \leqslant l-1)$ avaient un diviseur commun $\mathfrak{p}$, alors, de la divisibilité de $x + \zeta^i y$ et $x + \zeta^k y$ par $\mathfrak{L}\mathfrak{m}\mathfrak{p}$ résulterait que $\zeta^i y(1-\zeta^{k-i})$ et $x(1-\zeta^{k-i})$ sont aussi divisibles par $\mathfrak{L}\mathfrak{m}\mathfrak{p}$; cela entraînerait à son tour que x et y sont divisibles par $\mathfrak{m}\mathfrak{p}$, ce qui contredit la définition de m.

Écrivant (3) sous la forme

$$m^l \mathfrak{L}^{lm}\mathfrak{c}_0\mathfrak{c}_1 \ldots \mathfrak{c}_{l-1} = \mathfrak{L}^{lm}\mathfrak{a}^l,$$

nous en déduisons (puisque les $\mathfrak{c}_k$ sont premiers deux à deux) que

$$\mathfrak{c}_k = \mathfrak{a}_k^l \qquad (0 \leqslant k \leqslant l-1),$$

i. e.

$$(x + y) = \mathfrak{L}^{l(m-1)+1}\mathfrak{m}\mathfrak{a}_0^l, \tag{5}$$

$$(x + \zeta^k y) = \mathfrak{L}\mathfrak{m}\mathfrak{a}_k^l \qquad (1 \leqslant k \leqslant l-1). \tag{6}$$

Tirant m de (5) et portant dans (6), nous obtenons

$$(x + \zeta^k y)\mathfrak{L}^{l(m-1)} = (x + y)(\mathfrak{a}_k\mathfrak{a}_0^{-1})^l, \tag{7}$$

d'où il résulte que le diviseur $(\mathfrak{a}_k\mathfrak{a}_0^{-1})^l$ est principal (puisque $\mathfrak{L} = (1-\zeta)$). Utilisons maintenant la régularité du nombre *l*. Puisque le nombre de

classes de diviseurs du corps $\mathbf{Q}(\zeta)$ n'est pas divisible par l, alors, d'après le corollaire du théorème 3, chapitre III, § 7, le diviseur $\mathfrak{a}_k\mathfrak{a}_0^{-1}$ est aussi principal, i. e.

$$\mathfrak{a}_k\mathfrak{a}_0^{-1} = \left(\frac{\alpha_k}{\beta_k}\right) \qquad (1 \leqslant k \leqslant l-1), \tag{8}$$

où α_k et β_k sont des nombres *entiers* du corps $\mathbf{Q}(\zeta)$. Les diviseurs $\mathfrak{a}_k$ et a,, sont premiers avec $\mathfrak{L}$ et par suite on peut supposer que les nombres α^k et β_k ne sont pas divisibles par $\mathfrak{L}$. L'égalité des diviseurs principaux équivaut à l'égalité des nombres correspondants, à un facteur qui est une unité près. Ainsi, d'après (7) et (8), nous avons

$$(x + \zeta^k y)(1-\zeta)^{l(m-1)} = (x + y)\left(\frac{\alpha_k}{\beta_k}\right)^l \varepsilon_k \quad (1 \leqslant k \leqslant l-1), \tag{9}$$

où ε_k est une unité du corps Q(C).

Utilisons maintenant l'égalité évidente suivante

$$(x + \zeta y)(1 + \zeta) - (x + \zeta^2 y) = \zeta(x + y).$$

La multipliant par $(1-\zeta)^{l(m-1)}$ et tenant compte des égalités (9) pour $k = 1$ et $k = 2$, nous trouvons

$$(x + y)\left(\frac{\alpha_1}{\beta_1}\right)^l \varepsilon_1(1 + \zeta) - (x + y)\left(\frac{\alpha_2}{\beta_2}\right)^l \varepsilon_2 = (x + y)\zeta(1-\zeta)^{l(m-1)},$$

d'où

$$(\alpha_1\beta_2)^l - \frac{\varepsilon_2}{\varepsilon_1(1+\zeta)}(\alpha_2\beta_1)^l = \frac{\zeta}{\varepsilon_1(1+\zeta)}(1-\zeta)^{l(m-1)}(\beta_1\beta_2)^l.$$

Nous avons ainsi obtenu une égalité de la forme

$$\alpha^l + \varepsilon_0\beta^l = \varepsilon'(1-\zeta)^{l(m-1)}\gamma^l, \tag{10}$$

où α, β et y sont des nombres entiers de $\mathbf{Q}(\zeta)$ non divisibles par $\mathfrak{L}$ et ε_0 et ε' des unités du corps Q(C). Mettons-la sous la forme (2).

Nous avons vu ci-dessus que $m > 1$, d'où $m - 1 > 0$ et $l(m-1) \geqslant l$, d'où

$$\alpha^l + \varepsilon_0\beta^l \equiv 0 \pmod{\mathfrak{L}^l}.$$

Puisque β est premier avec $\mathfrak{L}$, il existe un entier β' tel que $\beta\beta' \equiv 1 \pmod{\mathfrak{L}^l}$. Multipliant la dernière congruence écrite par β'^l, nous obtenons

$$\varepsilon_0 \equiv \omega^l \pmod{\mathfrak{L}^l},$$

où $\omega = -\alpha\beta'$ est un nombre entier du corps $\mathbf{Q}(\zeta)$. Puisque $\mathbf{N}(\mathfrak{L}) = l$, tout nombre entier de $\mathbf{Q}(\zeta)$ est congru modulo $\mathfrak{L}$ à un entier rationnel.

Mais si $\omega \equiv a \pmod{\mathfrak{L}}$, alors $\omega^l \equiv a^l \pmod{l\mathfrak{L}}$, ce qui entraîne que l'unité ε_0 est congrue modulo $\mathfrak{L}^l$ à un nombre entier rationnel. D'après le lemme de Kummer (théorème 3 du § 6; nous utilisons à nouveau la régularité du nombre l), l'unité ε_0 est une puissance $l^{\text{ième}}$ dans $\mathbf{Q}(\zeta)$, i. e. $\varepsilon_0 = \eta_1^l$ où η_1 est aussi une unité du corps $\mathbf{Q}(\zeta)$. L'égalité (10) s'écrit alors

$$a' + (\eta_1\beta)^l = \varepsilon'(1-\zeta)^{l(m-1)}\gamma^l.$$

Nous avons obtenu une égalité du type (2), à cette différence près que l'exposant m est remplacé par $m-1$. Mais c'est impossible, puisque m a été choisi le plus petit possible. La contradiction obtenue montre que l'équation (1) n'a pas de solution en nombres entiers non nuls x, y et z dont l'un est divisible par l, i. e. le deuxième cas du théorème de Fermat est démontré pour an exposant l régulier.

2) Infinité de l'ensemble des nombres premiers irréguliers

Dans les limites des tables, la quantité des nombres premiers réguliers est supérieure à la quantité des nombres irréguliers. Pourtant, on ne sait pas si c'est toujours vrai pour l'intervalle (1, N). En fait, jusqu'à présent, on ignore même s'il existe une infinité de nombres réguliers. Le théorème suivant est lié à ces questions.

THÉORÈME 2. — *Il existe une infinité de nombres premiers irréguliers.*

La démonstration du théorème 2 s'appuie sur certaines propriétés des nombres de Bernoulli. Ces propriétés seront formulées et démontrées dans le paragraphe suivant.

Soit $p_1, \ldots, p_s$ un système fini quelconque de nombres premiers irréguliers. Le théorème 2 sera démontré si nous pouvons trouver un nombre premier irrégulier p différent de $p_1, \ldots, p_s$. Posons

$$n = r(p_1 - 1) \ldots (p_s - 1).$$

Puisque pour le nombre de Bernoulli B_{2k} on a

$$\left|\frac{\mathrm{B}_{2k}}{2k}\right| \to \infty \qquad \text{pour} \qquad k \to \infty,$$

(cf. fin du § 8), si l'entier rationnel r est assez grand, le nombre rationnel $\dfrac{\mathrm{B}_n}{n}$ sera supérieur à 1 en valeur absolue. Soit p un nombre premier figurant dans le numérateur (pour une écriture irréductible). Si $(p-1)|n$, alors, d'après le théorème 4 du § 8, le nombre p figure dans le dénominateur de B_n, ce qui n'est pas, d'après le choix de p. Ainsi $(p-1) \nmid n$ et p est donc diffé-

rent de $p_1, \ldots, p_s$ (et différent de 2). Désignons par m le reste de la division de n par $p-1$, i. e. $n = m + a(p-1)$. Il est clair que m est pair et

$$2 \leqslant m \leqslant p-3.$$

De plus, simultanément avec n, le nombre m n'est pas divisible par $p-1$. Utilisant maintenant la congruence dite de Kummer (théorème 5 du § 8), nous obtenons dans l'anneau des nombres rationnels p-entiers la congruence

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}.$$

Mais $\frac{B_n}{n} \equiv 0$ (modp), d'où $\frac{B_m}{m} \equiv 0$ (modp) et $B_m \equiv 0$ (modp). Puisque m est égal ici à l'un des nombres 2, 4, . . . , $p-3$, alors, d'après le corollaire du théorème 2 du § 6, le nombre p est irrégulier. Le théorème 2 est démontré.

EXERCICES

1. Démontrer que l'équation $x^3 + y^3 = 5z^3$ a pour unique solution $x=y=z=0$ dans les nombres entiers rationnels.

2. Démontrer qu'il existe une infinité de nombres premiers irréguliers de la forme $4n + 3$ (utiliser les exercices 9 et 10 du § 8).

§ 8. — LES NOMBRES DE BERNOULLI

Nous démontrerons ici les propriétés des nombres de Bernoulli qui ont été utilisées dans les paragraphes précédents.

Toutes les séries entières considérées ci-dessous convergent dans un certain voisinage de l'origine des coordonnées et il est facile de déterminer leur rayon de convergence. Nous ne nous intéresserons pourtant pas à ces questions de convergence puisqu'il suffit pour notre propos de considérer ces séries formellement (à l'exclusion de la démonstration du théorème 6).

DEFINITION. — ***Les nombres rationnels*** B_m $(m \geqslant 1)$ ***définis par le développement en série***

$$\frac{t}{e^t - 1} = 1 + \sum_{m=1}^{\infty} \frac{B_m}{m!} t_m, \tag{1}$$

sont appelés nombres de Bernoulli.

Nous utiliserons les notations abrégées suivantes. Si

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

est un polynôme, nous désignerons par f(B) le nombre

$$a_0 + a_1\mathrm{B}_1 + \ldots + a_n\mathrm{B}_n.$$

De manière analogue, si $f(x, t)$ est une série entière de la forme $\sum_{n=0}^{\infty} f_n(x)t^n$, où $f_n(x)$ est un polynôme, nous désignerons par $f(\mathrm{B}, t)$ la série

$$\sum_{n=0}^{\infty} f_n(\mathrm{B})t^n.$$

Ainsi par exemple, on peut écrire la série (1) définissant les nombres de Bernoulli sous la forme

$$\frac{t}{e^t - 1} = e^{\mathrm{B}t}.$$

Il est facile de voir que pour tout nombre a on a

$$e^{at}e^{\mathrm{B}t} = e^{(a+\mathrm{B})t}$$

(la démonstration s'effectue en multipliant terme à terme les séries de gauche).

THÉORÈME 1. — *Les nombres de Bernoulli vérifient la relation de récurrence*

$$(1 + \mathrm{B})^m - \mathrm{B}^m = 0 \qquad \text{pour} \qquad m \geqslant 2, \tag{2}$$

qui sous forme développée s'écrit

$$1 + \sum_{k=1}^{m-1} \mathrm{C}_m^k \mathrm{B}_k = 0 \qquad (m \geqslant 2).$$

Pour la démonstration, écrivons l'égalité (1) sous la forme

$$t = e^{(1+\mathrm{B})t} - e^{\mathrm{B}t}.$$

Égalant les coefficients des termes $\frac{t^m}{m!}$ $(m \geqslant 2)$, nous obtenons la relation (2). Pour $m = 2$, la formule (2) donne $1 + 2\mathrm{B}_1 = 0$, d'où

$$\mathrm{B}_1 = -\frac{1}{2}.$$

THÉORÈME 2. — *A l'exception de* B_1, *tous les nombres de Bernoulli d'indices impairs sont nuls* :

$$\mathrm{B}_{2m+1} = 0 \qquad \text{pour} \qquad m \geqslant 1. \tag{3}$$

Les égalités (3) équivalent au fait que la fonction

$$\frac{t}{e^t-1}+\frac{t}{2}=1+\sum_{m=2}^{\infty}\frac{B_m}{m!}t^m$$

est paire, ce qui est facile à vérifier.

Donnons les valeurs des douze premiers nombres de Bernoulli d'indices pairs :

$$B_2=\frac{1}{6},\quad B_4=-\frac{1}{30},\quad B_6=\frac{1}{42},\quad B_8=-\frac{1}{30},\quad B_{10}=\frac{5}{66},$$

$$B_{12}=-\frac{691}{2730},\quad B_{14}=\frac{7}{6},\quad B_{16}=-\frac{3\ 617}{510},\quad B_{18}=\frac{43\ 867}{798},$$

$$B_{20}=-\frac{174\ 611}{330},\quad B_{22}=\frac{854\ 513}{138},\quad B_{24}=-\frac{236\ 364\ 091}{2730}.$$

Les nombres de Bernoulli sont liés aux sommes des puissances des nombres entiers naturels. Posons

$$S_k(n)=1^k+2^k+\ldots+(n-1)^k.$$

THÉORÈME 3. — ***Les sommes*** $S_k(n)$ ***vérifient la formule***

$$(m+1)S_m(n)=(n+B)^{m+1}-B^{m+1},\qquad m\geqslant 1 \tag{4}$$

ou, sous forme développée,

$$(m+1)S_m(n)=\sum_{k=0}^{m}C_{m+1}^{k}B_k n^{m+1-k},\qquad m\geqslant 1\ (B_1=1). \tag{5}$$

En effet, l'expression de droite dans l'égalité (4) est égale au coefficient de $\frac{t^{m+1}}{(m+1)!}$ dans la série $e^{(n+B)t}-e^{Bt}$. Par ailleurs

$$e^{(n+B)t}-e^{Bt}=e^{Bt}(e^{nt}-1)=t\frac{e^{nt}-1}{e^t-1}=t\sum_{r=}^{n-1}e^{rt}$$

$$=nt+\sum_{m=1}^{\infty}\left(\sum_{r=1}^{n-1}r^m\right)\frac{t^{m+1}}{m!}=nt+\sum_{m=1}^{\infty}\frac{(m+1)S_m(n)t^{m+1}}{(m+1)!},$$

ce qui démontre la formule (4).

Remarquons que, pour $n=1$, la formule (4) coïncide avec (2).

THÉORÈME 4 (théorème de von Staudt). — *Soient p un nombre premier et m un nombre pair. Si* $(p-1)\nmid m$, *alors* B_m *est p-entier* (i. e. B_m *ne contient*

pas p en dénominateur). Si maintenant $(p-1) \mid m$, ***alors*** $p\mathrm{B}_m$ ***est un nombre p-entier et***

$$p\mathrm{B}_m \equiv -1 \pmod{p}.$$

Nous démontrerons le théorème **4** par récurrence sur m en utilisant la relation

$$(m+1)\mathrm{S}_m(p) = (m+1)\mathrm{B}_m p + \sum_{k=0}^{m-1} \mathrm{C}_{m+1}^{k} \mathrm{B}_k p^{m+1-k},$$

obtenue à partir de (5) en remplaçant n par p. Écrivons-la sous la forme

$$p\mathrm{B}_m = \mathrm{S}_{(p)} - \sum_{k=0}^{m-1} \frac{1}{m+1} \mathrm{C}_{m+1}^{k} p^{m-k} p\mathrm{B}_k \tag{6}$$

et démontrons que tous les nombres qui figurent dans la somme sont des nombres p-entiers et sont divisibles par p (dans l'anneau des nombres p-entiers).

Le facteur $p\mathrm{B}_k$ pour $k < m$ est p-entier par hypothèse de récurrence. Étudions le nombre

$$\frac{1}{m+1} \mathrm{C}_{m+1}^{k} p^{m-k}. \tag{7}$$

Si $p = 2$, alors, puisque $m+1$ est impair, ce nombre est l-entier et divisible par 2 (puisque $k < m$). Pour $p \neq 2$, écrivons le nombre (7) sous la forme

$$\frac{\mathrm{C}_{m+1}^{k+1}}{m+1} p^{m-k} = \frac{m(m-1) \ldots (k+1)}{(m-k+1)!} p^{m-k}.$$

Le nombre p figure dans $(m-k+1)! = r!$ avec l'exposant

$$\left[\frac{r}{p}\right] + \left[\frac{r}{p^2}\right] + \ldots < \frac{r}{p} + \frac{r}{p^2} + \ldots = \frac{r}{p-1} \leqslant \frac{r}{2} \leqslant r - 1 = m - k,$$

et par suite $\frac{1}{(m-k+1)!} p^{m-k}$ est un nombre p-entier divisible par p.

On a ainsi démontré que $p\mathrm{B}_m$ est p-entier et que

$$p\mathrm{B}_m \equiv \mathrm{S}_m(p) \pmod{p} \tag{8}$$

dans l'anneau des nombres p-entiers

D'autre part, on a les congruences

$$\mathrm{S}_{(p)} \equiv -1 \pmod{p} \quad \text{si} \quad (p-1) \mid m; \tag{9}$$

$$\mathrm{S}_{(p)} \equiv 0 \pmod{p} \quad \text{si} \quad (p-1) \nmid m. \tag{10}$$

En effet, si $(p-1) \mid m$, alors $x^m \equiv 1 \pmod p$ pour $1 \leqslant x \leqslant p-1$, d'où

$$S_m(p) = \sum_{x=1}^{p-1} x^m \equiv \sum_{x=1}^{p-1} 1 = p-1 \equiv -1 \pmod p.$$

Si maintenant $(p-1) \nmid m$, soit g une racine primitive modulo p; nous aurons

$$S_m(p) = \sum_{x=1}^{p-1} x^m \equiv \sum_{r=0}^{p-2} g^{mr} = \frac{g^{(p-1)m}-1}{g^m-1} \equiv 0 \pmod p,$$

puisque $g^{p-1} \equiv 1 \pmod p$ et $g^m \not\equiv 1 \pmod p$.

Réunissant (8) et (10), nous obtenons que, si $(p-1) \nmid m$, alors $pB_m \equiv 0 \pmod p$, i. e. B_m est p-entier. Le deuxième argument du théorème 4 résulte des congruences (8) et (9).

Dans le cas $m \leqslant p-1$, le nombre $p-1$ ne divise aucun des nombres $k < m$ et par suite tous les B_k pour $k < m$ sont p-entiers et par suite tous les termes qui figurent dans la somme de droite de l'égalité (6) sont divisible par p^2. On a donc le résultat suivant.

