MATHÉMATIQUES
à l'Université

Cours et exercices corrigés

Collection dirigée par
Charles-Michel Marle
Philippe Pilibossian

Extensions de corps

Théorie de Galois

niveau M1-M2

Josette Calais

MATHÉMATIQUES À L'UNIVERSITÉ

Collection dirigée par Charles-Michel MARLE et Philippe PILIBOSSIAN

niveau M1-M2

EXTENSIONS DE CORPS

Théorie de Galois

Josette CALAIS
Professeur émérite à l'Université de Reims-Champagne-Ardenne

ellipses

Dans la même collection "Mathématiques à l'Université"

- *L'algèbre discrète de la transformée de Fourier*, G. Peyré, 2004.
- *Algèbre et théorie des nombres – cryptographie, primalité*, S. Al Fakir, 2003.
- *Algèbre et théorie des nombres – théorie de Galois, codes, géométrie et arithmétique*, S. Al Fakir, 2004.
- *Algèbre fondamentale – Arithmétique*, G. Gras et M.-N. Gras, 2004.
- *Algèbre linéaire*, R. Goblot, 2005.
- *Algèbre linéaire*, F. Bories-Longuet, 2000.
- *Algèbre linéaire numérique – cours et exercices*, G. Allaire et S. M. Kaber, 2002.
- *Analyse complexe et distributions*, A. Yger, 2001.
- *Analyse fonctionnelle – exercices et problèmes corrigés*, B. Maury, 2004.
- *Calcul différentiel*, G. Christol, A. Cot et Ch.-M. Marle, 1997.
- *Cours d'algèbre*, R. Elkik, 2002.
- *Cours de calcul formel – algorithmes fondamentaux*, Ph. Saux Picart, 1999.
- *Cours de calcul formel – corps finis, systèmes polynomiaux, applications*, Ph. Saux Picart et E. Rannou, 2002.
- *Distributions – espaces de Sobolev, applications*, M.-Th. Lacroix-Sonrier, 1999.
- *Éléments d'algèbre commutative*, J. Briançon et Ph. Maisonobe, 2004.
- *Éléments d'analyse convexe et variationnelle*, D. Azé, 1997.
- *Éléments de géométrie*, A. Yger et A. Hénaut, 2004.
- *Éléments de théorie des anneaux – anneaux commutatifs*, J. Calais, 2006.
- *Éléments d'intégration et d'analyse fonctionnelle*, A. El Kacimi Alaoui, 1999.
- *Équations aux dérivées partielles et leurs approximations*, B. Lucquin, 2004.
- *Extensions de corps – théorie de Galois*, J. Calais, 2006.
- *Géométrie différentielle avec 80 figures*, C. Doss-Bachelet, J.-P. Françoise et Cl. Piquet, 2000.
- *Les Groupes finis et leurs représentations*, G. Rauch, 2000.
- *Initiation à la topologie générale*, D. Lehmann, 2004.
- *Intégrales curvilignes et de surface*, M. Lofficial et D. Tanré, 2006.
- *Intégration et théorie de la mesure – une approche géométrique*, P. Krée, 1997.
- *Une introduction à la géométrie projective*, D. Lehmann, 2003.
- *Introduction à Scilab – exercices pratiques corrigés d'algèbre linéaire*, G. Allaire et S. M. Kaber, 2002.
- *Logique, ensemble, catégories – le point de vue constructif*, P. Ageron, 2000.
- *Méthodes d'approximation, équations différentielles, applications Scilab*, S. Guerre-Delabrière et M. Postel, 2004.
- *Méthodes numériques directes de l'algèbre matricielle*, Cl. Brezinski et M. Redivo-Zaglia, 2005.
- *Méthodes numériques itératives – algèbre linéaire et non linéaire*, Cl. Brezinski et M. Redivo-Zaglia, 2006.
- *Précis d'analyse réelle – topologie, calcul différentiel, méthodes d'approximation, vol. 1*, V. Komornik, 2001.
- *Précis d'analyse réelle – analyse fonctionnelle, intégrale de Lebesgue, espaces fonctionnels, vol. 2*, V. Komornik, 2002.
- *Probabilités*, M. Brancovan et Th. Jeulin, 2006.
- *Quelques aspects des mathématiques actuelles*, ouvrage collectif, 1999.
- *Systèmes dynamiques – une introduction*, Ch.-M. Marle, 2003.
- *Théorie de Galois*, I. Gozard, 1997.
- *Topologie*, G. Christol, A. Cot et Ch.-M. Marle, 1997.
- La *Topologie des espaces métriques*, E. Burroni, 2005.