COROLLAIRE. — Si $p \neq 2$ et $m \leqslant p-1$ (m pair), *alors*

$$pB_m \equiv S_m(p) \pmod{p^2}. \tag{11}$$

THÉORÈME 5 (congruence de Kummer). — *Si p est premier et $(p-1) \nmid m$ (m est pair positif), alors le nombre $\frac{B_m}{m}$ est un nombre p-entier et on a la* **congruence**

$$\frac{B_{m+p-1}}{m+p-1} \equiv \frac{B_m}{m} \pmod p. \tag{12}$$

Autrement dit, les quotients $\frac{B_m}{m}$ (pour $(p-1) \nmid m$) sont périodiques modulo p, de période $p-1$.

DÉMONSTRATION. — Considérons la fonction

$$F(t) = \frac{gt}{e^{gt}-1} - \frac{t}{e^t-1} = \sum_{m=1}^{\infty} \frac{B_m(g^m-1)}{m!} t^m, \tag{13}$$

où g est une racine primitive modulo p, $1 < g < p$. Posons $e^t - 1 = u$. Alors

$$F(t) = \frac{gt}{(1+u)^g - 1} - \frac{t}{u} = tG(u),$$

où

$$G(u) = \frac{g}{(1+u)^g - 1} - \frac{1}{u} = \frac{g}{gu + \ldots + u^g} - \frac{1}{u} = \sum_{k=0}^{\infty} c_k u^k.$$

Il est clair que ces nombres c_k sont p-entiers.

Démontrons que, dans le développement de la fonction G(u) suivant les puissances de t :

$$G(u) = G(e^t - 1) = \sum_{k=0}^{\infty} c_k (e^t - 1)^k = \sum_{m=0}^{\infty} \frac{A_m}{m!} t^m, \tag{14}$$

tous les coefficients A_m sont p-entiers et de période $p - 1$ modulo p (pour $m > 0$). Il est clair que si cette dernière propriété est satisfaite pour certaines séries elle l'est aussi pour toute combinaison linéaire à coefficients p-entiers. Il nous suffit donc de le vérifier pour les fonctions $(e^t - 1)^k$. Mais ces fonctions, à leur tour, sont des combinaisons linéaires des fonctions e^{rt} pour des entiers $r \geqslant 0$. Mais

$$e^{rt} = \sum_{n=0}^{\infty} \frac{r^n}{n!} t^n$$

et, d'après le petit théorème de Fermat,

$$r^{n+p-1} \equiv r^n \pmod{p} \qquad \text{pour} \qquad n > 0 ;$$

par suite, les fonctions e^{rt} possèdent la propriété demandée et notre argument sur les coefficients A_m est démontré.

Égalant maintenant les coefficients correspondants dans (13) et (14), nous obtenons

$$\frac{B_m(g^m - 1)}{m!} = \frac{A_{m-1}}{(m-1)!},$$

d'où

$$\frac{B_m}{m}(g^m - 1) = A_{m-1}.$$

Puisque $g^m - 1 \not\equiv 0 \pmod{p}$ pour $(p-1) \nmid m$ et que la suite des nombres $g^m - 1$ possède, d'après le petit théorème de Fermat, la période $p - 1$ modulo p, alors, d'après la propriété démontrée des nombres A_m, les nombres $\frac{B_m}{m}$ pour $(p-1) \nmid m$ sont p-entiers et de période $p - 1$ modulo p. Le théorème 5 est démontré.

THÉORÈME 6. — *Les nombres de Bernoulli* B_{2m} *vérifient la formule*

$$B_{2m} = (-1)^{m-1} \frac{2(2m)!}{(2\pi)^m} \zeta(2m), \tag{15}$$

où $\zeta(2m)$ est la valeur de la fonction zêta de Riemann $\zeta(s)$ pour $s = 2m$.

Pour la démonstration, nous utiliserons la décomposition de $\frac{1}{e^t - 1}$ en série de fractions rationnelles :

$$\frac{t}{e^t - 1} = -\frac{1}{2} + \sum_{n=-\infty}^{+\infty} \frac{1}{t - 2\pi i n} = -\frac{1}{2} + \frac{1}{t} + \sum_{n=1}^{\infty} \frac{2t}{t^2 + (2\pi n)^2}. \quad (16)$$

On peut déduire ce développement par exemple du développement classique suivant de la cotangente :

$$\operatorname{cotg} z = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - (\pi n)^2},$$

en utilisant le fait que

$$\operatorname{cotg} z = i\frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = i + \frac{2i}{e^{2iz} - 1}.$$

Il résulte de (16) que

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + 2\sum_{n=1}^{\infty} \frac{t^2}{t^2 + (2\pi n)^2},$$

et puisque

$$\frac{t^2}{t^2 + (2\pi n)} = \sum_{m=1}^{\infty} (-1)^{m-1} \left(\frac{t}{2\pi n}\right)^{2m},$$

alors

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + 2\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} (-1)^{m-1} \frac{t^{2m}}{(2\pi n)^{2m}}$$

$$= 1 - \frac{t}{2} + \sum_{m=1}^{\infty} (-1)^{m-1} \frac{2\zeta(2m)}{(2\pi)^{2m}} t^{2m}.$$

Comparant cette égalité avec (1) et égalant les coefficients correspondants, nous obtenons l'égalité (15).

La formule (15) permet d'étudier la croissance de $|B_{2m}|$ quand l'indice croît. Puisque $\zeta(2m) > 1$ et $(2m)! > \left(\frac{2m}{e}\right)^{2m}$ (cela résulte de la formule bien connue de Stirling), alors

$$|B_{2m}| > 2\left(\frac{m}{\pi e}\right)^{2m}.$$

Nous obtenons en particulier que

$$\frac{|B_{2m}|}{2m} \to \infty \qquad \text{pour} \qquad m \to \infty.$$

EXERCICES

1. Démontrer que

$$(x + \mathbf{B})^m = (x - 1 - \mathbf{B})^m, \qquad m \geqslant 1.$$

2. Démontrer que

$$\left(\frac{1}{2} + \mathbf{B}\right)^m = \left(\frac{1}{2^{m-1}} - 1\right)\mathbf{B}_m.$$

3. Soit p un nombre premier, $p \neq 2$. Démontrer que

$$\sum_{x=1}^{\frac{p-1}{2}} x^{\frac{p-1}{2}} \equiv 2((f) - 2)\mathbf{B}_{\frac{p+1}{2}} \pmod{p}.$$

4. Soit $p > 3$ un nombre premier de la forme $4k + 3$. Démontrer que le nombre h des classes de diviseurs du corps quadratique imaginaire $\mathbf{Q}(\sqrt{-p})$ satisfait à la congruence

$$h \equiv -2\mathbf{B}_{\frac{p+1}{2}} \pmod{p}.$$

5. Démontrer que, pour $p > 3$ premier,

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$$

6. Démontrer la formule

$$(kx + \mathbf{B})^m = k^{m-1} \sum_{s=0}^{k-1} \left(x + \frac{s}{k} + \mathbf{B}\right)^m$$

(k et m sont des entiers naturels).

7. La fonction tg x admet la décomposition

$$\operatorname{tg} x = \sum_{n=1}^{\infty} \mathbf{T}_n \frac{x^{2n-1}}{(2n-1)!}$$

où

$$\mathbf{T}_n = 2^{2n}(2^{2n} - 1)\frac{|\mathbf{B}_{2n}|}{2n}.$$

Démontrer que tous les coefficients $\mathbf{T}_n$ sont des entiers naturels.

8. Pour $m > 1$, démontrer

$$2\mathbf{B}_{2m} \equiv 1 \pmod{4}.$$

9. Soit q un nombre premier tel que $2q + 1$ ne soit pas premier (par exemple $q \equiv 1 \pmod{3}$). Démontrer que le numérateur du nombre de Bernoulli $\mathbf{B}_{2q}$ contient (en écriture irréductible) un nombre premier de la forme $4n + 3$.

10. Soient $p_1, \ldots, p_s$ des nombres premiers supérieurs à 3,

$$\mathbf{M} = (p_1 - 1) \ldots (p_s - 1)$$

et q un entier naturel satisfaisant à la congruence $q \equiv 1 \pmod{\mathbf{M}}$. Démontrer qu'aucun des nombres premiers $p_1, \ldots, p_s$ ne figure dans le dénominateur de la fraction $\frac{\mathbf{B}_{2q}}{2q}$.

APPENDICE ALGÉBRIQUE

§ 1. — FORMES QUADRATIQUES SUR UN CORPS QUELCONQUE DE CARACTÉRISTIQUE DIFFÉRENTE DE 2

Nous exposerons dans ce paragraphe une série de résultats généraux sur les formes quadratiques sur un corps quelconque. Dans le cas de résultats bien connus, nous nous contenterons de les énoncer. K désignera, sauf précisions supplémentaires, un corps arbitraire dont la caractéristique est différente de 2. Pour toute matrice rectangulaire **A** on désignera par A' la matrice transposée.

1) Équivalence des formes quadratiques

On appelle forme quadratique sur un corps K un polynôme homogène de degré 2 à coefficients dans K. Toute forme quadratique f peut s'écrire sous la forme

$$f = \sum_{i,j} a_{ij} x_i x_j$$

avec $a_{ij} = a_{ji}$. La matrice symétrique $A = (a_{ij})$ s'appelle la matrice de la forme quadratique f. La forme quadratique est complètement déterminée par la donnée de sa matrice à la désignation des variables près. Le déterminant $d = \det A$ s'appelle le ***déterminant*** de la forme quadratique ; si $d = 0$, la forme f est dite ***singulière*** et ***non singulière*** dans le cas contraire. Désignant par X la matrice colonne des variables $x_1, x_2, \ldots, x_n$, nous pouvons écrire ainsi la forme quadratique f :

$$f = X'AX.$$

Supposons qu'à la place des variables $x_1, \ldots, x_n$ on introduise de nouvelles variables $y_1, \ldots, y_n$ par les formules

$$x_i = \sum_{j=1}^{n} c_{ij} y_i \qquad (1 \leqslant i \leqslant n,\ c_{ij} \in \mathrm{K}).$$

sous forme matricielle, cette transformation linéaire peut s'écrire sous la forme

$$X = CY,$$

où Y est la matrice colonne des variables $y_1, \ldots, y_n$ et C la matrice (c_{ij}). Remplaçant dans la forme quadratique f les variables $x_1, \ldots, x_n$ par leur expression en fonction de $y_1, \ldots$, y, nous obtenons (après avoir effectué toutes les opérations convenables) une nouvelle forme quadratique g (encore sur le corps K) des variables $y_1, \ldots$, y,. La matrice A, de la forme quadratique g est

$$A, = C'AC. \qquad (1)$$

Deux formes quadratiques f et g sont dites ***équivalentes*** et on note $f \sim g$, s'il existe une transformation linéaire non singulière des variables par laquelle une des formes est transformée en l'autre (à la désignation des variables près). De la formule (1) résulte :

THÉORÈME. — ***Si deux formes quadratiques sont équivalentes, alors leurs déterminants diffèrent l'un de l'autre par un facteur non nul qui est un carré dans* K.**

Soit y un élément quelconque de K. S'il existe dans **K** des éléments $\alpha_1, \ldots$, a, tels que

$$f(\alpha_1, \ldots, \alpha_n) = y,$$

on dit que la ***forme quadratique f représente y.*** En d'autres termes, l'élément y est représenté par la forme f s'il est la valeur de cette forme pour certaines valeurs des variables. On voit facilement que des formes quadratiques équivalentes représentent les mêmes éléments du corps K.

Nous dirons de plus que la ***forme quadratique représente zéro dans le corps*** K s'il existe des nombres de **K** non tous nuls $\alpha_i \in K$ $(1 \leqslant i \leqslant n)$ tels que $f(\alpha_1, \ldots, \alpha_n) = 0$. Il est clair que, pour une forme, la propriété de représenter zéro est conservée par passage à une forme équivalente.

THÉORÈME 2. — ***Si une forme quadratique à n variables représente un élément $a \neq 0$, elle est équivalente à une forme du type***

$$\alpha x_1^2 + g(x_2, \ldots, x_n)$$

où g est une forme quadratique à $n - 1$ variables.

Pour la démonstration de ce théorème, remarquons ce qui suit. Si

$$f(\alpha_1, \ldots, \alpha_n) = \alpha,$$

alors tous les α_i ne sont pas nuls; nous pouvons donc construire une matrice C non singulière dont la première ligne est constituée par les nombres $\alpha_1, \ldots$ a,,.

Si maintenant nous effectuons sur les variables de la forme f la transformation linéaire de matrice C, nous obtenons une forme dont le coefficient du carré de la première variable est égal à a. On continue alors la démonstration comme d'habitude.

Si la matrice d'une forme quadratique est diagonale (tous les coefficients des produits de variables différents sont égaux à 0), nous dirons que cette forme est *diagonale*. Du théorème 2 résulte facilement.

THÉORÈME 3. — *Toute forme quadratique sur un corps* K *peut être mise sous forme diagonale par une transformation linéaire non singulière des variables.*

Autrement dit, toute forme quadratique est équivalente à une forme diagonale.

En termes matriciels, le théorème 3 signifie que pour toute matrice symétrique A il existe une matrice non singulière C telle que la matrice C'AC soit diagonale.

2) Somme directe de formes quadratiques

Puisque la désignation des variables est sans importance, nous pouvons considérer que deux formes quadratiques f et g n'ont pas de variable commune. La forme f + g s'appelle alors *somme directe des formes f et g* et se désigne par *f-j-* g (à ne pas confondre avec l'addition usuelle des formes quadratiques des mêmes variables). Il est évident que si g $\sim h$, alors $f \dotplus g \sim f \dotplus h$. Ce dernier fait admet une réciproque.

THÉORÈME 4 (théorème de Witt). — *Soient f, g, h des formes quadratiques non singulières sur un corps* K. *Si les formes* $f \dotplus g$ *et* $f \dotplus h$ *sont équivalentes, alors les formes g et h sont aussi équivalentes.*

DÉMONSTRATION. — Soit f_0 une forme diagonale équivalente à la forme f. Alors, comme on l'a remarqué ci-dessus, $f \dotplus g \sim f_0 \dotplus g$ et $f \dotplus h \sim f_0 \dotplus h$, d'où $f_0 \dotplus g \sim f_0 \dotplus h$. Ainsi, nous pouvons supposer que f est une forme diagonale. Il est clair maintenant qu'il suffit de considérer le cas $f = ax_0^2$, $a \neq 0$. Désignons par A et B les matrices respectives des formes g et h. Puisque les formes $ax_0^2 \dotplus$ g et $ax_0^2 \dotplus h$ sont équivalentes, il existe une matrice

$$C = \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix}$$

telle que

$$\begin{pmatrix} \gamma & T' \\ S' & Q' \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix}$$

(ici **S** est une matrice ligne et T une matrice colonne). De cette égalité résulte

$$\gamma^2 a + T'AT = a \tag{2}$$

$$\gamma a S + T'AQ = 0 \tag{3}$$

$$S' a S + Q'AQ = B. \tag{4}$$

Il faut montrer qu'il existe une matrice C_0, non singulière, telle que

$$C_0' A C_0 = B.$$

Nous chercherons cette matrice sous la forme

$$C_0 = Q + \xi TS,$$

où ξ sera choisi de manière convenable. D'après (2) et (3), nous avons

$$\begin{aligned} C_0' A C_0 &= (Q' + EST')\, A(Q + \xi TS) \\ &= Q'AQ + \xi S'T'AQ + \xi Q'ATS + \xi^2 S'T'ATS \\ &= Q'AQ + a[(1-\gamma^2)\xi^2 - 2\gamma\xi]S'S. \end{aligned}$$

D'après l'égalité (4), cette dernière expression sera égale à la matrice B si $(1 - \gamma^2)\xi^2 - 2\gamma\xi = 1$. L'équation en ξ obtenue peut s'écrire sous la forme $\xi^2 - (\gamma\xi + 1)^2 = 0$ et a donc une solution ξ_0 dans le corps K pour tout $\gamma \in K$ (la caractéristique de K n'est pas égale à 2). Ainsi, nous avons trouvé une matrice $C_0 = Q + \xi_0 TS$ telle que $C_0' A C_0 = B$. Puisque par hypothèse la matrice B est non singulière, il en est de même de C_0. Le théorème 4 est démontré.

3) Représentation des éléments du corps

THÉORÈME 5. — *Si une forme quadratique non singulière représente zéro dans le corps* **K**, *elle représente aussi tous les éléments de* K.

DÉMONSTRATION. — Puisque des formes équivalentes représentent les mêmes éléments du corps, il suffit de démontrer le théorème pour une forme diagonale $f = a_1x_1^2 + \ldots + a_nx_n^2$. Soit $a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2 = 0$, une représentation non nulle de zéro et soit y un élément quelconque du corps K. Nous pouvons supposer que $\alpha_1 \neq 0$. Donnons aux variables $x_1, \ldots, x_n$ les valeurs

$$x_1 = \alpha_1(1 + t), \qquad x_k = \alpha_k(1 - t) \qquad k = 1, 2, \ldots, n,$$

où t est une nouvelle variable et substituons ces valeurs dans la forme f; nous obtenons

$$f^* = f^*(t) = 2a_1\alpha_1^2 t - 2a_2\alpha_2^2 t - \ldots - 2a_n\alpha_n^2 t = 4a_1\alpha_1^2 t$$

Si nous posons maintenant $t = \dfrac{\gamma}{4a_1\alpha_1^2}$, nous obtenons $f^*(t) = y$.

THÉORÈME *6.* — ***Une forme quadratique non singulière f représente un élément*** $y \neq 0$ ***de*** K ***si et seulement si la forme*** $-\gamma x_0^2 + f$ ***représente zéro.***

DÉMONSTRATION. — La nécessité de la condition est évidente. Supposons

$$-\gamma\alpha_0^2 + f(\alpha_1, \ldots, \alpha_n) = 0,$$

tous les α_i n'étant pas nuls. Si $\alpha_0 \neq 0$, alors $y = f\left(\frac{\alpha_1}{\alpha_0}, \ldots, \frac{\alpha_n}{\alpha_0}\right)$. Si maintenant $\alpha_0 = 0$, la forme f représente zéro et par suite, d'après le théorème 5, elle représente aussi tous les éléments du corps K.

Remarque. — Il résulte de la démonstration du théorème 6 que nous obtenons toutes les représentations de l'élément y par la forme f à partir des représentations de zéro par la forme $-\gamma_2 x_0^2 + f$ (il suffit de connaître toutes les représentations telles que $x_0 \neq 0$). Ainsi l'étude des représentations par des formes quadratiques non singulières des éléments non nuls d'un corps K se ramène à l'étude des représentations de zéro par des formes non singulières à une variable de plus.

THÉORÈME *7.* — ***Si pour une forme*** f ***représentant zéro, on connaît une représentation de zéro, on peut trouver explicitement une transformation linéaire non singulière des variables telle que la transformée de*** f ***soit du type***

$$y_1y_2 + g(y_3, \ldots, y_n).$$

DÉMONSTRATION. — D'après la démonstration du théorème 5, on peut trouver $\alpha_1, \ldots, \alpha_n$, tels que $f(\alpha_1, \ldots, \alpha_n) = 1$. D'après le théorème 2, on peut maintenant transformer f en la forme $x_1^2 + f_1(x_2, \ldots, x_n)$. Puisqu'on connaît une représentation de zéro de la forme $x_1^2 + f_1$ on peut trouver $\beta_2, \ldots, \beta_n$ tel que $f_1(\beta_2, \ldots, \beta_n) = -1$. Appliquant de nouveau le théorème *2,* f_1 prend la forme $-x_2^2 + g(y_3, \ldots, y_n)$. Posant $x_1 - x_2 = y_1$, $x_1 + x_2 = y_2$, nous obtenons le résultat demandé.

Remarque. — Supposons que pour toute forme quadratique sur K qui représente zéro dans ce corps, on sache trouver au moins une représentation de zéro. Alors on peut transformer toute forme non singulière en

$$y_1y_2 + \ldots + y_{2s-1}y_{2s} + h(y_{2s+1}, \ldots, y_n), \qquad (5)$$

où la forme h ne représente pas zéro. Pour toute représentation de zéro par la forme (5) la valeur d'une au moins des variables $y_1, y_2, \ldots, y_{2s-1}, y_{2s}$ est non nulle. Pour trouver toutes les représentations telles que, par exemple, $y_1 = \alpha_1 \neq 0$, nous pouvons donner aux variables $y_3, \ldots, y_n$ des valeurs arbitraires $\alpha_3, \ldots, \alpha_n$ et définir la valeur de y_2 par l'équation

$$\alpha_1 y_2 = \alpha_3\alpha_4 + \ldots + g(\alpha_{2s+1}, \ldots, \alpha_n).$$

Ainsi, le problème de la recherche effective de toutes les représentations de zéro dans le corps K par une forme quadratique non singulière est résolu si on connaît des critères permettant de savoir si une forme donnée représente zéro ou non et si on connaît un algorithme permettant de trouver une représentation de zéro pour toute forme représentant zéro.

THÉORÈME 8. — *Soit un corps* K *contenant plus de 5 éléments. Si la forme diagonale*

$$a_1x_1^2 + \ldots + a_nx_n^2 \qquad (a_i \in \mathrm{K})$$

représente zéro dans le corps K, *il existe une représentation de zéro telle que les valeurs de toutes les variables soient différentes de zéro.*

DÉMONSTRATION. — Montrons tout d'abord que si $a\xi^2 = A \neq 0$, alors, pour tout $b \neq 0$ il existe des éléments α et β différents de zéro tels que

$$a\alpha^2 + b\beta^2 = \lambda.$$

Pour le démontrer, considérons l'identité

$$\frac{(t-1)^2}{(t+1)^2} + \frac{4t}{(t+1)^2} = 1.$$

Multipliant cette identité par $a\xi^2 = A$, nous obtenons

$$a\left(\xi\frac{t-1}{t+1}\right)^2 + at\left(\frac{2\xi}{t+1}\right)^2 = A. \tag{6}$$

Choisissons maintenant dans le corps K un élément $\gamma \neq 0$ tel que la valeur $t = t_0 = \frac{b\gamma^2}{a}$ soit différente de ± 1. Puisque chacune des équations

$$bx^2 - a = 0 \qquad \text{et} \qquad bx^2 + a = 0$$

n'a pas plus de deux solutions en x dans K, il y a au plus 5 éléments du corps K qu'on ne peut pas prendre comme y. Puisque par hypothèse le corps K contient plus de 5 éléments, on peut trouver un tel y. Posant $t = t_0$ dans l'identité (6), nous obtenons

$$a\left(\xi\frac{t_0-1}{t_0+1}\right)^2 + b\left(\frac{2\xi\gamma}{t_0+1}\right)^2 = \lambda,$$

ce qui démontre l'affirmation ci-dessus.

Il est maintenant facile de terminer la démonstration du théorème. Si la représentation $a_1\xi_1^2 + \ldots + a_n\xi_n^2 = 0$ est telle que $\xi_1 \neq 0, \ldots, \xi_r \neq 0$, $\xi_{r+1} = \ldots = \xi_n = 0$, avec $r \geqslant 2$, alors, d'après ce qui précède, on peut trouver $\alpha \neq 0$ et $\beta \neq 0$ tels que $a_r\xi_r^2 = a_r\alpha^2 + a_{r+1}\beta^2$ et nous obtenons une

représentation avec une variable de plus non nulle. Répétant ce raisonnement, on obtient une représentation dont toutes les valeurs des variables sont non nulles.

4) Formes quadratiques binaires

On appelle forme ***binaire*** toute forme quadratique de deux variables.

THÉORÈME *9.* — ***Toutes les formes binaires non singulières représentant zéro dans le corps*** K ***sont équivalentes entre elles.***

En effet, d'après le théorème 7, toutes ces formes sont équivalentes à la forme y_1y_2.

THÉORÈME 10. — ***Pour qu'une forme quadratique binaire f de déterminant*** $d \neq 0$ ***représente zéro, il faut et il suffit que*** $-d$ ***soit un carré dans*** K (i. e. $-d = \alpha^2$, $\alpha \in$ K).

DÉMONSTRATION. — La nécessité de la condition découle des théorèmes **1** et 7. Réciproquement, si $f = ax^2 + by^2$ et $-d = -ab = \alpha^2$, alors

$$f(a, a) = a\alpha^2 + ba^2 = 0.$$

THÉORÈME 11. — ***Pour que deux formes binaires non singulières*** f ***et g soient équivalentes sur le corps*** K, ***il faut et il suffit que tout d'abord leurs déterminants diffèrent par un carré dans*** K ***et ensuite qu'il existe dans*** K ***au moins un élément non nul représentable simultanément par les deux formes*** f ***et g.***

DÉMONSTRATION. — La nécessité de ces deux conditions est évidente. Pour démontrer la suffisance, choisissons dans K un élément $\alpha \neq 0$ représentable par les formes f et g. D'après le théorème 2, les formes f et g sont équivalentes respectivement à des formes du type $f_1 = \alpha x^2 + \beta y^2$ et

$$g_1 = \alpha x^2 + \beta' y^2.$$

Mais, d'après la première condition, $\alpha\beta$ diffère de $\alpha\beta'$ par un carré, d'où $\beta' = \beta\gamma^2$, y $\in$ K, ce qui entraîne $f_1 \sim g_1$, d'où $f \sim g$.

EXERCICES

1. Démontrer que toute forme quadratique singulière représente zéro.
2. Démontrer que le théorème **5** n'est pas valable en général pour les formes singulières.
3. Démontrer que si la forme binaire $x^2 - ay^2$ représente deux éléments γ_1 et γ_2 de K elle représente aussi leur produit $\gamma_1\gamma_2$.

4. Montrer que le théorème 8 n'est pas toujours vrai pour les corps dont le nombre d'éléments ne dépasse pas cinq.

5. Considérons la répartition suivante de toutes les formes quadratiques non singulières à $n = 0, 1, 2, \ldots$ variables sur un corps donné K en classse appelées classes de Witt (nous interpréterons zéro comme une forme non singulière d'un ensemble vide de variables et considérerons que cette forme représente zéro). On dit que deux formes f_1 et f_2 appartiennent à la même classe de Witt, $[f_1] = [f_2]$, si après réduction de ces formes à des formes du type (5) les formes correspondantes h (qui ne représentent pas zéro) contiennent le même nombre de variables et sont équivalentes. L'addition des classes de Witt est alors définie par

$$[f_1] + [f_2] = [f_1 + f_2].$$

Démontrer que les classes de Witt forment un groupe pour cette opération.

6. Définir le groupe des classes de Witt pour les formes quadratiques sur le corps des nombres réels ou sur le corps des nombres complexes.

7. Démontrer qu'une forme quadratique sur un corps fini représente zéro si et seulement si le nombre de ses variables est supérieur ou égal à 3 (on suppose la caractéristique du corps différente de 2).

§ 2. — EXTENSIONS ALGÉBRIQUES

Nous énoncerons sans démonstration les théorèmes de ce paragraphe. Le lecteur pourra trouver les démonstrations dans le livre d'algèbre moderne de Van der Waerden, t. 1, chap. 5.

1) Extensions finies

Si un corps Ω contient un corps k comme sous-corps, nous dirons que Ω est une extension du corps k. Si on veut préciser que Ω est considéré comme une extension du corps k, on écrit Ω/k. Un corps K qui est un sous-corps du corps Ω contenant k, i. e. $k \subset K \subset \Omega$, est appelé un ***corps intermédiaire de l'extension*** Ω/k.

On peut considérer toute extension Ω/k comme un espace vectoriel sur le corps k (pour les opérations d'addition dans Ω et de multiplication par les éléments de k).

DÉFINITION. — ***Une extension*** K/k ***est dite finie si le corps*** K, ***considéré comme espace vectoriel sur k, est de dimension finie. Cette dimension s'appelle le degré de l'extension*** K/k ***et est désignée par*** $(K : k)$. ***Toute base de l'espace vectoriel*** K ***sur k est appelée une base de l'extension*** K/k.

Si l'extension K/k est finie, alors, pour tout corps intermédiaire K,,, les extensions K_0/k et K/K_0 sont aussi finies. La réciproque est vraie :

THÉORÈME 1. — ***Soit*** K_0 ***un corps intermédiaire d'une extension*** K/k. ***Si les extensions*** K/K_0 ***et*** K_0/k ***sont finies, alors*** K/k ***est également une extension finie et son degré est égal au produit des degrés des extensions*** K/K_0 ***et*** K_0/k :

$$(K : k) = (K : K_0)(K_0 : k).$$

DÉMONSTRATION. — Soient $\theta_1, \ldots, \theta_m$ une base de K/K_0 et $\omega_1, \ldots, \omega_n$ une base de K_0/k. Puisque tout élément de K se représente comme combinaison linéaire des produits $\omega_i\theta_j$, alors l'extension K/k est finie. De plus, il est facile de voir que ces produits sont linéairement indépendants sur K et par suite $(K : k) = mn$.

Pour tout corps k, on désigne par $k[t]$ l'anneau des polynômes en t à coefficients dans k.

Soit Ω/k une extension du corps k. Un élément $a \in \Omega$ est dit ***algébrique sur k*** si c'est une racine d'un polynôme non nul de l'anneau $k[t]$. Choisissons parmi ces polynômes $f(t)$ (dont a est une racine) le polynôme $\varphi(t)$ non nul de plus bas degré dont le coefficient du terme dominant est égal à 1. Puisque tout $f(t)$ est divisible par $\varphi(t)$ (sinon, le reste de la division par $\varphi(t)$ ne serait pas nul, aurait α comme racine et serait d'un degré inférieur à celui de φ), le polynôme $\varphi(t)$ est défini de manière unique par ces conditions; on l'appelle le ***polynôme minimal*** de l'élément du corps Ω algébrique sur k. Le polynôme minimal $\varphi \in k[t]$ est toujours irréductible puisque la décomposition $\varphi = gh$ entraîne que α est racine de g(t) ou de h(t). Tout élément $a \in k$ est algébrique sur k et son polynôme minimal est $t - a$. **Un élément** $\xi \in \Omega$ qui n'est pas algébrique sur k est dit ***transcendant sur k.***

L'extension Ω/k est dite ***algébrique*** si tout élément $\alpha \in \Omega$ est algébrique sur k.

THÉORÈME *2.* — *Toute extension finie K/k est algébrique.*

THÉORÈME *3.* — ***Soit α un élément d'une extension Ω/k, algébrique sur k et soit $\varphi(t) \in k[t]$ son polynôme minimal, de degré m. Alors les puissances 1, α, . ..) α^{m-1} sont linéairement indépendantes sur k et leurs combinaisons linéaires***

$$a, + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}, \qquad (1)$$

à coefficients $a_i \in k$ forment un corps intermédiaire noté k(u). L'extension $k(\alpha)/k$ est finie et de degré m.

Pour effectuer la somme de deux éléments du corps $k(u)$ écrits sous la forme (1), il est clair qu'il faut additionner les coefficients correspondants. Pour mettre sous la forme (1) le produit des éléments $\xi = g(\alpha)$ et $\eta = h(a)$, où $g(t)$ et $h(t)$ sont des éléments de $k[t]$ de degré $\leqslant m - 1$, on divise gh par φ,

$$g(t)\,h(t) = \varphi(t)\,q(t) + r(t),$$

le reste r(t) étant de degré inférieur ou égal à $m - 1$; puisque $\varphi(\alpha) = 0$, alors $\xi\eta = r(a)$. Ainsi l'opération de multiplication dans l'extension $k(\alpha)/k$ est complètement définie par la connaissance du polynôme minimal $\varphi(t)$ de l'élément α.

Soient $\alpha_1, \ldots, \alpha_s$ un nombre fini d'éléments du corps Ω, algébriques sur k et soient $m_1, \ldots, m_s$ les degrés respectifs de leurs polynômes minimaux sur k. L'ensemble de toutes les combinaisons linéaires des éléments

$$\alpha_1^{k_1} \ldots \alpha_s^{k_s} \qquad (0 \leqslant k_1 < m_1, \ldots, 0 \leqslant k_s < m_s),$$

à coefficients dans k, est un corps intermédiaire que nous désignerons par $k(\alpha_1, \ldots, \alpha_s)$; on l'appelle le corps engendré par les éléments $\alpha_1, \ldots, \alpha_s$. Son degré sur k est inférieur ou égal au produit $m_1 \ldots m_s$.

Toute extension finie $\mathbf{K}/k$ contenue dans Ω se représente sous la forme $\mathbf{K} = k(\alpha_1, \ldots, \alpha_s)$ pour certains $\alpha_1, \ldots, \alpha_s$.

DÉFINITION. — *Une extension finie $\mathbf{K}/k$ est dite monogène s'il existe un élément θ dans* K *tel que* K = $k(\theta)$. *Tout élément $\theta \in$* K *tel que* K = $k(\theta)$ *est appelé un élément primitif du corps* K *sur* le *corps k.*

Les éléments primitifs du corps K sur k sont caractérisés, c'est clair, par le fait que le degré de leur polynôme minimal est égal au degré de l'extension $\mathbf{K}/k$.

THÉORÈME 4. — *Soient Ω/k et Ω'/k deux extensions du corps k et soient des éléments $\theta \in \Omega$ et $\theta' \in \Omega'$ algébriques sur k, possédant le même polynôme minimal $\varphi(t)$; alors il existe un isomorphisme (et un seul) du corps* K(θ) *sur le corps* K(θ') *tel que $\theta \to \theta'$ et $a \to a$ pour tout $a \in k$.*

Soit m le degré du polynôme $\varphi(t)$. L'isomorphisme $k(\theta) \to k(\theta')$ défini par le théorème 4 coïncide avec l'application

$$a_0 + a_1\theta + \ldots + a_{m-1}\theta^{m-1} \to a_0 + a_1\theta' + \ldots + a_{m-1}\theta'^{m-1} \qquad (2)$$

($a_0, a_1, \ldots, a_{m-1}$ sont des éléments quelconques du corps k).

Jusqu'à présent, nous n'avons considéré que des extensions finies $\mathbf{K}/k$ contenues dans une extension précédemment donnée Ω/k. Étudions maintenant la construction des extensions finies d'un corps fondamental fixé k.

THÉORÈME 5. — *Soit k un corps. Pour tout polynôme irréductible $\varphi(t) \in k[t]$ de degré n, il existe une extension finie $\mathbf{K}/k$ de degré n dans laquelle ce polynôme φ a une racine. L'extension $\mathbf{K}/k$ est unique, à un isomorphisme laissant invariant les éléments de k près. Si $\varphi(\theta) = 0$, $\theta \in$* K, *alors* K = $k(\theta)$.

Le corps K (pour $n > 1$) se construit ainsi. Choisissons un nouvel objet θ et considérons l'ensemble K de toutes les combinaisons linéaires formelles de θ,

$$a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} \qquad (3)$$

à coefficients $a_i \in$ K. Si on désigne par $g(t)$ le polynôme

$$a_0 + a_1 t + \ldots + a_{n-1}t^{n-1},$$

l'expression (3) peut aussi s'écrire sous la forme g(0). Soit $\xi = g(\theta)$ et $\eta = h(\theta)$ deux combinaisons linéaires du type (3) (g et $h \in k[t]$ et sont de degrés $\leqslant n - 1$). Désignons par s(t) la somme g(t) + $h(t)$ et par r(t) le reste de la division du produit de $h(t)$ g(t) par $\varphi(t)$. Posons

$$\xi + \eta = s(\theta)$$
$$\xi\eta = r(\theta).$$

Il est maintenant facile de vérifier que pour ces opérations, l'ensemble K est le corps cherché.

COROLLAIRE. — *Pour tout polynôme $h(t) \in k[t]$, il existe une extension finie K/k dans laquelle h(t) se décompose en facteurs linéaires.*

2) Normes et traces

Soit K/k une extension finie de degré n. Pour tout élément $\alpha \in K$, l'application $\xi \to \alpha\xi$ ($\xi \in K$) est une transformation linéaire de K (comme espace vectoriel sur k). Le polynôme caractéristique $f_\alpha(t)$ de cette transformation linéaire est aussi appelé *polynôme caractéristique de l'élément* $\alpha \in K$ dans l'extension K/k. Soient $\omega_1, \ldots, \omega_n$ une base de l'extension K/k et

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j, \qquad a_{ij} \in k ; \tag{4}$$

alors

$$f_\alpha(t) = \det (tE - (a_{ij})),$$

où E est la matrice unité d'ordre n.

THÉORÈME 6. — *Le polynôme caractéristique $f_\alpha(t)$ d'un élément $a \in K$ dans l'extension K/k est égal à une puissance de son polynôme minimal $\varphi_\alpha(t)$ par rapport à k.*

DÉMONSTRATION. — Soit

$$\varphi_\alpha(t) = t^m + c_1 t^{m-1} + \ldots + c_r.$$

D'après le théorème 3, les nombres $1, \alpha, \ldots, \alpha^{m-1}$ forment une base de l'extension $k(\alpha)/k$. Si $\theta_1, \ldots, \theta_s$ est une base de $K/k(\alpha)$, on peut prendre comme base de K/k les produits

$$\theta_1, \alpha\theta_1, \ldots, \alpha^{m-1}\theta_1 ; \ldots ; \theta_s, \alpha\theta_s, \ldots, \alpha^{m-1}\theta_s.$$

La matrice de la transformation linéaire $\xi \to \alpha\xi$ par rapport à cette base est

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & & 0 & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \dots & -c_2 & -c_1 \end{pmatrix}$$

Son polynôme caractéristique, comme on le vérifie facilement est égal à $t^m + c_1 t^{m-1} + \dots + c_m$, i. e. est égal à $\varphi_\alpha(t)$. Par suite $f_\alpha = \varphi_\alpha^s$ et le théorème 6 est démontré.

Puisque, par passage d'une base de l'espace à un autre, la matrice d'une application linéaire est remplacée par une matrice équivalente, le déterminant et la trace de la matrice (a_{ij}) définie par les égalités (4) ne dépend pas du choix de la base $\omega_1, \dots, \omega_n$.

DÉFINITION. — ***Le déterminant*** $\det(a_{ij})$ ***de la matrice*** (a_{ij}) ***et sa trace***

$$\operatorname{Tr}(a_{ij}) = \sum_{i=1}^{n} a_{ii}$$

sont appelés respectivement norme et trace ***de l'élément*** $\alpha \in K$ ***dans l'extension*** K/k. La norme et la trace sont désignées respectivement par $N_{K/k}(\alpha)$. et $\mathrm{Tr}_{K/k}(\alpha)$ ou, plus simplement, par $N(a)$ et Tr (a).