ISBN 2-7298-2780-3

Présentation de la collection "Mathématiques à l'Université"

Depuis 1997, cette collection se propose de mettre à la disposition des étudiants de troisième, quatrième et cinquième années d'études supérieures en mathématiques des ouvrages couvrant l'essentiel des programmes actuels des universités françaises. Certains de ces ouvrages pourront être utiles aussi aux étudiants qui préparent le CAPES ou l'Agrégation, ainsi qu'aux élèves des grandes écoles et aux ingénieurs désirant actualiser leurs connaissances.

Nous avons voulu rendre ces livres accessibles à tous : les sujets traités sont présentés de manière simple et progressive, tout en respectant scrupuleusement la rigueur mathématique. Chaque volume comporte, en général, un exposé du cours avec des démonstrations détaillées de tous les résultats essentiels, des énoncés d'exercices ou de problèmes.

Ce nouveau livre de Madame Josette Calais fait suite à son ouvrage sur les anneaux, publié dans la même collection. Les lecteurs déjà familiarisés avec les propriétés des anneaux commutatifs pourront l'aborder indépendamment du précédent. La théorie de Galois, dont Madame Calais donne ici une présentation remarquablement claire, est une magnifique construction de l'esprit humain qui a permis de répondre de manière complète et définitive à des questions, dont certaines étaient posées depuis l'Antiquité : quelles figures géométriques planes, en particuliers quels polygones réguliers, peuvent être construits de manière exacte à la règle et au compas ? quelles sont les équations polynômiales qui peuvent être résolues par radicaux ? Cette théorie est toujours d'actualité et comporte des développements récents, notamment pour l'application aux équations différentielles analytiques. Comme le précédent, ce livre comporte de nombreux exercices qui permettront au lecteur de bien assimiler toutes les notions introduites.

Charles–Michel Marle Philippe Pilibossian

Préface

Ce livre commence par une étude approfondie des Extensions de corps, prélude indispensable à la THEORIE de GALOIS.

La Théorie de Galois occupe, historiquement, et encore actuellement, une place importante dans le monde des mathématiques.
Elle repose sur l'idée géniale (au sens propre du terme) d'Evariste GALOIS (1811-1832), consistant à associer à un polynôme $f(X)$ à coefficients dans un corps K, une certaine extension E de K et de faire correspondre à E, le groupe de ses K-automorphismes, qui sera appelé le *groupe de Galois* du polynôme $f(X)$ ou de l'extension $E : K$.
Ce procédé conduit à une remarquable mise en parallèle entre, les propriétés des extensions de corps et celles de leurs groupes de Galois (Ch. 7).
Il en résulte une méthode d'investigation extrêmement puissante, qui permit de résoudre plusieurs problèmes fondamentaux, dont certains préoccupaient les mathématiciens depuis l'Antiquité, tels la construction de figures géométriques, par la règle et le compas (Ch. 2 et 7), et qui amena E. GALOIS à la caractérisation des équations polynomiales résolubles par radicaux (Ch. 9).
Cette dernière question intéressait, tout particulièrement, les mathématiciens contemporains d'E.Galois, dont Niels Henrik ABEL (1802-1829), qui avait déjà obtenu un résultat décisif, concernant ce problème (Voir l'introduction historique du Ch. 9).
Mais ce sont les travaux d'E. GALOIS qui apportèrent une réponse complète et définitive à la question. Cependant, en raison de sa disparition en 1832, ses résultats ne furent connus que beaucoup plus tard. C'est le mathématicien Joseph LIOUVILLE (1809-1882) qui les publia en 1843, après avoir eu la possibilité de connaître et d'étudier les manuscrits d'Evariste Galois.