Pour $a \in k$, la matrice de la transformation linéaire $\xi \to a\xi$ ($\xi \in K$) est la matrice diagonale $a\mathrm{E}$. Par suite, pour $a \in k$, on a

$$N_{K/k}(a) = a^n$$
$$\mathrm{Tr}_{K/k}(a) = na.$$

D'après les propriétés des matrices des applications linéaires, on a, pour $\alpha, \beta \in K$,

$$N_{K/k}(\alpha\beta) = N_{K/k}(\alpha) N_{K/k}(\beta), \tag{5}$$
$$\mathrm{Tr}_{K/k}(\alpha + \beta) = \mathrm{Tr}_{K/k}(\alpha) + \mathrm{Tr}_{K/k}(\beta). \tag{6}$$

La matrice de la transformation linéaire $\xi \to a\alpha\xi$ ($a \in k$, $\alpha \in K$) est obtenue en multipliant par a tous les termes de la matrice de la transformation $\xi \to \alpha\xi$. Par suite, on a la formule

$$\mathrm{Tr}_{K/k}(a\alpha) = a\,\mathrm{Tr}_{K/k}(\alpha) \qquad (a \in k,\ \alpha \in K). \tag{7}$$

Si $a \neq 0$, d'après la non-singularité de l'application $\xi \to \alpha\xi$, la norme $N_{K/k}(a)$ est différente de zéro. La formule (5) montre que l'application

$\alpha \to N_{K/k}$ (a) est un homomorphisme du groupe multiplicatif K* du corps K dans le groupe multiplicatif k^* du corps k. En ce qui concerne l'application $a \to Tr_{K/k}$ a de K dans k, il résulte de (6) et (7) qu'elle est linéaire.

THÉORÈME 7. — *Soit Ω/k une extension telle que le polynôme caractéristique $f_\alpha(t)$ de l'élément $\alpha \in K$ dans une extension finie K/k soit décomposable en facteurs linéaires dans Ω :*

$$f_\alpha(t) = (t - a_1) \dots (t - \alpha_n).$$

Alors

$$N_{K/k}(\alpha) = \alpha_1\alpha_2 \dots \alpha_n$$

$$Tr_{K/k}(\alpha) = \alpha_1 + \alpha_2 + \dots + a_n.$$

DÉMONSTRATION. — Si

$$f_\alpha(t) = \det(tE - (a_{ij})) = t^n + a_1t^{n-1} + \dots + a_n,$$

alors

$$a_1 = -\operatorname{Tr}(a_{ij}), \qquad a_n = (-1)^n \det(a_{ij}).$$

D'autre part, d'après les formules de Viète,

$$\alpha_1 + \alpha_2 + \dots + a_n = -a_n, \qquad \alpha_1\alpha_2 \dots a_n = (-1)^n a_n,$$

d'où le théorème.

THÉORÈME 8. — *Avec les notations et hypothèses du théorème 7, le polynôme caractéristique $f_\gamma(t)$ d'un élément $\gamma = g(a) \in K$ ($g(t) \in k[t]$) admet la décomposition*

$$(t - g(\alpha_1))(t - g(\alpha_2)) \dots (t - g(\alpha_n)) \tag{8}$$

dans le corps Ω.

DÉMONSTRATION. — Remarquons tout d'abord que les coefficients du polynôme (8), étant des expressions symétriques de $\alpha_1, \dots, a_n$, appartiennent au corps k. Soit $\varphi_\gamma(t)$ le polynôme minimal de l'élément γ sur K. En soumettant l'égalité $\varphi_\gamma(\alpha) = 0$ à l'isomorphisme $k(\alpha) \to k(\alpha_i)$ (tel que $a \to \alpha_i$ et $a \to a$ pour $a \in k$), on obtient $\varphi_\gamma(g(\alpha_i)) = 0$. Toutes les racines du polynôme (8) sont ainsi les racines du polynôme $\varphi_\gamma(t)$, irréductible sur k et cela n'est possible que si ce polynôme est une puissance de $\varphi_\gamma(t)$. Pour terminer la démonstration, il suffit d'appliquer le théorème 6.

Soit $k \subset K \subset L$ une chaîne d'extensions finies. Choisissons pour K/k et L/K respectivement des bases $\omega_1, \dots, w_n$ et $\theta_1, \dots, \theta_m$. Pour tout $\gamma \in L$, posons

$$\gamma\theta_j = \sum_{s=1}^{m} \alpha_{js}\theta_s, \qquad \alpha_{js} \in K$$

$$\alpha_{js}\omega_i = \sum_{r=1}^{n} a_{jsir}\omega_r, \qquad a_{jsir} \in k.$$

Puisque

$$\gamma\omega_i\theta_j = \sum_{s,r} a_{jsir}\omega_r\theta_s,$$

alors

$$\mathrm{Tr}_{L/K}(\gamma) = \sum_{i,j} a_{jjii}.$$

D'autre part, nous avons aussi

$$\mathrm{Tr}_{K/k}(\mathrm{Tr}_{L/K}(\gamma)) = \mathrm{Tr}_{K/k}\left(\sum_j a_{jj}\right) = \sum_{i,j} a_{jjii}.$$

Par suite, pour tout $y \in K$, on a

$$\mathrm{Tr}_{L/k}(\gamma) = \mathrm{Tr}_{K/k}(\mathrm{Tr}_{L/K}(\gamma)). \tag{9}$$

On a une formule analogue pour la norme (exercice 2).

3) Extensions séparables

DÉFINITION. — *Une extension finie K/k est dite séparable si l'application linéaire $\xi \to \mathrm{Tr}_{K/k}(\xi)$, $\xi \in K$, n'est pas identiquement nulle.*

Si la caractéristique du corps k est nulle, alors $\mathrm{Tr}_{K/k}(1) = n = (K : k)$. Par suite, toutes les extensions finies d'un corps de caractéristique zéro sont séparables. C'est vrai aussi, bien entendu, pour toutes les extensions finies d'un corps de caractéristique p dont le degré n'est pas divisible par p.

Choisissons dans une extension finie séparable K/k une base $\omega_1, \ldots, \omega_n$ et considérons la matrice

$$(\mathrm{Tr}(\omega_i\omega_j))_{1 \leqslant i,j \leqslant n}. \tag{10}$$

Si le déterminant de cette matrice était nul, alors on pourrait trouver dans le corps k des éléments non tous nuls $c_1, \ldots, c_n$ tels que

$$\sum_{j=1}^{n} c_j \mathrm{Tr}(\omega_i\omega_j) = 0 \qquad (i = 1, \ldots, n).$$

Posant $y = c_1\omega_1 + \ldots + c_n\omega_n$, nous pouvons transcrire ces égalités sous la forme

$$\mathrm{Tr}(\omega_i\gamma) = 0 \qquad (i = 1, \ldots, n). \tag{11}$$

Soit ξ un élément quelconque de K. Puisque $y \neq 0$, on peut représenter ξ sous la forme

$$\xi = a_1\omega_1\gamma + \ldots + a_n\omega_n\gamma \qquad (a_i \in k),$$

d'où, d'après (6), (7) et (Il), Tr $(\xi) = 0$. Cela contredit la séparabilité de K/k. Ainsi la matrice (10) est toujours non singulière pour toute extension séparable.

DÉFINITION. — *Le déterminant* $\det(\mathrm{Tr}(\omega_i\omega_j))$ *est appelé le discriminant de la base* $\omega_1, \ldots, \omega_n$ *de l'extension finie séparable* K/k *et est désigné par* $D(\omega_1, \ldots, \omega_n)$.

D'après ce qui précède, le discriminant de toute base d'une extension finie séparable est un élément non nul du corps de base.

Soit $\omega_1', \ldots, \omega_n'$ une autre base de l'extension K/k et soit

$$\omega_i' = \sum_{j=1}^{n} c_{ij}\omega_j \qquad (i = 1, \ldots, n).$$

Puisque la matrice $(\mathrm{Tr}(\omega_i'\omega_j'))$ est égale au produit $(c_{ij})\,(\mathrm{Tr}(\omega_i\omega_j))\,(c_{ij})'$ (le prime indique la transposition de la matrice), alors

$$D(o;, \ldots, \omega_n') = (\det(c_{ij}))^2\, D(\omega_1, \ldots, \omega_n). \tag{12}$$

Ainsi, les discriminants de deux bases différentes diffèrent l'un de l'autre par un facteur qui est le carré d'un élément du corps fondamental.

Fixons une base quelconque de l'extension K/k. Alors pour des éléments quelconques $c_1, \ldots, c_n$ du corps k il existe un élément $\alpha \in K$ (et un seul) tel que

$$\mathrm{Tr}(\omega_i\alpha) = c \qquad (i = 1, \ldots, n). \tag{13}$$

En effet, écrivant α sous la forme $a = x_1\omega_1 + \ldots + x_n\omega_n$ $(x_j \in k)$ et substituant cette expression de a dans l'égalité (13), nous obtenons un système de n-équations linéaires à n inconnues $x_1, \ldots, x_n$ dont le déterminant est différent de zéro. Ainsi, on peut trouver dans le corps K n éléments $\omega_1^*, \ldots, \omega_n^*$ tels que

$$\mathrm{Tr}(\omega_i\omega_i^*) = \begin{cases} 1 & \text{pour } i = j \\ 0 & \text{pour } i \neq j \end{cases} \tag{14}$$

Ces n éléments ω_j^* sont linéairement indépendants sur k puisque si

$$c_1\omega_1^* + \ldots + c_n\omega_n^* = 0 \qquad (c_i \in k),$$

alors multipliant cette égalité par ω_i et prenant la trace on obtient $c_i = 0$ pour tout i = 1, . . ., n.

DÉFINITION. — *La base* $\omega_1^*, \ldots, \omega_n^*$ *de l'extension séparable* K/k *définie de manière unique par les égalités* (14) *est appelée base duale de la base* $\omega_1, \ldots, \omega_n$.

La base duale permet d'écrire sous forme simple les valeurs des coefficients $a_i \in k$ dans la décomposition

$$a = a_1\omega_1 + \ldots + a_n\omega_n,$$

d'un élément quelconque a de K. En effet, prenant la trace du produit $\alpha\omega_i^*$, nous obtenons les formules

$$a_i = \mathrm{Tr}\,(\alpha\omega_i^*) \qquad (i = 1, \ldots, n).$$

Supposons que le polynôme minimal $\varphi(t)$ d'un élément α dans une extension séparable K/k se décompose en facteurs linéaires dans l'extension Ω/k :

$$\varphi(t) = (t - \alpha_1) \ldots (t - a_n).$$

Il résulte de manière évidente de la formule (9) que, de même que K/k, l'extension $k(\alpha)/k$ est aussi séparable. Puisque le polynôme minimal φ est aussi le polynôme caractéristique de a dans l'extension $k(\alpha)/k$, alors, d'après les théorèmes 7 et 8

$$\mathrm{Tr}_{k(\alpha)/k}(\alpha^k) = \sum_{s=1}^{m} \alpha_s^k,$$

et par suite le discriminant D = D (1, a, . . . , α^{m-1}) de la base 1, $a, \ldots, \alpha^{m-1}$ de l'extension $k(\alpha)/k$ s'écrit

$$\mathrm{D} = \det\left(\sum_{s=1}^{m} a_s^{i+j}\right)_{0 \leqslant i,\, j \leqslant m-1} = \det\left(\alpha_s^i\right) \cdot \det\left(\alpha_s^j\right) = \prod_{0 \leqslant i,\, j \leqslant m-1} (\alpha_i - \alpha_j)^2.$$

Mais D $\neq 0$, d'où $\alpha_i \neq \alpha_j$ et nous avons établi le résultat suivant.

THÉORÈME 9. — *Le polynôme minimal de tout élément d'une extension séparable n'a pas de racine multiple* (dans tout corps où il se décompose en facteurs linéaires).

THÉORÈME 10 (théorème de l'élément primitif). — *Toute extension finie séparable* K/k *est monogène,* i. *e. il existe un élément* θ *tel que* $\mathrm{K} = k(\theta)$.

THÉORÈME 11. — *Pour toute extension finie séparable de degré n, il existe n isomorphismes (et n seulement) de l'extension* Ω/k *laissant fixe tout élément de k. Si* $\sigma_1, \ldots, \sigma_n$ *sont ces isomorphismes, pour tout élément* $a \in \mathrm{K}$, *le polynôme caractéristique* $f_\alpha(t)$ *admet dans* Ω *la décomposition*

$$f_\alpha(t) = (t - \sigma_1(\alpha))\,(t - \sigma_2(\alpha)) \ldots (t - \sigma_n(\alpha)).$$

Les éléments $\sigma_1(\alpha), \ldots,$ a,(a) (appartenant au corps CI) sont appelés les *conjugués* de l'élément $a \in \mathrm{K}$. Les images o,(K), . . . , o,(K) du corps K par les isomorphismes σ_i sont appelés *corps conjugués* du corps K. Si θ est un élément primitif du corps K/k, il est évident que $\sigma_i(\mathrm{K}) = k(\sigma_i(\theta))$.

COROLLAIRE 1. — *Avec ces notations, nous avons*

$$N_{K/k}(\alpha) = \sigma_1(\alpha)\,\sigma_2(\alpha) \ldots \sigma_n(\alpha)$$
$$Tr_{K/k}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha).$$

COROLLAIRE *2. -Pour toute extension finie de degré n du corps des nombres rationnels, il existe exactement n isomorphismes dans le corps des nombres complexes.*

Soit $\omega_1, \ldots \omega_n$ une base de K/k. Puisque

$$\mathrm{Tr}\,(\omega_i\omega_j) = \sum_{s=1}^{n} \sigma_s(\omega_i)\sigma_s(\omega_j),$$

la matrice (Tr $(\omega_i\omega_j)$) est égale au produit des matrices $(\sigma_i(\omega_j))$ $(\sigma_i(\omega_j))$ (le prime signifie la transposition) et par suite on a la formule suivante :

$$D(\omega_1, \ldots \omega_n) = (\det\,(\sigma_i(\omega_j)))^2. \qquad (15)$$

EXERCICES

1. Soit Ω = k(x) le corps des fonctions rationnelles en x à coefficients dans le corps k. Démontrer que tout élément de Ω qui n'appartient pas à k est transcendant sur k.

2. Soit $k \subset K \subset L$ une chaîne d'extensions finies. Pour tout $\theta \in L$, établir la formule

$$N_{K/k}(N_{L/K}(\theta)) = N_{L/k}(\theta)$$

(Supposer tout d'abord que L = $K(\theta)$ et prendre comme base de l'extension L/k la base $\omega_i\theta^j$, où ω_i est une base de K/k).

3. Trouver un élément primitif pour l'extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ du corps Q des nombres rationnels et l'exprimer avec les nombres $\sqrt{2}$ et $\sqrt{3}$.

4. Démontrer qu'une extension finie K/k est monogène si et seulement si pour cette extension il n'existe qu'un nombre fini de corps conjugués.

5. Soit k un corps quelconque de caractéristique $p \neq 0$. Démontrer que le polynôme f(t) = $t^p - t - a$ $(a \in k)$ ou bien se décompose en un produit de facteurs linéaires dans le corps k ou bien est irréductible. Montrer de plus que, dans le deuxième cas, l'extension $k(\theta)/k$, où $f(\theta) = 0$, est séparable.

6. Soient k_0 un corps de Caractéristique~ $\neq 0$ et $k = k_0(x)$ le corps des fonctions rationnelles en x à coefficients dans k_0. Montrer que le polynôme $f(t) = t^p - x$ est irréductible dans l'anneau $k[t]$. Démontrer de plus que l'extension $k(\theta)/k$, où f(0) = 0, n'est pas séparable.

7. Démontrer que si, pour une extension finie K/k de degré n, il existe n isomorphismes distincts dans une extension Ω/k, laissant invariants les éléments de k, alors l'extension K/k est séparable.

8. Soit k un corps quelconque de caractéristique $\neq p$ contenant une racine primitive d'ordre p de 1. Démontrer que si un élément $a \in k$ n'est pas égal à la puissance $p^{\text{ième}}$ d'un élément de k, alors :

$$(k(\sqrt[p]{\alpha}) : k) = p.$$

9. Soient K/k une extension finie séparable et φ une forme linéaire sur l'espace vectoriel K sur le corps k. Démontrer qu'il existe dans le corps K un élément a tel que

$$\varphi(\xi) = \mathrm{Tr}_{K/k}(\alpha\xi), \qquad \xi \in K,$$

§ 3. — CORPS FINIS

Un corps Σ est dit *fini* s'il ne contient qu'un nombre fini d'éléments. Un exemple de corps fini est le corps $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ des classes résiduelles modulo un nombre premier p dans l'anneau $\mathbf{Z}$ des entiers rationnels. Tous ces corps ont une caractéristique qui est un nombre premier et si la caractéristique d'un corps fini Σ est égale à p, alors ce corps contient un sous-corps premier (n'admettant pas de sous-corps propre), qui est isomorphe au corps $\mathbf{F}_p$. C'est pourquoi on peut considérer que $\mathbf{F}_p \subset \Sigma$. L'extension $\Sigma/\mathbf{F}_p$ est finie; si son degré est égal à m et si $\omega_1, \ldots, \omega_m$ est une base de Σ sur $\mathbf{F}_p$, tout élément $\xi \in \Sigma$ s'écrit de manière unique $\xi = c_1\omega_1 + \ldots + c_m\omega_m$, où les c_i parcourent, indépendamment l'un de l'autre les p éléments de $\mathbf{F}_p$. Puisque le nombre de ces combinaisons linéaires est égal à p^m, cela démontre que ***le nombre d'éléments d'un corps fini est égal à une puissance de sa caractéristique.***

Le groupe multiplicatif Σ^* du corps fini Σ est un groupe abélien fini. Précisons sa structure.

LEMME. — ***Tout sous-groupe G du groupe multiplicatif*** K^* ***d'un corps fini*** K ***est cyclique.***

DÉMONSTRATION. — Montrons tout d'abord que si, dans un groupe abélien G, il existe des éléments d'ordres m et n, alors il existe également dans G un élément dont l'ordre est égal au plus petit commun multiple k des nombres m et n. Supposons que les éléments x et y de G sont d'ordres respectifs m et n. Si $(m, n) = 1$, le produit xy est d'ordre $k = mn$. Dans le cas général, utilisons les décompositions canoniques des nombres m et n comme produit de puissances de nombres premiers; nous pouvons les écrire sous la forme

$$m = m_0m_1, \qquad n = n_0n_1$$

tels que $(m_1, n_0) = 1$ et $k = m_0n_0$. Les éléments x^{m_1} et y^{n_1} sont d'ordres respectifs m_0 et n_0 et leur produit $x^{m_1}y^{n_1}$ est d'ordre $k = n_0m_0$.

Soit maintenant un sous-groupe fini d'ordre g du groupe multiplicatif

du corps K. Si m est le plus grand des ordres des éléments du groupe G, il est clair que $m \leqslant g$. D'autre part, d'après ce qui précède, l'ordre de tout élément de G divise m, i. e. tous les éléments du groupe G sont des racines du polynôme $t^m - 1$. Mais, dans un corps, un polynôme de degré m ne peut avoir plus de m racines, d'où $g \leqslant m$. Ainsi $g = m$ et cela signifie que le groupe G est cyclique.

Appliquant le lemme ci-dessus au cas d'un corps fini, nous obtenons :

THÉORÈME 1. — ***Le groupe multiplicatif d'un corps fini à p^m éléments est un groupe cyclique d'ordre $p^m - 1$.***

COROLLAIRE. — ***Toute extension finie d'un corps fini est monogène.***

En effet, si θ est un élément du groupe Σ^*, alors il est évident que $\mathbf{F}_p(\theta) = \Sigma$. Pour tout corps intermédiaire Σ_0, on a donc $\Sigma_0(\theta) = \Sigma$.

Du théorème 1 découle aussi que tous les éléments de Σ sont les racines du polynôme $t^{p^m} - t$ et puisque le degré de ce polynôme est égal au nombre d'éléments de Σ on a dans l'anneau $\Sigma[t]$ la décomposition

$$t^{p^m} - t = \prod_{\xi \in \Sigma} (t - \xi)$$

(ξ parcourt tous les éléments du corps C).

THÉORÈME 2. — ***Pour tout entier premier p et pour tout entier naturel m, il existe un corps fini et un seul à isomorphisme près, contenant p^m éléments.***

DÉMONSTRATION. — D'après le corollaire du théorème 5, § 2, il existe une extension $\Omega/\mathbf{F}_p$ dans laquelle le polynôme $t^{p^m} - t$ se décompose en facteurs linéaires. Désignons par Σ l'ensemble de toutes ces racines (contenues dans Ω). Puisque dans tout corps de caractéristique p, on a la formule

$$(x \pm y)^{p^m} = x^{p^m} \pm y^{p^m},$$

la somme et la différence de deux éléments de Y sont encore des éléments de Σ. L'ensemble Σ est fermé aussi par rapport aux opérations de multiplication et de division (par un diviseur non nul). Par suite Σ est un sous-corps du corps Ω. Le polynôme $t^{p^m} - t$ n'a pas de racines multiples (puisque sa dérivée $p^m t^{p^m - 1} - 1 = -1$ n'est nulle pour aucune valeur de t); ainsi Σ contient p^m élément. Ceci démontre l'existence d'un corps fini à p^m éléments.

Soient maintenant Σ et Σ' deux extensions de degré m de $\mathbf{F}_p$. Choisissons dans Σ un élément primitif θ (corollaire du théorème 1) et désignons par $\varphi(t)$ son polynôme minimal. Puisque $\varphi(t)$ est un diviseur du polynôme $t^{p^m} - t$ et que ce dernier est décomposable dans Σ' en facteurs linéaires, alors $\varphi(t)$ a une racine $\theta' \in \Sigma'$. L'extension $\mathbf{F}_p(\theta')/\mathbf{F}_p$ est de degré égal au degré du

polynôme $\varphi(t)$, i. e. m; par suite, $\mathbf{F}_p(\theta') = Y$. L'existence de l'isomorphisme des corps Σ et Σ' résulte alors du théorème 4, § 2.

On désigne habituellement par $GF(p^m)$ ou $\mathbf{F}_{p^m}$ le corps fini à p^m éléments (appelé corps de Galois).

COROLLAIRE. — *Sur tout corps fini* $\Sigma_0 = GF(p^r)$, *il existe des polynômes irréductibles de degré n quelconque.*

En effet, $p^r - 1$ est un diviseur de $p^{rn} - 1$ et par suite toutes les racines du polynôme $t^{p^r} - t$ dans le corps $\Sigma = GF(p^{rn})$ constituent un sous-corps isomorphe au corps Σ_0. Nous pouvons donc considérer que $\Sigma_0 \subset \Sigma$. Le polynôme minimal d'un élément primitif quelconque $\theta \in \Sigma$ par rapport à Σ_0 est un polynôme irréductible de l'anneau $\Sigma_0[t]$, de degré n puisque

$$(\Sigma : \Sigma_0) = \frac{(\Sigma : \mathbf{F}_p)}{(\Sigma_0 : \mathbf{F}_p)} = \frac{rn}{r} = n.$$

Remarquons pour terminer que pour qu'un anneau commutatif fini soit un corps, il suffit qu'il n'ait pas de diviseur de zéro. En effet, soit $\mathfrak{D}$ un anneau commutatif fini sans diviseurs de zéro et soit a un élément différent de zéro de $\mathfrak{D}$. Si $ax_1 = ax_2$, alors $(x_1 - x,) = 0$, d'où $x_1 = x,$; ainsi, si $x_1 \neq x_2$, les produits ax_1 et ax_2 sont aussi distincts et cela signifie le produit ax parcourt avec x tous les éléments de l'anneau $\mathfrak{D}$. Mais alors pour tout $b \neq 0$ l'équation $ax = b$ est résoluble dans $\mathfrak{D}$, i. e. tous les éléments non nuls de l'anneau $\mathfrak{D}$ constituent un groupe multiplicatif.

EXERCICES

1. Montrer que le nombre r(m) de polynômes irréductibles de degré m distincts de l'anneau $\mathbf{F}_p[t]$ de coefficients dominants égaux à 1 s'exprime par la formule

$$r(m) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) p^d$$

(d parcourt tous les diviseurs du nombre m et $\mu(k)$ désigne la fonction de Moëbius).

2. Trouver tous les polynômes irréductibles de degré 2 sur le corps $\mathbf{F}_5 = GF(5)$.

3. Montrer que le corps $GF(p^m)$ est contenu dans le corps $GF(p^n)$ (au sens d'un plongement isomorphe) si et seulement si $m|n$.

4. Quel est le degré sur $\mathbf{F}_p$ du corps de décomposition du polynôme $t^n - 1$?

5. Soit $\Sigma = GF(p^m)$. Montrer que les applications

$$\sigma_i : \xi \to \xi^{p^i}, \qquad \xi \in \Sigma \qquad (i = 0, 1, \ldots m-1)$$

sont des automorphismes deux à deux distincts du corps Σ et que tout automorphisme de Σ coïncide avec un des σ_i.

6. Soient $\Sigma_0 = GF(p^r)$ et Σ une extension finie de degré n de Σ_0. Démontrer que les applications $\xi \to \xi^{p^{ri}}$, $\xi \in \Sigma$ ($i = 0, 1, \ldots, n-1$), constituent un système complet de n automorphismes deux à deux distincts de Σ laissant invariant les éléments de Σ_0. Montrer que le polynôme caractéristique $f_\xi(t)$ d'un élément $\xi \in \Sigma$ pour l'extension Σ/Σ_0 admet dans le corps Σ la décomposition

$$f_\xi(t) = (t - \xi)(t - \xi^q) \ldots \left(t - \xi^{q^{n-1}}\right)$$

où $q = p^r$ (utiliser le théorème 8 du § 2). En déduire que

$$\mathrm{Tr}_{\Sigma/\Sigma_0}(\xi) = \xi + \xi^q + \ldots + \xi^{q^{n-1}}, \quad \mathrm{N}_{\Sigma/\Sigma_0}(\xi) = \xi^{1+q+\ldots+q^{n-1}}.$$

7. Démontrer que toute extension finie d'un corps fini est séparable.

8. Avec les notations de l'exercice 6, démontrer que tout élément du corps Σ_0 est la norme d'un certain élément de Σ.

9. Soient $\Sigma = GF(p^{mr})$, $p^m = q$, $\alpha \in \Sigma$. Démontrer que l'équation $\xi^q - \xi = a$ est résoluble dans le corps Σ si et seulement si $a + \alpha^q + \ldots + \alpha^{q^{r-1}} = 0$.

10. Soit ε une racine primitive de 1 d'ordre premier p. Puisque les éléments du sous-corps premier $\Sigma_0 = GF(p)$ du corps $\Sigma = GF(p^m)$ sont des classes résiduelles de l'anneau des nombres entiers rationnels modulo p, la puissance $\varepsilon^{\mathrm{Tr}\, y}$ a un sens pour tout $y \in \Sigma$ (la trace est considérée dans l'extension Σ/Σ_0). Démontrer que

$$\sum_{\xi \in \Sigma} \varepsilon^{\mathrm{Tr}\, \xi\alpha} = \begin{cases} 0 & \text{si} \quad \alpha \neq 0, \\ p^m & \text{si} \quad a = 0. \end{cases}$$

11. Soient χ un caractère du groupe multiplicatif du corps $\Sigma = GF(p^m)$, $p^m = q$ (pour la définition des caractères, cf. § 5). Prolongeons χ à tout le corps Σ en posant $\chi(0) = 0$. L'expression

$$\tau_\alpha(\chi) = \sum_{\xi \in \Sigma} \chi(\xi) \varepsilon^{\mathrm{Tr}\, \alpha\xi} \qquad (\alpha \in \Sigma),$$

qui est un nombre complexe, est appelé une somme de Gauss du corps fini Σ. Supposant que le caractère χ est différent du caractère unité χ_0, démontrer les formules

$$\tau_\alpha(\chi) = \chi(\alpha)^{-1} \tau_1(\chi), \qquad \alpha \neq 0 ;$$

$$| \tau_\alpha(\chi) | = \sqrt{q}, \qquad \alpha \neq 0 ;$$

$$\sum_{\alpha \neq 0} \tau_\alpha(\chi) = 0.$$

12. Soit $p \neq 2$. Puisque tous les carrés du groupe multiplicatif Σ^* du corps $\Sigma = GF(p^m)$ forment un sous-groupe d'indice 2, alors, posant $\psi(\alpha) = +1$ si $a \neq 0$ est un carré et $\psi(\alpha) = -1$ dans le cas contraire nous obtenons un caractère ψ du groupe Σ^*. Démontrer, pour $\alpha\beta \neq 0$,

$$\tau_\alpha(\psi)\, \tau_\beta(\psi) = \psi(-\alpha\beta) p^m.$$

13. Démontrer, pour $a \neq 0$, la relation

$$\sum_{\xi \in \Sigma} \psi(\xi^2 - a) = -1.$$

14. Soit $f(x_1, \ldots, x_n)$ une forme quadratique non singulière, de déterminant δ, à coefficients dans $\Sigma = GF(p^m)$, $p^m = q$, $p \neq 2$ et soit a un élément quelconque de Σ. Démontrer que le nombre N de solutions dans Σ de l'équation

$$f(x_1, \ldots, x_n) = \alpha$$

s'exprime par les formules

$$N = q^{2r} + q^r \psi((-1)^r \alpha\delta), \qquad \text{si} \quad n = 2r + 1,$$

$$N = q^{2r-1} + \omega q^{r-1} \psi((-1)^r \delta), \quad \text{si} \quad n = 2r,$$

avec $\omega = -1$ pour $a \neq 0$ et $\omega = q - 1$ pour $a = 0$.

15. Soient p et q des nombres rationnels premiers impairs distincts. Nous désignerons par la même lettre x les classes résiduelles d'un entier x dans les corps $GF(p)$ et GF(q). Choisissons une extension A du corps GF(q) dans laquelle le polynôme $t^p - 1$ se décompose en facteurs linéaires et désignons par ε une racine primitive d'ordre p de 1 appartenant à A. Le symbole de Legendre $\left(\frac{x}{p}\right)$ coïncide, c'est clair, avec le caractère $\psi(x)$ du corps $GF(p)$ introduit dans l'exercice 12. Puisque ses valeurs sont ± 1, on peut considérer que $\left(\frac{x}{p}\right) \in A$. Démontrer que la « somme de Gauss »

$$\tau = \sum_{x \in GF(p)} \left(\frac{x}{p}\right) \varepsilon^x \in A$$

du corps $GF(p)$ vérifie les égalités :

$$\tau^2 = (-1)^{\frac{p-1}{2}} p, \tag{1}$$

$$\tau^q = \left(\frac{q}{p}\right)\tau. \tag{2}$$

16. Utilisant la valeur $\left(\frac{q}{p}\right) = p^{\frac{q-1}{2}}$ du symbole de Legendre dans le corps $GF(q)$, déduire des formules (1) et (2) la loi de réciprocité de Gauss :

$$(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

§ 4. — NOTIONS SUR LES ANNEAUX COMMUTATIFS

Dans ce paragraphe, nous entendrons par anneau un anneau commutatif avec élément unité 1 et sans diviseurs de zéro.

1) Divisibilité dans les anneaux

Soit $\mathfrak{D}$ un anneau. Si pour des éléments a et $\beta \neq 0$ de $\mathfrak{D}$ il existe un élément $\xi \in \mathfrak{D}$ tel que $\beta\xi = a$, on dit que a est divisible par β (ou que β divise a) et on écrit $\beta \mid a$. Puisque $\mathfrak{D}$ n'a pas de diviseurs de zéro, l'égalité $\beta\xi = a$

définit de manière unique l'élément ξ. La notion de divisibilité dans un anneau quelconque possède, c'est clair, les propriétés de la divisibilité pour les entiers rationnels. Par exemple, si γ/β et β/α, alors γ/α.

Un élément $\varepsilon \in \mathfrak{D}$ qui est un diviseur de l'élément 1 s'appelle une unité de l'anneau $\mathfrak{D}$ (ou élément inversible).

THÉORÈME 1. — ***Les unités d'un anneau $\mathfrak{D}$ constituent un groupe multiplicatif.***

DÉMONSTRATION. — Soit E l'ensemble de toutes les unités de l'anneau $\mathfrak{D}$. Si $\varepsilon \in$ E et $\eta \in$ E, alors $\varepsilon\varepsilon' = 1$ et $\eta\eta' = 1$ pour $\varepsilon', \eta' \in \mathfrak{D}$; mais alors

$$(\varepsilon\eta)\,(\varepsilon'\eta') = 1$$

et par suite $\varepsilon\eta \in$ E. Puisque $1 \in$ E et que pour toute unité ε il existe un élément ε' défini par l'égalité $\varepsilon\varepsilon' = 1$, alors $\varepsilon' \in$ E et E est donc un groupe.

Des éléments $a \neq 0$ et $\beta \neq 0$ de l'anneau $\mathfrak{D}$ sont dits ***associés*** s'ils sont divisibles l'un par l'autre. Des égalités $a = \beta\xi$ et $\beta = \alpha\eta (\xi, \eta \in \mathfrak{D})$, il résulte que $a = \alpha\xi\eta$, d'où $1 = \xi\eta$ (puisque $a \neq 0$ et qu'il n'y a pas de diviseurs de zéro dans l'anneau). Ainsi, dire que deux éléments non nuls sont associés signifie qu'ils diffèrent l'un de l'autre par un facteur qui est une unité de $\mathfrak{D}$.

Soit $\mu \neq 0$ un élément de l'anneau $\mathfrak{D}$ qui n'est pas une unité. On dit que deux éléments a et β de $\mathfrak{D}$ sont congrus modulo μ et on écrit $a \equiv \beta \pmod{\mu}$, si la différence $\alpha - \beta$ est divisible par μ. Cette notion de congruence vérifie les propriétés habituelles des congruences dans l'anneau des nombres entiers. Pour tout $a \in \mathfrak{D}$, on désigne par $\bar{\alpha}$ l'ensemble de tous les éléments de $\mathfrak{D}$ congrus à a modulo μ. L'ensemble $\bar{\alpha}$ est appelé une classe résiduelle modulo μ. L'égalité $\bar{\alpha} = \bar{\beta}$ est satisfaite, c'est clair, si et seulement si $a \equiv \beta \pmod{\mu}$. On peut définir la somme et le produit de deux classes dans l'ensemble des classes résiduelles modulo μ en posant

$$\bar{\alpha} + \bar{\beta} = \overline{\alpha + \beta}, \qquad \alpha\beta = \alpha\beta.$$

Puisque la relation de congruence est compatible avec l'addition et la multiplication de l'anneau $\mathfrak{D}$, la somme et le produit des classes ainsi définis ne dépendent pas du choix des représentants α et β. Une simple vérification montre que l'ensemble de toutes les classes résiduelles modulo μ constitue un anneau commutatif pour les opérations ci-dessus, à élément unité 1 (c'est vrai même s'il y a des diviseurs de zéro). Cet anneau s'appelle l'anneau des classes résiduelles modulo μ.

Si dans chaque classe résiduelle modulo μ on choisit un représentant, l'ensemble S de ces éléments s'appelle un ***système complet de résidus***

modulo μ. Un système complet de résidus S est donc caractérisé par le fait que tout élément de l'anneau $\mathfrak{D}$ est congru modulo μ à un élément de S et un seul.

2) Idéaux

Un sous-ensemble A d'un anneau $\mathfrak{D}$ s'appelle un idéal si c'est un sous-groupe du groupe additif de l'anneau $\mathfrak{D}$ et si pour tout $a \in A$ et tout $\xi \in \mathfrak{D}$, le produit $\xi\alpha$ appartient à A. L'ensemble réduit à l'élément zéro et l'anneau $\mathfrak{D}$ tout entier constituent des exemples triviaux d'idéaux (appelés respectivement idéal nul et idéal unité).

Soient $\alpha_1, \ldots, a,$ des éléments quelconques de l'anneau $\mathfrak{D}$. II est évident que l'ensemble A de toutes les combinaisons linéaires

$$\xi_1\alpha_1 + \xi_2\alpha_2 + \ldots + \xi_m\alpha_m$$

de ces éléments à coefficients $\xi_i \in \mathfrak{D}$ est un idéal de l'anneau $\mathfrak{D}$, appelé idéal engendré par les éléments $\alpha_1, \ldots, \alpha_m$ et désigné par $A = (\alpha_1, \ldots, \alpha_m)$. Les éléments $\alpha_1, \ldots, a,$ sont appelés des générateurs de l'idéal A. Dans le cas général, il n'existe pas pour tout idéal de système fini de générateurs. Un idéal A est dit ***principal*** s'il admet un système de générateurs formé d'un seul élément, i. e. s'il est de la forme A = (a). Il est clair que tout idéal principal non nul (a) est égal à l'ensemble des éléments de l'anneau $\mathfrak{D}$ qui sont divisibles par a. Les idéaux nul et unité sont principaux : l'idéal nul est engendré par 0 et l'idéal unité par une unité quelconque ε de l'anneau $\mathfrak{D}$. Deux idéaux principaux (α) et (β) coïncident si et seulement si a et β sont associés.

Soient A et B deux idéaux d'un anneau $\mathfrak{D}$. L'ensemble de tous les éléments $\xi \in \mathfrak{D}$ de la forme

$$\xi \equiv \alpha_1\beta_1 + \ldots + \alpha_s\beta_s$$

où $\alpha_i \in A$, $\beta_i \in B$ $(s \geqslant 1)$ est encore un idéal dans $\mathfrak{D}$, que nous appellerons l'idéal produit des idéaux A et B; il sera désigné par AB. Puisque la multiplication des idéaux est commutative et associative, les idéaux de l'anneau $\mathfrak{D}$ (commutatif) constituent un monoïde pour cette opération.