Les sujets d'intérêt d'E.Galois, en mathématiques, ne se limitèrent pas aux équations polynomiales ; il obtient, en particulier, des résultats concernant les fonctions et les intégrales elliptiques.
De plus, il amorça l'étude des corps finis (longtemps appelés *champs de Galois*), qui furent utilisés au 20ème siècle, en particulier pour la conception des codes correcteurs d'erreurs, permettant d'augmenter la fiabilité des informations transmises par les ordinateurs.

Aujourd'hui, la Théorie de Galois reste bien présente, par ses applications et ses prolongements dans plusieurs domaines des mathématiques ([45]) : la théorie algébrique des nombres, les anneaux non commutatifs, les corps gauches (anneaux à division), les équations différentielles ; elle fût aussi utilisée dans les travaux conduisant à la classification des groupes simples finis ([47]).

Evariste Galois conserve une place à part, dans l'esprit et dans le coeur de tout mathématicien. Nul ne peut rester indifférent à l'évocation de la vie, si tumultueuse, si controversée,

si dense et si courte, de ce génie mathématique, mort en duel, le 30 mai 1832, à 21 ans. Il existe de nombreux écrits sur l'oeuvre et la vie d'Evariste Galois ([6], [11], [46], [48]). Je signale, en particulier, au lecteur, le Numéro Spécial consacré à Evariste GALOIS (Le mathématicien maudit) par la revue américaine « Scientific American », publié dans la revue française, « Pour la SCIENCE », trimestre : Février 2003 - Mai 2003 (Série : Les Génies de la Science).

Je tiens à remercier Elise Benlolo, maître de conférences au Département de Mathématiques de l'Université de Reims-Champagne-Ardenne, qui a pris part à la relecture de ce livre, avec beaucoup d'attention et de minutie.

J'exprime toute ma reconnaissance à Charles-Michel Marle et Philippe Pilibossian qui ont bien voulu accueillir ce livre et le précédent, « Eléments de théorie des anneaux »([13]), dans leur collection.

Je remercie chaleureusement, Monsieur Charles-Michel Marle pour l'aide précieuse et bienveillante qu'il m'a apportée, lors de la mise aux Normes des Editions Ellipses de mes deux livres.

J.C.

Introduction

Ce volume comprend neuf chapitres et deux appendices (A et B).

Dans les chapitres 1, 2, 3, sont développées les proprétés essentielles des *extensions de corps* (extensions algébriques - transcendantes - normales - séparables - purement séparables).
L'application de la notion d'extension algébrique, au problème de la *construction par la règle et le compas*, est abordée dès le chapitre 2.

Le chapitre 4 est consacré aux *corps finis*, qui trouvent leur utilité dans des domaines très divers, en particulier, dans la conception de codes correcteurs d'erreurs ([21]), d'où leur intérêt en Informatique et en Statistiques.

La notion de *clôture algébrique* est étudiée au chapitre 5, dans lequel, on trouvera, entre autres, une démonstration explicite du théorème dit *Théorème fondamental de l'Algèbre* : « $\mathbb{C}$ est algébriquement clos ».
Par ailleurs, bien que l'Appendice B ait pour objet les preuves classiques de la transcendance de e et de π, sur $\mathbb{Q}$, une autre démonstration en est proposée dans ce chapitre 5, en application de la notion d'*éléments algébriquement indépendants* ; cette preuve s'appuie essentiellement sur le théorème de Lindemann-Weierstrass.

Les *polynômes et extensions cyclotomiques* sont traités au chapitre 6. Les cas où le corps de base est soit $\mathbb{Q}$, soit un corps fini, sont étudiés en détail. Le chapitre 6 se termine par l'*algorithme de Berlekamp* qui permet, en particulier, de déterminer les facteurs irréductibles, distincts, d'un polynôme cyclotomique sur un corps fini.

La *Théorie de Galois* classique (sur un corps commutatif, de caractéristique 0) est présentée au chapitre 7, avec, comme premières applications, la *construction des polygônes réguliers* par la règle et le compas, et une seconde preuve du *Théorème fondamental de l'Algèbre*.

Les chapitres 8 et 9 dépendent du chapitre 7, mais sont indépendants l'un de l'autre.

Au chapitre 8, les propriétés des *corps de nombres*, auxquels sont directement rattachés les *anneaux d'entiers algébriques*, donnent l'occasion d'introduire et d'étudier les *anneaux de Dedekind.*

Le chapitre 9 traite du problème de la *résolution des équations polynômiales par radicaux*, auquel, historiquement, nous conduit la Théorie de Galois.

Quelques propriétés du corps $\mathbb{R}$, utiles au chapitre 5, sont rappelées au début de l'Appendice A. Mais, le but de cet appendice est de définir les *corps de nombres p-adiques*, qui

sont introduits, ici, à partir de la notion de *complété d'un corps valué.*

Comme dans les livres "Eléménts de théorie des anneaux" ([13]) et "Eléménts de théorie des groupes" ([12]), les propriétés énoncées sont généralement prouvées de façon détaillée et à la fin de chaque chapitre, des exercices peuvent, éventuellement, permettre une compréhention plus approfondie du cours.

Table des matières

Notations

Les notations générales sont celles du livre "Eléments de théorie des anneaux" ([13]).

Si K est un corps, $K^* = K \setminus \{0\}$
$card(K) = \mid K \mid$: cardinal de K
$car K$, 1
$L : K$, 4
$K(T), K(\alpha)$, 4
$[L : K]$, 6
$\mathbb{F}_p$, 55
$\overline{K}$, 74
U_n, 83
Ω_n, 84
$\Phi_n(X)$, 85
$\mu(d)$, 87
$G(L : K)$, 109
$In_L(H)$, 110
$[L : K]_s$, 114
$N_{L:K}(\alpha)$, $T_{L:K}(\alpha)$, 132
$N(\alpha)$, $T(\alpha)$, 132
$\Delta[x_1, x_2, \ldots, x_n]$, 147
$\mathcal{A}$, 149
$\mathcal{D}$, 153
$\hat{K}$, 203
$\mathbb{Z}_p$, $\mathbb{Q}_p$, 205

Chapitre premier
Notion d'extension de corps

Les notations générales seront les mêmes que dans le livre : "Eléments de théorie des anneaux" (Cf. [13]) ; en particulier, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ont la même signification que dans ([13]).

Rappels et remarques préliminaires :
a) On appelle **corps,** tout anneau unitaire, commutatif, dans lequel tout élément non nul a un *inverse* ([13], Déf. 1.6).
Tout corps est nécessairement intègre ([13], Rem. 1.20).
b) Lorsque K et K' sont deux corps tels que $K' \subseteq K$, on dit que K' est un **sous-corps** de K, si le corps K' est un sous-anneau unitaire de K([13], Rem. 1.34),
et si de plus, $K' \neq K$, alors K' est un **sous-corps propre** de K.
On notera que tout sous-anneau unitaire ([13], Rem. 1.34) d'un corps K n'est pas nécessairement un corps. Par exemple, $\mathbb{Z}$ est un sous-anneau unitaire du corps $\mathbb{Q}$, mais n'est pas un corps.

1. Corps premiers

A. Caractéristique d'un corps

Proposition 1.1. *La* **caractéristique** *d'un corps est soit* 0, *soit un* nombre premier.