Deux éléments a et β de $\mathfrak{D}$ sont dits congrus modulo un idéal A et on note $a \equiv \beta \pmod{A}$, si la différence $a - \beta$ appartient à A, i. e. si a et β appartiennent à la même classe résiduelle relative au sous-groupe additif A. Il est clair que la congruence $a \equiv \beta \pmod{A}$ est satisfaite si et seulement si $\bar{\alpha} = \bar{\beta}$, en désignant par $\bar{\gamma}$ la classe résiduelle relative au sous-groupe A qui contient $\gamma \in \mathfrak{D}$. La relation de congruence modulo un idéal, dans le cas d'un idéal principal (μ) coïncide avec la congruence modulo l'élément μ (cf. 1)). Considérons le groupe $\mathfrak{D}/A$ quotient du groupe additif de l'anneau $\mathfrak{D}$

par le sous-groupe **A.** Dans le cas où A est un idéal, on peut définir une multiplication dans le groupe quotient $\mathfrak{D}/\mathbf{A}$: pour $\bar{\alpha}$ et $\bar{\beta}$ dans $\mathfrak{D}/\mathbf{A}$, posons

$$\alpha\beta = \alpha\beta.$$

Si $\bar{\alpha} = \alpha_1$ et $\bar{\beta} = \bar{\beta_1}$, alors, d'après l'égalité

$$\alpha_1\beta_1 - \alpha\beta = \alpha_1(\beta_1 - \beta) + \beta(\alpha_1 - \alpha)$$

et puisque $\alpha_1 - a$ et $\beta_1 - \beta$ appartiennent à A, on a $\alpha_1\beta_1 \equiv \alpha\beta \pmod{A}$ (ici le fait que A soit un idéal est essentiel) et cela signifie que le produit $\bar{\alpha},\bar{\beta}$ ne dépend pas du choix des représentants a et β. Il est facile de vérifier que le groupe quotient $\mathfrak{D}/\mathbf{A}$ est un anneau pour cette multiplication et pour l'addition $\bar{\alpha} + \bar{\beta} = a + \beta$. L'anneau $\mathfrak{D}/\mathbf{A}$ est appelé anneau quotient de l'anneau $\mathfrak{D}$ par l'idéal A. Dans le cas d'un idéal principal (μ), l'anneau quotient $\mathfrak{D}/(\mu)$ n'est autre que l'anneau des classes résiduelles modulo μ.

3) Éléments entiers

Tout anneau $\mathfrak{U}$ (commutatif et sans diviseurs de zéro) peut être plongé dans un corps. Pour montrer ce résultat, considérons l'ensemble de toutes les fractions formelles $\frac{a}{b}$, où a et b sont des éléments de 'U et $b \neq 0$. Deux fractions $\frac{a}{b}$ et $\frac{c}{d}$ seront dites égales si et seulement si $ad = bc$. Définissons l'addition et la multiplication par les formules

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Il est facile de vérifier que ces opérations sont compatibles avec l'égalité et que l'ensemble de toutes les fractions considérées est ainsi muni d'une structure de corps; désignons ce corps par k_0. Si nous identifions les fractions $\frac{a}{1} = \frac{ac}{c}$, $c \neq 0$ à l'élément a $\in$ 'U, alors $\mathfrak{U}$ est un sous-anneau du corps k_0. Tout élément de k_0 est alors le quotient de deux éléments de 'U.

Soit maintenant Ω un corps quelconque contenant $\mathfrak{U}$ comme sous-anneau. L'ensemble k de tous les quotients $\frac{a}{b}$, où a, $b \in \mathfrak{U}$ $(b \neq 0)$ est un sous-corps du corps Ω. Ce sous-corps est appelé corps des fractions de

l'anneau $\mathfrak{U}$ (il est facile de voir que le corps k est isomorphe au corps k_0 construit ci-dessus et qu'il est défini par l'anneau $\mathfrak{U}$ de manière unique (à un isomorphisme près).

DÉFINITION. — *Soit un anneau $\mathfrak{U}$ contenu dans un corps Ω. Un élément $\alpha \in \Omega$ est dit entier sur $\mathfrak{U}$ si c'est une racine d'un polynôme à coefficients dans $\mathfrak{U}$ et dont le coefficient dominant est égal à 1.*

Puisque tout élément $a \in \mathfrak{U}$ est racine du polynôme $t - a$, alors tout élément de $\mathfrak{U}$ est entier sur 'U.

Soient $\omega_1, \ldots, \omega_m$ des éléments quelconques de Ω. L'ensemble M de toutes les combinaisons linéaires $a_1\omega_1 + \ldots + a_m\omega_m$ à coefficients $a_i \in \mathfrak{U}$ est appelé un 'U-module de type fini dans Ω et les éléments $\omega_1, \ldots, \omega_m$ sont appelés des générateurs du 'XL-module M. Puisque $1 \in \mathfrak{U}$, tous les ω_i appartiennent à M.

LEMME 1. — *Si un '-U-module de type fini* M *est un anneau, alors tous ses éléments sont entiers sur $\mathfrak{U}$.*

DÉMONSTRATION. — Nous pouvons bien entendu supposer qu'aucun des ω_i n'est nul. Soit a un élément quelconque de M. Puisque pour tout i le produit $\alpha\omega_i$ appartient à M, alors

$$\alpha\omega_i = \sum_{j=1}^{m} a_{ij}\omega_j, \qquad a_{ij} \in \mathfrak{U}, \qquad (i = 1, \ldots, m).$$

Il en résulte que $\det(\alpha E - (a_{ij})) = 0$ (E est la matrice unité d'ordre n). Ainsi l'élément a est racine du polynôme $f(t) = \det(tE - (a_{ij}))$ *à coefficients* dans $\mathfrak{U}$ et dont le coefficient dominant est 1. Cela démontre le lemme.

THÉORÈME 2. — *L'ensemble $\mathfrak{D}$ de tous les éléments de Ω entiers sur $\mathfrak{U}$ est un anneau.*

DÉMONSTRATION. — Il faut montrer que la somme, la différence et le produit de deux éléments entiers α et β de Ω sont aussi des éléments entiers. Si a et β sont respectivement des racines des polynômes

$$t^m - a_m t^{m-1} - \ldots - a_, \qquad t^n - b_n t^{n-1} - \ldots - b_1 ;$$

où a et $b_j \in \mathfrak{U}$, alors

$$\alpha^m = a, + a_2\alpha + \ldots + a_m\alpha^{m-1}, \qquad \beta^n = b_1 + b_1\beta + \ldots + b_n\beta^{n-1}.$$

Il en résulte facilement que le 'U-module constitué par toutes les combinaisons linéaires des produits

$$\alpha^i\beta \qquad (0 \leqslant i \leqslant m,\ 0 \leqslant j < m) \tag{1}$$

à coefficients dans $\mathfrak{U}$, est un anneau (puisque les produits $\alpha^k\beta^l$ pour $k \geqslant 0$ et $l \geqslant 0$ s'écrivent comme des combinaisons linéaires des éléments (1) à coefficients dans 'U). D'après le lemme 1, tous les éléments de cet anneau sont donc entiers sur $\mathfrak{U}$; en particulier, $\alpha \pm \beta$ et $\alpha\beta$ sont entiers. Le théorème 2 est démontré.

DÉFINITION. — ***Soit $\mathfrak{U}$ un sous-anneau d'un corps Ω. L'ensemble $\mathfrak{D}$ de tous les éléments de Ω entiers sur $\mathfrak{U}$ s'appelle la fermeture intégrale de l'anneau $\mathfrak{U}$ dans le corps Ω.***

DÉFINITION. — ***Un sous-anneau $\mathfrak{D}_0$ d'un corps K est dit intégralement fermé dans K si sa fermeture intégrale dans K coïncide avec $\mathfrak{D}_0$.***

On dit simplement que l'anneau $\mathfrak{U}$ est ***intégralement*** clos s'il est intégralement fermé dans son corps des fractions.

THÉORÈME *3.* — ***Soit $\mathfrak{U}$ un sous-anneau d'un corps Ω. La fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{U}$ dans le corps est intégralement fermée dans Ω.***

DÉMONSTRATION. — Soit θ un élément quelconque de Ω entier sur $\mathfrak{D}$ donc tel que

$$\theta^n = \alpha_1 + \alpha_2\theta + \ldots + \alpha_n\theta^{n-1}, \tag{2}$$

où tous les α_i appartiennent à $\mathfrak{D}$. Il faut démontrer que $\theta \in \mathfrak{D}$. Pour tout $i = 1, \ldots, n$, il existe un entier m tel que l'on ait l'égalité

$$\alpha^{m_i} = \sum_{j=1}^{m_i} a_{ij}\alpha_i^{j-1}, \qquad a_{ij} \in \mathfrak{U} \tag{3}$$

(puisque α_i est entier sur $\mathfrak{U}$). Considérons le 'U-module M engendré par les produits

$$\alpha_1^{k_1} \ldots \alpha_n^{k_n}\theta^k \qquad (0 \leqslant k_i < m_i, \quad 0 \leqslant k < n). \tag{4}$$

Il résulte facilement de (2) et (3) que tout produit $\alpha_1^{l_1} \ldots \alpha_n^{l_n}\theta^l$ avec des exposants positifs s'exprime comme combinaison linéaire des éléments (4) à coefficients dans $\mathfrak{U}$ et cela signifie que le module M est un anneau. D'après le lemme 1, tous les éléments de M sont donc entiers sur 'U. En particulier, θ est entier, C. Q. F. D.

LEMME *2.* — ***Soit 'U un anneau intégralement clos (dans son corps des fractions k) et supposons que le coefficient dominant d'unpolynômef (t) $\in \mathfrak{U}[t]$ est égal à 1. Si le coefficient dominant d'undiviseur $q(t) \in k[t]$ du polynôme $f(t)$ est égal à 1, alors $\varphi(t) \in \mathfrak{U}[t]$.***

DÉMONSTRATION. — Considérons une extension Ω/k du corps k dans laquelle f(t) se décompose en facteurs linéaires (corollaire du théorème 5, § 2). Toutes les racines de f(t) appartiennent à la fermeture intégrale $\mathfrak{D}$ de l'anneau $\mathfrak{U}$ dans le corps Ω. En particulier, toutes les racines de $\varphi(t)$ appartiennent à l'anneau $\mathfrak{D}$. Mais il résulte de la décomposition

$$\varphi(t) = (t - \gamma_1) \ldots (t - \gamma_s)$$

que tous les coefficients de $\varphi(t)$ appartiennent à $\mathfrak{D}$ et puisque $\mathfrak{D} \cap k = \mathfrak{U}$ (puisque $\mathfrak{U}$ est intégralement clos), ces coefficients appartiennent à $\mathfrak{U}$. C. Q. F. D.

Du lemme 2 découle de manière évidente le théorème suivant.

THÉORÈME *4. — Soit $\mathfrak{U}$ un anneau intégralement clos (dans son corps des fractions) et soit Ω/k une extension algébrique du corps k. Pour qu'un élément $\alpha \in \Omega$ soit entier sur $\mathfrak{U}$, il faut et il suffit que tous les coefficients de son polynôme minimal appartiennent à $\mathfrak{U}$.*

EXERCICES

1. Un idéal A d'un anneau $\mathfrak{D}$ est dit maximal si $A \neq \mathfrak{D}$ et si tout idéal B contenant A (i. e. tel que $A \subset B \subset \mathfrak{D}$) coïncide soit avec A soit avec $\mathfrak{D}$. Démontrer qu'un idéal A est maximal si et seulement l'anneau quotient $\mathfrak{D}/A$ est un corps.

2. Démontrer que si un anneau $\mathfrak{O}$ est intégralement clos, alors l'anneau $\mathfrak{O}[t]$ des polynômes à coefficients dans $\mathfrak{O}$ est aussi intégralement clos.

§ 5. — CARACTÈRES

Dans ce paragraphe, nous exposerons quelques notions relatives aux caractères des groupes abéliens finis et aux caractères modulaires.

1) Structure des groupes abéliens finis

La structure des groupes abéliens finis quelconques est décrite par le théorème suivant (cf. par exemple M. Hall, *Theory of groups*, *New* York, The MacMillan Company, 1959).

THÉORÈME 1. — *Tout groupe abélien fini peut se représenter comme produit direct de sous-groupes cycliques.*

En accord avec les exercices 1 et 2, un groupe cyclique fini n'est pas décomposable en produit direct de sous-groupes propres si et seulement si son

ordre est une puissance d'un nombre premier. Par suite, si dans la décomposition d'un groupe abélien fini quelconque G en produit direct,

$$G = A_1 \times \ldots \times A,$$

les facteurs cycliques A_i ne sont pas décomposables, alors leurs ordres sont des puissances de nombres premiers. La décomposition du groupe G en produit direct n'est pas définie de manière unique par ses facteurs non décomposables. Cependant, l'ensemble des ordres des facteurs non décomposables A_i est défini de manière unique par le groupe G. Ces ordres, qui sont des puissances de nombres premiers, s'appellent les ***invariants*** du groupe abélien fini. Le produit de tous les invariants d'un groupe donné est égal à son ordre.

2) Caractères des groupes abéliens finis

DÉFINITION. — ***On appelle caractère d'un groupe abélien fini G tout homomorphisme de G dans le groupe multiplicatif du corps des nombres complexes.***

Autrement dit, un caractère du groupe G est une fonction χ sur G, à valeurs complexes, ne s'annulant pas, et telle que

$$\chi(xy) = \chi(x)\,\chi(y) \tag{1}$$

pour x, y ∈ G.

Puisque pour tout homomorphisme de groupe, l'élément unité a pour image l'unité, alors $\chi(1) = 1$; si l'éltment $x \in G$ est d'ordre k, alors

$$(\chi(x))^k = \chi(x^k) = 1, \tag{2}$$

i. e. $\chi(x)$ est une racine $k^{\text{ième}}$ de 1. Si m est le plus grand des ordres des éléments du groupe G, alors, d'après l'exercice 3, l'ordre de tout élément de G est un diviseur de m. Toute valeur $\chi(x)$ est donc une racine d'ordre m de 1 et par suite on peut définir les caractères comme les homomorphismes de G dans le groupe des racines $m^{\text{ièmes}}$ de 1.

Représentons le groupe G comme un produit direct de sous-groupes cycliques :

$$G = \{a_1\} \times \ldots \times \{a_s\}.$$

Puisque tout élément $x \in G$ peut s'écrire sous la forme

$$x = a_1^{k_1} \ldots a_s^{k_s}, \tag{3}$$

alors, d'après (1),

$$\chi(x) = \chi(a_1)^{k_1} \ldots \chi(a_s)^{k_s};$$

ainsi, le caractère χ est complètement déterminé par les valeurs $\chi(a_1), \ldots, \chi(a_s)$. Si a_i est d'ordre m_i, d'après (2), $\chi(a_i)$ est une racine d'ordre m_i de 1. Réciproquement, choisissons pour tout $i = 1, \ldots, s$ une racine quelconque ε_i d'ordre m_i de 1 et pour tout élément $x \in G$ représenté sous la forme (3), posons

$$\chi(x) = \varepsilon_1^{k_1} \ldots \varepsilon_s^{k_s}. \tag{4}$$

Il est facile de voir que la valeur (4) ne dépend pas du choix des exposants k_i dans la décomposition (3) (chaque exposant k est défini modulo m_i) et que la fonction χ ainsi définie sur G satisfait à la condition (1) et par suite est un caractère du groupe G. On peut choisir la racine ε_i de m_i manières et par suite nous avons $m_1 \ldots m_s$ fonctions χ distinctes du type (4). Ceci démontre le théorème suivant.

THÉORÈME 2. — *Le nombre des caractères d'un groupe abélien fini est égal à son ordre.*

Définissons la multiplication des caractères. Pour deux caractères χ et χ' du groupe G, posons

$$(\chi\chi')(x) = \chi(x)\,\chi'(x), \qquad x \in G.$$

Il est évident que la fonction $\chi\chi'$ est encore un caractère du groupe G. Le caractère χ_0 tel que $\chi_0(x) = 1$ pour tout $x \in G$ est appelé *caractère unité.* Il est clair que $\chi\chi_0 = \chi$ pour tout caractère χ. Si pour tout caractère χ du groupe G nous posons

$$\bar{\chi}(x) = \chi(x), \qquad x \in G$$

($\chi(x)$ est le nombre complexe conjugué de x(x)), alors la fonction $\bar{\chi}$ ainsi définie est un caractère du groupe G tel que $\chi\bar{\chi} = \chi_0$. Puisque la multiplication des caractères est associative, l'ensemble de tous les caractères forme un groupe pour la multiplication ci-dessus.

Soit $G = \{ a \}$ un groupe cyclique d'ordre m et soit ε une racine primitive d'ordre m de 1 fixée. Désignons par χ le caractère du groupe G tel que

$$\chi(a) = \varepsilon \qquad (\text{d'où } \chi(a^k) = \varepsilon^k).$$

Puisque $\chi^r(a) = \varepsilon^r$, les caractères $\chi_0 = \chi^m, \chi, \chi^2, \ldots, \chi^{m-1}$ sont deux à deux distincts et par suite épuisent tout le groupe des caractères du groupe G. Ainsi, nous voyons que le groupe des caractères d'un groupe cyclique fini est aussi cyclique. Dans le cas général, on peut facilement démontrer le théorème suivant : ***tout groupe abélien fini est isomorphe au groupe de ses caractères.***

Dans un groupe abélien G d'ordre n, considérons un sous-groupe H d'ordre m. Si on considère la restriction à H d'un caractère du groupe G,

il est clair que cette fonction est un caractère du groupe H; désignons-le par $\widehat{\chi}$. Il est clair que l'application $\chi \to \widehat{\chi}$ est un homomorphisme du groupe X des caractères du groupe G dans le groupe Y des caractères du sous-groupe H; soit A son noyau. Les caractères $\chi \in A$ sont caractérisés par le fait que $\chi(z) = 1$ pour tout $z \in H$. Si $\chi \in A$ et x, x' appartiennent à la même classe résiduelle de G selon H, il est clair que $\chi(x) = \chi(x')$. Posant $\bar{x}(x)=x(x)$, $x \in A$ et $\bar{x}$ classe résiduelle de x dans G selon H, nous avons une fonction $\bar{\chi}$ sur le groupe quotient G/H et cette fonction est un caractère du groupe G/H. Réciproquement, si ξ est un caractère quelconque du groupe quotient G/H, posant

$$\chi(x) = \psi(\bar{x}), \qquad x \in G,$$

nous obtenons un caractère $\chi \in A$ tel que $\bar{\chi} = \psi$. Puisque par l'application $\chi \to \bar{\chi}$ ($\chi \in A$), à des caractères distincts de A correspondent des caractères distincts du groupe G/H, nous avons établi que le nombre de caractères χ de A est égal au nombre de caractères du groupe G/H, i. e. égal à $\frac{n}{m}$ (théorème 2). Mais, dans ce cas, l'image du groupe X par l'homomorphisme $\chi \to \widehat{\chi}$ (du groupe X dans le groupe Y) est d'ordre $n : \frac{n}{m} = m$ et puisque, d'après le théorème 2, le groupe Y est aussi d'ordre m, alors cette image est égale à Y. Cela signifie que tout caractère du groupe H est de la forme $\widehat{\chi}$ pour un certain caractère χ du groupe G. Il est clair que le nombre des caractères $\chi \in X$ qui induisent le même caractère sur H est égal à $\frac{m}{n} = (G : H)$. Ceci démontre le théorème suivant :

THÉORÈME *3. — Soit G un groupe abélien fini et* H *un sous-groupe. Tout caractère du groupe* H *est prolongeable en un caractère du groupe G et le nombre de ces prolongements est égal à l'indice (G :* H).