Démonstration. La notion de *caractéristique* d'un anneau unitaire, commutatif, a été définie dans ([13], Déf. 1.68), ainsi que celle de *nombre premier* ([13], App. A, Déf. A.5, Rem. A.6).
K désignant un corps, soit ϕ l'unique morphisme d'anneaux unitaires de $\mathbb{Z}$ dans K ([13], Prop. 1.66). Pour tout $n \in \mathbb{Z}$, $\phi(n) = n1_K$, où 1_K désigne l'élément unité du corps K; ϕ est appelé *morphisme canonique* de $\mathbb{Z}$ dans K.
La caractéristique du corps K est, par définition ([13], Déf. 1.68), l'unique entier $k \in \mathbb{N}$ tel que $Ker\,\phi = k\mathbb{Z}$.
Si ϕ est injectif, alors $Ker\,\phi = (0)$, donc $car K = 0$.
Si ϕ est non injectif, on a $Ker\,\phi = k\mathbb{Z} \neq (0)$ et $Im\,\phi \simeq \mathbb{Z}/k\mathbb{Z}$.
$Im\,\phi$ étant un sous-anneau du corps K, l'anneau $\mathbb{Z}/k\mathbb{Z}$ est intègre, par suite, $k = car K$ est un nombre premier ([13], Cor. 1.14). □

Remarque 1.2. a) On rappelle que les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0 et que pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p ([13], Exemple 1.70).

b) Si K' est un sous-corps d'un corps K, alors ([13], Rem. 1.71)

$$1_{K'} = 1_K \Longrightarrow car K' = car K.$$

B. Sous-corps premier d'un corps

K étant un corps, soit $\{K_i\}_{i\in I}$, la famille des sous-corps de K. Cette famille est non vide, car elle contient K.
Posons $\Delta := \bigcap_{i\in I} K_i$; Δ est alors le plus petit sous-corps de K.

Définition 1.3. Dans le contexte ci-dessus, Δ est appelé le **sous-corps premier** de K.

Proposition 1.4. *Le corps $\mathbb{Q}$ et les corps du type $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier, n'ont pas dë sous-corps propre.*

Démonstration. 1) Supposons que le corps $\mathbb{Q}$ des nombres rationnels ait un sous-corps K; le corps K, contenant 0 et 1, contient alors l'anneau des entiers $\mathbb{Z}$. Or, le plus petit corps contenant $\mathbb{Z}$ est son corps de fractions, c'est-à-dire $\mathbb{Q}$ ([13], Exem. 5.4, Rem. 5.8) ; on en déduit que $K = \mathbb{Q}$.
2) Soit p un nombre premier ; si $\mathbb{Z}/p\mathbb{Z}$ avait un sous-corps propre, celui-ci serait de la forme $m\mathbb{Z}/p\mathbb{Z}$, avec $m > 1$ et $p\mathbb{Z} \subset m\mathbb{Z} \subset \mathbb{Z}$ ([13], Th. 2.35). Ces conditions impliquent $m|p$ avec $m \neq p$ et $m \neq 1$, ce qui contredit l'hypothèse p premier, donc $\mathbb{Z}/p\mathbb{Z}$ n'a pas de sous-corps propre. □

On en conclut que les corps $\mathbb{Q}$ et $\mathbb{Z}/p\mathbb{Z}$ s'identifient à leurs sous-corps premiers respectifs, ce qui justifie la définition suivante.

Définition 1.5. On dit que le corps $\mathbb{Q}$, ainsi que les corps du type $\mathbb{Z}/p\mathbb{Z}$ sont des **corps premiers.**
Plus généralement, on appellera **corps premier**, tout corps isomorphe soit à $\mathbb{Q}$, soit à un corps du type $\mathbb{Z}/p\mathbb{Z}$.