COROLLAIRE 1. — *Si x est un élément de G différent de l'unité, il existe un caractère χ du groupe G tel que $\chi(x) \neq 1$.*

En effet, considérons le groupe cyclique $\{ x \} = H$. Puisque son ordre est > 1, alors il existe un caractère χ' sur H différent du caractère unité et donc tel que $\chi'(x) \neq 1$. Prolongeant χ' en un caractère de groupe G, nous obtenons ainsi le caractère χ demandé.

COROLLAIRE *2. — Si un élément $x \in G$ n'appartient pas à un sous-groupe* H, *alors il existe un caractère χ du groupe G tel que $\chi(x) \neq 1$ et $\chi(z) = 1$ pour tout $z \in H$.*

En effet, on peut prolonger le caractère unité du groupe H en un carac-

tère différent du caractère unité du sous-groupe { x, H }, qui se prolonge à son tour en un caractère du groupe G.

Établissons maintenant quelques relations. Si χ_0 est le caractère unité, alors $\chi_0(x) = 1$ pour tout $x \in G$ et par suite $\sum_{x \in G} \chi_0(x) = n$, où n est l'ordre du groupe G. Supposons que le caractère χ est différent de χ_0, i. e. $\chi(z) \neq 1$ pour un certain $z \in G$. Si x parcourt tous les éléments du groupe G, zx parcourt aussi tous les éléments de G; posant $S = \sum_{x \in G} \chi(x)$, nous aurons donc

$$S = \sum_{x \in G} \chi(zx) = \chi(z)S.$$

Puisque $\chi(z) \neq 1$, cette égalité n'est possible que si $S = 0$. Ainsi nous avons établi la formule :

$$\sum_{x \in G} \chi(x) = \begin{cases} n & \text{si} \quad \chi = \chi_0 \\ 0 & \text{si} \quad \chi \neq \chi_0. \end{cases} \tag{5}$$

La valeur de chaque caractère sur l'élément unité du groupe est égale à 1 et par suite $\sum_{\chi} \chi(1) = n$ (χ parcourt ici tous les caractères du groupe G). Posons $T = \sum_{\chi} \chi(x)$. D'après le corollaire 1 du théorème 3, il existe un caractère χ' tel que $\chi'(x) \neq 1$ (si $x \neq 1$). Le produit $\chi'\chi$ parcourt en même temps que χ tous les caractères du groupe G, d'où

$$T = \sum_{\chi} (\chi'\chi)(x) = \sum_{\chi} \chi'(x)\, \chi(x) = \chi'(x)T,$$

et puisque $\chi'(x) \neq 1$, on a $T = 0$. On a donc établi la formule

$$\sum_{\chi} \chi(x) = \begin{cases} n & \text{si} \quad x = 1, \\ 0 & \text{si} \quad x \neq 1. \end{cases} \tag{6}$$

3) Caractères modulaires

Pour tout nombre entier naturel m, désignons par G_m le groupe multiplicatif des classes résiduelles modulo m des entiers rationnels relativement premiers avec m. Nous désignerons par $\bar{a}$ la classe résiduelle de a modulo m.

A tout caractère χ du groupe G_m, nous pouvons associer la fonction χ^* définie sur l'ensemble des nombres a premiers avec m par la formule

$$\chi^*(a) = \chi(\bar{a}).$$

Prolongeons cette fonction χ^* à l'ensemble de tous les entiers rationnels en posant $\chi^*(a) = 0$ si a et m ne sont pas premiers entre eux. La fonction χ^* ainsi définie (sur l'ensemble des entiers rationnels) est appelée un ***caractère modulaire*** modulo ***m.*** Dans la suite, nous désignerons χ^* par la même lettre χ que le caractère du groupe G_m qui l'engendre. Il est clair que des caractères distincts du groupe G_m engendrent des caractères modulaires distincts et par suite le nombre de caractères modulaires modulo m est égal à $\varphi(m)$.

De cette définition découlent facilement les propriétés suivantes des caractères modulaires :

1° pour tout entier rationnel a, la valeur $\chi(a)$ est un nombre complexe et $\chi(a) \neq 0$ si et seulement si a est relativement premier avec m;

2° si $a \equiv a'$ (mod m), alors $\chi(a) = \chi(a')$;

3° pour tout couple d'entiers rationnels a et b, on a $\chi(ab) = \chi(a)\,\chi(b)$.

Montrons que les caractères modulaires sont entièrement caractérisés par ces trois propriétés. En effet, soit η une fonction satisfaisant aux conditions 1°, 2° et 3°. Pour toute classe $\bar{a} \in G_m$, (a, m) = 1, posons $\chi(\bar{a}) = \eta(a)$; d'après 2°, la valeur $\chi(\bar{a})$ ne dépend pas du choix du représentant a et est différente de 0 d'après 1°. En outre, si (a, m) = 1 et (b, m) = 1, on a, d'après la condition 3°,

$$\chi(a\,b) = \chi(ab) = \eta(ab) = \eta(a) \quad \eta(b) = \chi(\bar{a}) \quad \chi(\bar{b}).$$

Ainsi, χ est un caractère du groupe G_m et le caractère χ^* qu'il engendre coïncide avec la fonction η.

Soit m' un entier naturel divisible par m. Nous pouvons associer à tout caractère χ modulo m un certain caractère χ' modulo m' : si a est relativement premier à m' (et par suite aussi à m), posons $\chi'(a) = \chi(a)$; si (a, m') > 1, posons $\chi'(a) = 0$. La fonction numérique χ' satisfait aux trois conditions 1°, 2° et 3° et par suite est un caractère modulaire modulo m'. Nous dirons que le caractère χ' est induit par le caractère χ.

DÉFINITION. — ***Soit χ un caractère modulaire modulo m. s'il existe un diviseur propre d du nombre m et un caractère χ_1 modulo d qui induit χ, on dit que le caractère χ est non primitif. Dans le cas contraire, il est dit primitif.***

THÉORÈME 4. — ***Pour qu'un caractère χ modulo m soit primitif, il faut et il suffit que pour tout diviseur propre d du nombre m il existe un nombre x,*** $x \equiv 1$ (mod d), (x, m) = 1 ***tel que*** $\chi(x) \neq 1$.

DÉMONSTRATION. — Si le caractère χ est non primitif, il est induit par un caractère χ_1 modulo d, où d est un diviseur propre de m. Ainsi, pour tout x relativement premier avec m, on a $\chi(x) = \chi_1(x)$; si de plus $x \equiv 1$ (mod d), alors $\chi(x) = \chi_1(x) = 1$. Réciproquement, supposons que pour un certain

diviseur propre d du nombre m on ait $\chi(x) = 1$ pour tout x tel que $x \equiv 1 \pmod{d}$ et $(x, m) = 1$. Pour tout a relativement premier à d, on peut trouver a' tel que $(a', m) = 1$ et $a' \equiv a \pmod{d}$. Posons

$$\chi_1(a) = \chi(a').$$

La valeur $\chi_1(a)$ est indépendante du choix de u'. En effet, si $a' \equiv u'' \pmod{d}$, $(a'', m) = 1$, alors $a'' \equiv xa' \pmod{m}$ pour un certain x relativement premier avec m. Puisque $x \equiv 1 \pmod{d}$, on a donc par hypothèse $\chi(x) = 1$, d'où $\chi(a'') = \chi(x)\,\chi(a') = \chi(a')$. Posant de plus $\chi_1(a) = 0$ si $(a, d) \neq 1$, nous obtenons une fonction numérique χ_1 qui est un caractère modulaire modulo d. Puisque $\chi_1(a) = \chi(a)$ pour $(a, m) = 1$, χ est induit par le caractère χ_1. Cela termine la démonstration du théorème 4.

EXERCICES

1. Montrer qu'un groupe cyclique fini dont l'ordre est une puissance d'un nombre premier n'est pas décomposable en produit direct de sous-groupes propres.

2. Supposons que l'ordre d'un groupe cyclique fini G est égal au produit de deux nombres premiers k et l. Montrons qu'on peut représenter G comme produit direct de deux sous-groupes cycliques d'ordre k et l.

3. Soit a un élément d'ordre maximum d'un groupe abélien fini G. Démontrer que le sous-groupe cyclique { a } est facteur direct dans G.

4. Soit k un entier naturel. Démontrer qu'un élément x d'un groupe abélien fini G est la puissance $k^{\text{ième}}$ d'un élément de G si et seulement si on a $\chi(x) = 0$ pour tout caractère χ du groupe G tel que $\chi^k = \chi_0$ (χ_0 est le caractère unité).

5. Soit G un groupe abélien fini d'ordre n. Numérotons ses éléments $x_1, \ldots, x_n$ et ses caractères $\chi_1, \ldots, \chi_n$. Démontrer que la matrice

$$\left(\frac{1}{n}\,\chi_i(x_j)\right)_{i,j}$$

est unitaire.

6. Soient $m_1, \ldots, m_k$ des entiers naturels premiers deux à deux et $m = m_1 \ldots m_k$. Démontrer que pour tout caractère χ modulo m il existe des caractères χ_i modulo m_i $(i = 1, \ldots, k)$, définis de manière unique, tels que pour tout entier rationnel a on ait l'égalité

$$\chi(a) = \chi_1(a) \ldots \chi_k(a).$$

(Pour tout i le caractère χ_i est défini par l'égalité $\chi_i(a) = \chi(a')$, où a' est défini par les congruences

$$a' \equiv a \pmod{m_i}, \qquad a' \equiv 1 \left(\mod \frac{m}{m_i}\right).$$

7. Sous les hypothèses de l'exercice 6, montrer que si le caractère χ modulo m est primitif, alors, pour tout $i = 1, \ldots, k$, le caractère χ_i modulo m_i est aussi primitif.

8. Soient d_1 et d_2 des diviseurs d'un nombre entier naturel m et $d = d_1 d_2$. Démontrer que si un caractère χ modulo m est induit par un certain caractère modulo d_1

et est induit par un certain caractère modulo d_2, alors il est induit aussi par un caractère modulo d.

9. Montrer que tout caractère χ modulo m est induit par un caractère primitif modulo f, défini de manière unique (f est un diviseur de m). Le nombre f est appelé le *conducteur* du caractère χ.

10. Démontrer que le nombre des caractères primitifs modulo m est égal à

$$\sum_{d|m} \mu(d)\varphi\left(\frac{m}{d}\right)$$

(d parcourt tous les diviseurs du nombre m; μ est la fonction de Moëbius; φ est la fonction d'Euler).

11. Démontrer qu'il existe des caractères primitifs modulo m si et seulement si m est soit impair soit divisible par 4.

12. Soit $\mathcal{F}$ l'espace vectoriel sur le corps des nombres complexes formé des fonctions f définies sur un groupe abélien G, à valeurs complexes $f(a)$, $\sigma \in G$. Pour tout élément $\omega \in G$, désignons par T_ω l'opérateur de translation défini par la formule $(T_\omega f)(\sigma) = f(\omega\sigma)$. Démontrer que tous les caractères χ du groupe G sont des vecteurs propres des opérateurs T_ω. Quelles sont les valeurs propres correspondantes ?

13. Conservant les notations de l'exercice précédent, considérons, pour une fonction fixée $f \in \mathcal{F}$, la matrice carrée

$$A = (f(\sigma\tau^{-1}))_{\sigma,\tau},$$

où σ et τ parcourent tous les éléments du groupe G disposés dans un certain ordre. Démontrer que le déterminant de cette matrice est égal à

$$\prod_{\chi}\left(\sum_{\sigma} f(\sigma)\chi(\sigma)\right)$$

(σ parcourt tous les éléments et χ tous les caractères du groupe G).

Indication. — La matrice A est la matrice de l'opérateur

$$T \sum_{\omega} f(\omega)T_\omega$$

par rapport à la base formée par les fonctions L_σ telles que

$$La(T) = \begin{cases} 1 & \text{pour } \sigma = \tau \\ 0 & \text{pour } \sigma \neq \tau. \end{cases}$$

Trouver les valeurs propres de l'opérateur T.

14. Démontrer la formule de l'exercice 13 en considérant le déterminant du produit de la matrice $(\chi(\sigma))_{\chi,\sigma}$ par la matrice A.

TABLES

TABLE 1

Nombre h des classes de diviseurs et unités fondamentales $\varepsilon > 1$ des corps quadratiques réels $\mathbf{Q}(\sqrt{d})$, $2 \leqslant d \leqslant 101$, d *sans* carrés, $\omega = \dfrac{1+\sqrt{d}}{2}$ pour $d \equiv 1 \pmod 4$ et $\omega = \sqrt{d}$ pour $d \equiv 2,3 \pmod 4$.

d	h	ε	$N(\varepsilon)$	d	h	ε	$N(\varepsilon)$
2	1	$1+\omega$	-1	53	1	$3+\omega$	-1
3	1	$2+\omega$	$+1$	55	2	$89+12w$	$+1$
5	1	ω	-1	57	1	$131+40\omega$	$+1$
6	1	$5+2\omega$	$+1$	58	2	$99+13\omega$	-1
7	1	$8+3\omega$	$+1$	59	1	$530+69\omega$	$+1$
10	2	$3+\omega$	-1	61	1	$17+5\omega$	-1
11	1	$10+3\omega$	$+1$	62	1	$63+8$	$+1$
13	1	$1+\omega$	-1	65		$7+2\omega$	-1
14	1	$15+4\omega$	$+1$	66	2	$65+8\omega$	$+1$
15	2	$4+\omega$	$+1$	67	1	$48\,842+5\,967\omega$	$+1$
17	1	$3+2\omega$	-1	69	1	$11+3\omega$	$+1$
19	1	$170+39\omega$	$+1$	70	2	$251+30\omega$	$+1$
21	1	$2+\omega$	$+1$	71	1	$3\,480+413\omega$	$+1$
22	1	$197+42\omega$	$+1$	73	1	$943+250\omega$	-1
23	1	$24+5\omega$	$+1$	74	2	$43+5\omega$	-1
26	2	$5+\omega$	-1	77	1	$4+\omega$	$+1$
29	1	$2+\omega$	-1	78	2	$53+6\omega$	$+1$
30	2	$11+2\omega$	$+1$	79	3	$80+9\omega$	$+1$
31	1	$1\,520+273\omega$	$+1$	82	4	$9+\omega$	-1
33	1	$19+8\omega$	$+1$	83	1	$82+9\omega$	$+1$
34	2	$35+6\omega$	$+1$	85	2	$4+\omega$	-1
35	2	$6+\omega$	$+1$	86	1	$10\,405+1\,122\omega$	$+1$
37	1	$5+2\omega$	-1	87	2	$28+3\omega$	$+1$
38	1	$37+6\omega$	$+1$	89	1	$447+106\omega$	-1
39	2	$25+4\omega$	$+1$	91	2	$1\,574+165\omega$	$+1$
41	1	$27+10\omega$	-1	93	1	$13+3\omega$	$+1$
42	2	$13+2\omega$	$+1$	94	1	$2\,143\,295+\$21\,064\omega$	$+1$
43	1	$3\,482+531\omega$	$+1$	95	2	$39+4\omega$	$+1$
46	1	$24\,335+3\,588\omega$	$+1$	97	1	$5\,035+1\,138\omega$	-1
47	1	$48+7\omega$	$+1$	101	1	$9+2\omega$	-1
51	2	$50+7\omega$	$+1$				

TABLE 2

Nombre h des classes de diviseurs et norme N(ε) de l'unité fondamentale ε des corps quadratiques réels $\mathbf{Q}(\sqrt{d})$, d sans carrés, $101 \leqslant d < 500$.

d	h	N(ε)	d	h	N(ε)	d	h	N(ε)	d	h	N(ε)
101	1	−1	181	1	−1	257	3	−1	335	2	+1
102	2	+1	182	2	+1	258	2	+1	337	1	−1
103	1	+1	183	2	+1	259	2	+1	339	2	+1
105	2	+1	185	2	−1	262	1	+1	341	1	+1
106	2	−1	186	2	+1	263	1	+1	345	2	+1
107	1	+1	187	2	+1	265	2	−1	346	6	−1
109	1	−1	190	2	+1	266	2	+1	347	1	+1
110	2	+1	191	1	+1	267	2	+1	349	1	−1
111	2	+1	193	1	−1	269	1	−1	353	1	−1
113	1	−1	194	2	+1	271	1	+1	354	2	+1
114	2	+1	195	4	+1	273	2	+1	355	2	+1
115	2	+1	197	1	−1	274	4	−1	357	2	+1
118	1	+1	199	1	+1	277	1	−1	358	1	+1
119	2	+1	201	1	+1	278	1	+1	359	3	+1
122	2	−1	202	2	−1	281	1	−1	362	2	−1
123	2	+1	203	2	+1	282	2	+1	365	2	−1
127	1	+1	205	2	+1	283	1	+1	366	2	+1
129	1	+1	206	1	+1	285	2	+1	367	1	+1
130	4	−1	209	1	+1	286	2	+1	370	4	−1
131	1	+1	210	4	+1	287	2	+1	371	2	+1
133	1	+1	211	1	+1	290	4	−1	373	1	−1
134	1	+1	213	1	+1	291	4	+1	374	2	+1
137	1	−1	214	1	+1	293	1	−1	377	2	+1
138	2	+1	215	2	+1	295	2	+1	379	1	+1
139	1	+1	217	1	+1	298	2	−1	381	1	+1
141	1	+1	218	2	−1	299	2	+1	382	1	+1
142	3	+1	219	4	+1	301	1	+1	383	1	+1
143	2	+1	221	2	+1	302	1	+1	385	2	+1
145	4	−1	222	2	+1	303	2	+1	386	2	+1
146	2	+1	223	3	+1	305	2	+1	389	1	−1
149	1	−1	226	8	−1	307	1	+1	390	4	+1
151	1	+1	227	1	+1	309	1	+1	391	2	+1
154	2	+1	229	3	−1	310	2	+1	393	1	+1
155	2	+1	230	2	+1	311	1	+1	394	2	−1
157	1	−1	231	4	+1	313	1	−1	395	2	+1
158	1	+1	233	1	−1	314	2	−1	397	1	−1
159	2	+1	235	6	+1	317	1	−1	398	1	+1
161	1	+1	237	1	+1	318	2	+1	399	8	+1
163	1	+1	238	2	+1	319	2	+1	401	5	−1
165	2	+1	239	1	+1	321	3	+1	402	2	+1
166	1	+1	241	1	−1	322	4	+1	403	2	+1
167	1	+1	246	2	+1	323	4	+1	406	2	+1
170	4	−1	247	2	+1	326	3	+1	407	2	+1
173	1	−1	249	1	+1	327	2	+1	409	1	−1
174	2	+1	251	1	+1	329	1	+1	410	4	+1
177	1	+1	253	1	+1	330	4	+1	411	2	+1
178	2	+1	254	3	+1	331	1	+1	413	1	+1
179	1	+1	255	4	+1	334	1	+1	415	2	+1

d	h	N(ε)	d	h	N(ε)	d	h	N(ε)	d	h	N(ε)
417	1	+1	438	4	+1	461	1	−1	482	2	+1
418	2	+1	439	5	+1	462	4	+1	483	4	+1
419	1	+1	442	8	−1	463	1	+1	485	2	−1
421	1	−1	443	3	+1	465	2	+1	487	1	+1
422	1	+1	445	4	−1	466	2	+1	489	1	+1
		+1	446	1	+1	467	1	+1	491	1	+1
426	6	+1	449	1	+1		3				−1
429	2	+1	451	2	−1	469	2	+1	494	2	+1
					+1	471	2	+1	497		+1
430	1	−1	454	1	+1	473	3	+1	498	2	+1
433	1	+1	455	1	+1	474	2	+1	499	5	+1
434	4			4	+1	478	1	+1			
		+1	457	1	−1	479	1	+1			
435	4	+1	458	2	−1	481	2	−1			

TABLE 3

Nombre h des classes de diviseurs des corps quadratiques réels $\mathbf{Q}(\sqrt{p})$ pour $p < 2\,000$ premier (E. L. Ince, Cycles of reduced ideals in quadratic fields, British association for the advancement of science. ***Mathematical tables,*** vol. IV, 1934, London).