Théorème 1.6. *Le sous-corps premier d'un corps quelconque est isomorphe soit à $\mathbb{Q}$, soit à un corps du type $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. K étant un corps, soit ϕ le morphisme canonique de $\mathbb{Z}$ dans K et Δ le sous-corps premier de K (Déf. 1.3).
Δ contient les éléments 0 et 1 du corps K, donc Δ contient

$$Im\phi = \{n1\,;\, n \in \mathbb{Z}\}.$$

Si $carK = 0$, alors ϕ est injectif (voir la preuve de la Prop. 1.1) d'où $Im\phi \simeq \mathbb{Z}$. On en déduit que Δ contient un sous-corps isomorphe au corps $\mathbb{Q}$ des fractions de $\mathbb{Z}$; mais Δ étant le plus petit sous-corps de K, on a nécessairement $\Delta \simeq \mathbb{Q}$.
Si $carK = p(\neq 0)$, on a (Prop. 1.1) $Im\phi \simeq \mathbb{Z}/p\mathbb{Z}$, donc $Im\phi$ est un sous-corps de Δ; mais Δ est le plus petit sous-corps de K, d'où $\Delta = Im\phi \simeq \mathbb{Z}/p\mathbb{Z}$. □

Remarque 1.7. Soit Δ le sous-corps premier d'un corps K.
Si $carK = 0$ (resp. $carK = p \neq 0$), on identifie souvent Δ à $\mathbb{Q}$ (resp. $\mathbb{Z}/p\mathbb{Z}$) et on dit que « $\mathbb{Q}$ (resp. $\mathbb{Z}/p\mathbb{Z}$) est le corps premier de K ».
On en déduit que

$$carK = 0 \Longrightarrow card(K) \text{ infini};$$
$$card(K) \text{ fini } \Longrightarrow carK \neq 0.$$

On notera que les implications ci-dessus n'admettent pas de réciproques.
En effet, p étant un nombre premier, le corps $(\mathbb{Z}/p\mathbb{Z})(X)$ des fractions rationnelles à une indéterminée sur $\mathbb{Z}/p\mathbb{Z}$ ([13], Ch. 5) est de cardinal infini et de caractéristique $p \neq 0$.

2. Notion d'extension de corps

On rappelle que tout morphisme *non nul* d'un corps K dans un anneau, donc a fortiori dans un corps L, est *injectif* ([13], Prop. 1.58).
En particulier, si λ est un morphisme d'anneaux unitaires d'un corps K dans un corps L, alors $\lambda(1_K) = 1_L$ implique $\lambda \neq 0$, donc λ injectif ; par suite $Im\,\lambda$ est un sous-corps de L.

Définition 1.8. Etant donné un corps K, on appelle **extension** de K tout corps L contenant un sous-corps isomorphe à K.

Remarque 1.9. a) D'après ce qui précède, un corps L est extension d'un corps K, s'il existe un morphisme d'anneaux unitaires de K dans L ; un tel morphisme (nécessairement injectif) sera appelé un **plongement** ou un **monomorphisme** de K dans L ([13], Ex. 16, Ch. 1).
On en déduit qu'un corps L n'est pas extension d'un corps K si et seulement si l'ensemble des morphismes d'anneaux unitaires de K dans L est vide.
b) Si K est un sous-corps de L, alors l'injection canonique de K dans L est un monomorphisme, donc L est extension de K.
En conséquence, étant donné une extension L d'un corps K, si λ est un plongement de K dans L, on identifiera souvent K à $Im\,\lambda$; on supposera donc $K \subseteq L$, si cela ne restreint pas la généralité.

Exemple 1.10. Les résultats du paragraphe précédent permettent de justifier les exemples suivants.
1) Tout corps de caractéristique 0 est extension du corps $\mathbb{Q}$.
En particulier, les inclusions $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ montrent que $\mathbb{R}$ et $\mathbb{C}$ sont extensions de $\mathbb{Q}$ et que $\mathbb{C}$ est extension de $\mathbb{R}$.
Tout corps de caractéristique $p \neq 0$ est extension du corps $\mathbb{Z}/p\mathbb{Z}$.

2) Soit $L := \{p+qi ; (p,q) \in \mathbb{Q} \times \mathbb{Q}, i^2 = -1 \text{ dans } \mathbb{C}\}$.
On vérifie que L est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$, donc L est une extension de $\mathbb{Q}$ et $\mathbb{C}$ est une extension de L.