Il existe 303 nombres premiers p inférieurs à 2 000 (y compris $p = 2$).

— Pour les 26 nombres :

p = ***79, 223, 229, 257, 359, 443, 659, 733,*** 761, 839, 1 091, 1 171, 1 223, 1 229, 1 367, 1 373, 1 489, 1 523, 1 567, 1 627, 1 787, 1 811, 1 847, 1 901, 1 907, 1 987

le nombre h est égal à 3 pour le corps $\mathbf{Q}(\sqrt{p})$.

— Pour les 7 nombres :

p = 401, 439, 499, 727, 1 093, 1 327, 1 429

le nombre h est égal à 5.

— Pour les 4 nombres :

p = ***577,*** 1 009, 1 087, 1 601,

il est égal à 7.

Pour p = 1 129, on a h = 9 (avec un groupe des classes de diviseurs qui est cyclique). Pour p = 1 297, on a h = 11. Pour tous les 264 nombres premiers $p < 2\,000$ restants le nombre des classes de diviseurs du corps $\mathbf{Q}(\sqrt{p})$ est égal à 1.

TABLE 4

Nombre h des classes de diviseurs des corps quadratiques imaginaires $\mathbf{Q}(\sqrt{-a})$, a sans carrés, $1 \leqslant a < 500$.

a	h	a	h	a	h	a	h	a	h
1	1	78	4	158	8	233	12	314	26
2	1	79		159	10	235		317	10
3	1	82	4	161	16	237	12	318	12
5	2	83		163	1	238	8	319	10
6	2	85	4	165	8	239	15	321	20
7	1	86	10	166	10	241	12	322	8
10	2	87	6	167	11	246	12	323	4
11	1	89	12	170	12	247	6	326	22
13	2	91		173	14	249	12	327	12
14	4	93	4	174	12	251	7	329	24
15	2	94	8	177	4	253	4	330	8
17	4	95		178	8	254	16	331	3
19	1	97	4	179	5	255	12	334	12
21	4	101	14	181	10	257	16	335	18
22	2	102	4	182	12	258		337	8
23	3	103	5	183	8	259	4	339	6
26	6	105	8	185	16	262	6	341	28
29	6	106	6	186	12	263	13	345	8
30	4	107	3	187	2	265	8	346	10
31	3	109	6	190	4	266	20	347	5
33	4	110	12	191	13	267	2	349	14
34	4	111		193	4	269	22	353	16
35	2	113	8	194	20	271	11	354	16
37	2	114	8	19.5	4	273	8	355	4
38	6	115	2	197	10	274	12	357	8
39	4	118	6	199	9	277		358	6
41	8	119	10	201	12	278	14	359	19
42	4	122	10	202	6	281	20		18
43	1	123	2	203	4	282	3	362 365	20
46	4	127	5	205	8	283	16	367 366	12
47	5	129	12	206	20	285			9
51	2	130	4	209	20	286	12		12
53	6	131	5	210	8	287	14	370 371	8
55	4	133	4	211	3	290	20	373	10
57	4	134	14	213	8	291			28
58	2	137	8	214		293	18	374 377	16
59	3	138	8	215	14	295	8	379	3
61	6	139	3	217	8	298	6	381	20
62	8	141	8	218	10	299	8		8
65	8	142	4	219	4	301	8	382	17
66	8	143	10	221	16	302	12	383	8
67	1	145	8	222	12	303	10		20
69	8	146	16	223	7	305	16	386 389	22
70	4	149	14	226	8	307	3	390	16
71	7	151	7	227	5	309	8	391	14
73	4	154	8	229	10	310	19	393	12
74	10	155	4	230	20	311		394	10
77	8	157	6	231	12	313	8	395	8

a	h	a	h	a	h	a	h	a	h
397	**6**	418	**8**	438	8	458	**26**	**479**	25
398	**20**	419	**9**	439	15	461	**30**	**481**	**16**
399	**16**	421	**10**	**442**	**8**	**462**	**8**	**482**	**20**
401	**20**	422	**10**	**443**	**5**	**463**	**7**	**483**	**4**
402	16	**426**	**24**	**445**	**8**	465	**18**	**485**	**16**
403	2	**427**	**2**	**446**	**32**	466	**7**	487	
406	**16**	429	**16**	**447**	**14**	467		**489**	27
407	**16**	430	**12**	**449**	**20**	469	16	**491**	9
409	**16**	431	**21**	451	**6**	470	20	493	**12**
410	**16**	433	**12**	453	**12**	471	16	494	**28**
411	**6**	434	**24**	**454**	**14**	473	**12**	**497**	24
413	**20**	435	**4**	**455**	**29**	474	**20**	**498**	8
415	**10**	437	**20**	457	8	**478**	8	499	3
417	**12**								

TABLE 5

Discriminants des ordres connus des corps quadratiques imaginaires tels que tout genre de modules associés (*) soit formé d'une seule classe (L. E. Dickson, Introduction *to the theory of numbers, 1929).*

1° Discriminants d'ordres maximaux (65 valeurs) :

— 3	— 43	— 148	-340	— 595	— 1 320
-4	— 51	— 163	— 372	— 627	— 1 380
-7	— 52	— 168	— 403	— 660	— 1 428
— 8	— 67	—187	-408	— 708	— 1 435
— 11	— 84	—195	—420	— 715	— 1540
— 15	— 88	—228	—427	— 760	— 1 848
— 19	— 91	—232	—435	— 795	— 1 995
— 20	— 115	— 235	—483	— 840	— 3 003
— 24	— 120	— 267	— 520	— 1 012	— 3 315
— 35	— 123	— 280	— 532	—1 092	— 5 460
-40	— 132	— 312	— 555	-1 155	

2° Discriminants d'ordres non maximaux (36 valeurs) :

$-3\cdot2^2$	$-4\cdot2^2$	$-7\cdot8^2$	$-15\cdot4^2$	$-88\cdot2^2$	$-408\cdot2^2$
$-3\cdot3^2$	$-4\cdot3^2$	$-8\cdot2^2$	$-15\cdot8^2$	$-120\cdot2^2$	$-520\cdot2^2$
$-3\cdot4^2$	$-4\cdot4^2$	$-8\cdot3^2$	$-20\cdot3^2$	$-168\cdot2^2$	$-760\cdot2^2$
$-3\cdot5^2$	$-4\cdot5^2$	$-8\cdot6^2$	$-24\cdot2^2$	$-232\cdot2^2$	$-840\cdot2^2$
$-3\cdot7^2$	$-7\cdot2^2$	$-11\cdot3^2$	$-35\cdot3^2$	$-280\cdot2^2$	$-1\,320\cdot2^2$
— 3.8"	$-7\cdot4^2$	$-15\cdot2^2$	$-40\cdot2^2$	$-312\cdot2^2$	$-1\,848\cdot2^2$

(*) Rappelons qu'un module est dit associé à un ordre s'il admet cet ordre pour anneau des stabilisateurs (N. d. T.).

Nombres « convenables » d'Euler.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1 320, 1 365, 1 848.

TABLE 6

Nombre h de classes de diviseurs pour certains corps cubiques $\mathbf{Q}(\sqrt[3]{m})$.

m	2	3	5	6	7	10	11
h	1	1	1	1	3	1	2
m	12	13	14	15	17	19	20
h	1	3	3	2	1	3	3
m	21	22	23	26	28	29	30
h	3	3	1	3	3	1	3
m	31	33	34	45	37	38	39
h	3	1	3	3	3	3	6
m	41	42	43	44	35	46	47
h	1	3	12	1	1	1	2
m	63	65	91	124	126	182	215
h	6	18	9	9	9	27	21
m	217	342	422				
h	27	27	21				

TABLE 7

Nombre h des classes de diviseurs des corps cubiques totalement réels de discriminant $< 20\,000$ (H. J. Godwin, P. A. Samet, J. *London Math.* Soc., 1959, 34, 108-110; H. J. Godwin, ***Proc.*** *Cambridge Philos. Soc.*, 1961, 57, 728-730).

Un corps cubique $\mathbf{Q}(\theta)$ est dit totalement réel si $s = 3$, $t = 0$, i. e. si tous ses isomorphismes dans le corps des nombres complexes sont réels.

Si de plus le polynôme minimal du nombre θ se décompose entièrement dans Q(0) en facteurs linéaires, alors Q(0) est dit cyclique. Les corps cubiques cycliques sont caractérisés par le fait que leurs discriminants sont des carrés.

11 existe 830 corps cubiques totalement réels de discriminant $< 20\ 000$. Parmi eux, il y a 24 corps cycliques. Pour 16 de ces corps cubiques cycliques le nombre h est égal à 1. Ces corps ont pour discriminants :

$$7^2,\ 9^2,\ 13^2,\ 19^2,\ 31^2.\ 37^2,\ 43^2,\ 61^2,$$
$$67^2,\ 73^2,\ 79^2,\ 97^2,\ 103^2,\ 109^2,\ 127^2,\ 139^2.$$

Pour chacun des discriminants :

$$63^2,\ 91^2,\ 117^2,\ 133^2$$

il y a exactement deux corps cubiques cycliques et, pour ces 8 corps, $h = 3$.

Les corps cubiques totalement réels non cycliques dont les discriminants sont compris entre 1 et 20 000 se répartissent ainsi (pour tout discriminant on a seulement un corps) :

Bornes pour le discriminant	Nombre de corps	Bornes pour le discriminant	Nombre de corps
1- 1 000	22	11 001-12 000	52
1 001- 2 000	32		37
2 001- 3 000	35	12 13 001-13 001-14 000 000	43
3 001- 4 000	39		42
4 001- 5 000	34	1415 001-15 001-16 000 000	46
5 001- 6 000	41	16 001-17 000	52
6 001- 7 000	37		39
7 001-8000	47	1718 001-18 001-19 000 000	39
8 001- 9 000	40	19 001-20 000	48
9 001-10 000	39		
10 001-11 000	42	En tout	806

Parmi eux, on a $h = 1$ pour 748 corps. Le nombre de corps tels que $h = 2$ est égal à 29. Leurs discriminants sont égaux à :

1 957, 2 777, 3 981, 6 809, 7 053, 7 537,
8 468, 8 789, 9 301, 10 273, 10 889, 11 197,
11 324, 11 348, 12 197, 13 676, 13 768, 14013,
14 197, 15 188, 15 529, 16 609, 16 997, 17 417,
17 428, 17 609, 17 989, 18 097, 19 429.

Les corps tels que $h = 3$ (en tout 26 corps) ont pour discriminants :

2 587, 4 212, 4 312, 5 684, 6 885, 7 220,
8 829, 9 653, 9 800, 9 996, 10 309, 11 417,
13 916, 13 932, 14 661, 14 945, 15 141, 15 884,
16 660, 16 905, 18 228, 18 252, 18 792, 19 220,
19 604, 19 764.

Pour 3 corps de discriminants :

8 069, 16 357, 19 821

le nombre h est égal à 4. Il n'y a pas de corps tels que $h \geqslant 5$ (parmi les corps cubiques totalement réels de discriminant $< 20\ 000$).

Remarque. — Dans les limites de la table, pour tout discriminant $< 20\ 000$ il existe seulement un corps cubique totalement réel non cyclique. Pourtant, ce fait n'a pas toujours lieu. Ainsi, par exemple, il existe au moins 3 corps de discriminant 23 356 (cf. exercice 21, chap. II, § 2).

TABLE 8

Le facteur $h^* = h^*(l)$ du nombre de classes de diviseurs du $l^{\text{ième}}$ corps cyclotomique, pour $l < 100$ premier.

l	h^*	l	h^*
3	1	43	211
5	1	47	*5.139*
7	1	53	**4** *889*
11	1	59	*3.59.233*
13	1	61	**41.1 861**
17	1	67	**67.12** *739*
19	1	71	*72.79* **241**
23	3	73	*89.134* **353**
29	2^3	79	**5.53.377** 911
31	9	83	**3.279 405 653**
37	37	89	**113.118 401** *449*
41	11^2	97	**57.73 457.206** *209*

TABLE 9

Nombres premiers irréguliers $\leqslant 4\,001$. Dans chaque colonne de droite on a indiqué les nombres 2a pour lesquels le numérateur du nombre de Bernoulli B_{2a} ($2 \leqslant 2a \leqslant l - 3$) est divisible par l (les nombres de Bernoulli sont numérotes de deux en deux : $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, etc.). Il existe en tout 216 nombres premiers irréguliers $\leqslant 4\,001$. Les nombres premiers impairs $< 4\,000$ qui ne figurent pas dans la table sont tous réguliers (leur nombre est égal à 334) (D. H. Lehmer, Emma Lehmer, H. S. Vandiver, J. L. Selfridge et C. A. Nicol, *Proc. Nat. Acad. Sci. U. S. A.*, 1954, 40, n° 1, 25-33; 1954, n° 8, 732-735; 1955, 41, n° 11, 970-973).

l	2a	l	2a	l	2a
37	32	547	270,486	887	418
59	44	557	222	929	520, 820
67	58	577	52	953	156
101	68	587	90, 92	971	166
103	24	593	22	1 061	474
131	22	607	592	1 091	888
149	130	613	522	1 117	794
157	62, 110	617	20, 174, 338	1 129	348
233	84	619 631	428 80, 226	1 151 153	534, 802 784, 968
257	164				
263	100	647	48, 242, 554	1 193	262
	84	653	224	1 201	676
283	20	659		1217	784, 866, 1118
293	156	673	408, 502	1229	784
307	88	677	628	1 237	874
311	292	683	32	1 279	518
347	280	691	312. 200	1 283	510
353	186, 300	727		1 291	206, 824
379	100, 174	751	290	1 297	202,220
389	200	757	514	1 301	176
401	382	761	260	1 307	382, 852
409	126	773	732	1 319	304
421	240	797	220	1 327	466
433	366	809	330, 628	1 367	234
461	196	811	544	1 409	358
463	130	821	744	1 429	996
467	94, 194	827	66	1 439	574
491	292, 336, 338	839 877	868	1 483 499	224
523	490				94
541	86	881	162	1 523	1 310

(Suite)

l	*2a*	*l*	*2a*	*l*	*2a*
1 559	862	2 371	242, 2 274	3 313	2 222
1 609	1 356	2 377	1 226	3 323	3 292
1 613	172	2 381	2060	3 329	1 378
1 619	560	2 383	842, 2 278	3 391	2 232, 2 534
1 621	980	2 389	776	3 407	2 076, 2 558
1 637	718	2 411	2 126	3 433	1 300
1 663	270	2 423	290, 884	3 469	1 174
1 669	388, 1 086	2441	366, 1 750	3 491	2 544
1 721	30	2 503	1 044	3 511	1 416, 1 724
1 733	810, 942	2 543	2 374	3 517	1 836, 2 586
1 753	712	2 557	1 464	3 529	3 490
1 759	1 520	2 579	1 730	3 533	2 314, 3 136
1 777	1 192	2 591	854, 2 574	3 539	2 082, 2 130
1 787	1 606	2 621	1 772	3 559	344, 1 592
1 789	848, 1 442	2 633	1416	3 581	1 466
1 811	550, 698, 1 520	2 647	1 172	3 583	1 922
1 831	1 274	2 657	710	3 593	360, 642
1 847	954, 1 016, 1 558	2 663	1 244	3 607	1 976
1 871	1 794	2 671	404, 2 394	3 613	2 082
1 879	1 260	2 689	926	3 617	16, 2 856
1 889	242	2 753	482	3 631	1 104
1 901	1 722	2 767	2 528	3 637	2 526, 3 202
1 933	1 058, 1 320	2 777	1 600	3 671	1 580
1 951	1 656	2 789	1 984, 2 154	3 677	2 238
1 979	148	2 791	2 554	3 697	1 884
1 987	510	2 833	1 832	3 779	2 362
1 993	912	2 857	98	3 797	1 256
1 997	772, 1 888	2 861	352	3 821	3 296
003	60, 600	2 909	400, 950	3 833	1 840, 1 998, 3 286
2 017	1 204	2 927	242	3 851	216, 404
2 039	1 300	2 939	332, 1 102, 2 748	3 853	748
053	1 932	2 957	138, 788	3 881	1 686, 2 138
2 087	376, 1 298	2 999	776	3 917	1490
2 099	1 230	3011	1496	3 967	106
2 111	1 038	3 023	2 020	3 989	1 936
137	1 624	3049	700	4001	534
2 143	1 916	3 061	2 522		
153	1 832	3 083	1 450		
2 213	154	3 089	1 706		
2 239	1 826	3 119	1704		
2 267	2 234	3 181	3 142		
2 273	876, 2 166	3 203	2 368		
2 293	2 040	3 221	98		
2 309	1 660, 1 772	3 229	1 634		
2 357	2 204	3 257	922		

INDEX TERMINOLOGIQUE

TABLE DES MATIÈRES

IMPRIMÉ EN FRANCE
IMPRIMERIE BARNÉOUD S. A., LAVAL, N° 5307. — 11-1966
4e TRIMESTRE 1966.

DÉPÔT LÉGAL ÉD. N° 1472. N° de code 518-21
6608

∞) $X^2 - AY^2 = 1$

puisque si $\sqrt{A} \cong \frac{P_\alpha}{Q_1}, \frac{P_{\alpha+1}}{Q_{\alpha+1}}$

$$P_\alpha Q_{\alpha+1} - P_{\alpha+1} Q_\alpha = 1$$

sont 2 fractions consécutives des dev f. c. de $\sqrt{A}$
on peut remplacer P, Q dans l'éq par X et Y et obtenir une sol de l'équation.
plus généralement si $X^2 - AY^2 = m$ voir sol.

---

corps quad. ex: $X^2 - 2Y^2$ irréductible sur $\mathbb{Q}$ mais se décompose en facteurs linéaires dans $\mathbb{Q}(\sqrt{2})$

la norme est $N(X + Y\sqrt{2}) \Rightarrow X^2 - 2Y^2$