3) Posons $P := \{p+q\sqrt{2} ; (p,q) \in \mathbb{Q} \times \mathbb{Q}\}$.
On montre que P est un sous-corps de $\mathbb{R}$; on a, en particulier,

$$\text{pour } p+q\sqrt{2} \neq 0,\ (p+q\sqrt{2})^{-1} = \frac{p}{p^2-2q^2} - \frac{q}{p^2-2q^2}\sqrt{2} \text{ dans } P;$$

donc $\mathbb{R}$ est extension du corps P.

4) Tout corps K est un sous-corps du corps $K(X)$ des fractions rationnelles à coefficients dans K ([13], Ch. 5), donc $K(X)$ est une extension de K.

Définition 1.11. S étant une partie non vide d'un corps K, on appelle **sous-corps de K engendré par S**, l'intersection de tous les sous-corps de K contenant S ; c'est donc le plus petit sous-corps de K contenant S.

Exemple 1.12. 1) Le sous-corps premier d'un corps K (Déf. 1.3) est le sous-corps de K engendré par $\{0,1\}$.

2) Soit $\{i\} \subset \mathbb{C}$, où $i^2 = -1$; alors le sous-corps de $\mathbb{C}$ engendré par $\{i\}$ est le corps

$$L := \{p+qi; (p,q) \in \mathbb{Q} \times \mathbb{Q}\}.$$

En effet, le sous-corps de $\mathbb{C}$ engendré par $\{i\}$, noté (i), est de caractéristique 0, donc contient $\mathbb{Q}$. On en déduit que $L \subseteq (i)$. Or (i) est, par définition, le plus petit sous-corps de $\mathbb{C}$ contenant l'élément i, par suite, $(i) = L$.

Notation : Le fait qu'un corps L est extension d'un corps K se traduit symboliquement par la formule $L : K$.

Définition 1.13. Soit $L : K$ une extension de corps. On suppose $K \subseteq L$; alors pour toute partie non vide T de L, le sous-corps de L engendré par $K \cup T$ est noté $K(T)$ et appelé **extension de K obtenue par l'adjonction de T à K.**

Cas particuliers : les notations sont celles de la définition 1.13.
1) Pour $T = \{\alpha\}$, où $\alpha \in L$, $K(T)$ s'écrit $K(\alpha)$ et est dite **extension simple** de K, obtenue par l'adjonction de α à K.
On note que si $\alpha \in K$ alors $K(\alpha) = K$.
2) Plus généralement, pour $T = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, où $n \in \mathbb{N}^*$ et les α_i, $1 \leq i \leq n$, sont des éléments de L, $K(T)$ est noté $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ et appelé extension de K obtenue par l'adjonction de $\alpha_1, \alpha_2, \ldots, \alpha_n$ à K.

Proposition 1.14. *Avec les hypothèses et notations précédentes, pour $n > 1$, le corps $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ peut être considéré comme l'extension de K obtenue par les adjonctions successives de $\alpha_1, \alpha_2, \ldots, \alpha_n$; c'est-à-dire que :*

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2),\ K(\alpha_1, \alpha_2, \alpha_3) = K(\alpha_1, \alpha_2)(\alpha_3), \ldots$$
$$\ldots, K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n).$$

Démonstration. On démontre ce résultat par récurrence sur n.
Supposons $n = 2$; les éléments α_1 et α_2 étant, par hypothèse, dans le corps L, d'après la définition 1.11, $K(\alpha_1, \alpha_2)$ est le plus petit sous-corps de L contenant K, α_1 et α_2. Or on a $K(\alpha_1) \subseteq K(\alpha_1, \alpha_2)$ et $\alpha_2 \in K(\alpha_1, \alpha_2)$, d'où

$$K(\alpha_1)(\alpha_2) \subseteq K(\alpha_1, \alpha_2) \subseteq L.$$

Le corps $K(\alpha_1)(\alpha_2)$ étant un sous-corps de L, contenant K, α_1 et α_2, on en déduit que

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2).$$

Supposons $n > 2$; si $K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$ est l'extension de K obtenue par les adjonctions successives de $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$, alors le raisonnement fait pour $n = 2$, permet de prouver que

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n),$$

d'où le résultat énoncé. □

Remarque 1.15. Compte tenu de sa définition (Déf. 1.13), l'extension $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ de K est indépendante de l'ordre dans lequel sont faites les adjonctions des α_i, $1 \leq i \leq n$. On a, en particulier

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2) = K(\alpha_2)(\alpha_1).$$

Exemple 1.16. 1) $\mathbb{C} = \{a+bi; (a,b) \in \mathbb{R} \times \mathbb{R}, i^2 = -1\} = \mathbb{R}(i)$.

2) $\{p+qi; (p,q) \in \mathbb{Q} \times \mathbb{Q}, i^2 = -1\} = \mathbb{Q}(i)$.

3) $\{p+q\sqrt{2}; (p,q) \in \mathbb{Q} \times \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$.

Remarque 1.17. Les exemples ci-dessus sont des extensions simples, car du type $K(\alpha)$; de plus, dans chacun des cas considérés, tout élément de $K(\alpha)$ s'exprime linéairement sur K en fonction de α. Ces exemples sont des *cas particuliers* d'extensions simples, comme le montre le résultat général suivant.

Proposition 1.18. *Soit L une extension d'un corps K; alors, pour tout $\alpha \in L$ on a*

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} ; \frac{f(X)}{g(X)} \in K(X), g(\alpha) \neq 0 \right\}, \tag{1.1}$$

où $K(X)$ désigne le corps des fractions rationnelles à coefficients dans K.
Plus généralement, $K(X_1, X_2, \ldots, X_n)$ étant le corps des fractions rationnelles à n indéterminées sur K, pour $\alpha_1, \alpha_2, \ldots, \alpha_n$, dans $L, n > 1$, dans $\mathbb{N}$, on a

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)} \right\}, \tag{1.2}$$

$$\text{où} \quad \frac{f(X_1, X_2, \ldots, X_n)}{g(X_1, X_2, \ldots, X_n)} \in K(X_1, X_2, \ldots, X_n) \text{ et } g(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0.$$

Démonstration. On vérifie facilement que l'ensemble écrit au second membre de la relation (1.1) est un sous-corps de L contenant K et α, donc contenant le corps $K(\alpha)$.
D'autre part, dans L, tout élément $\dfrac{f(\alpha)}{g(\alpha)}$, où $\dfrac{f(X)}{g(X)} \in K(X), g(\alpha) \neq 0$, appartient nécessairement au corps $K(\alpha)$, d'où l'égalité (1.1).
De la même façon, on démontre la relation (1.2). □

Remarque 1.19. a) Il existe des extensions de corps qui ne sont ni simples, ni obtenues par l'adjonction d'un nombre fini d'éléments, par exemple l'extension $\mathbb{R} : \mathbb{Q}$, ce que l'on justifiera plus loin.
b) Une extension simple peut éventuellement se présenter sous une forme qui ne met pas directement en évidence sa simplicité.
Montrons, par exemple, que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
On a d'une part,

$$\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \Longrightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

D'autre part, vérifions que $\sqrt{2}$ et $\sqrt{3}$ appartiennent à $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \Longrightarrow \sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$
$$\sqrt{6}(\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2} = 2(\sqrt{2} + \sqrt{3}) + \sqrt{3},$$

d'où $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$; on en déduit que $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ et par suite

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Définition 1.20. On dira qu'un corps K' est un **corps intermédiaire** pour une extension $L : K$, si $K \subseteq K' \subseteq L$.

3. Degré d'une extension de corps

Etant donné une extension de corps $L : K$, en supposant $K \subseteq L$ (Rem. 1.9, b)), on considère le corps L comme un espace vectoriel sur K.
On rappelle que tout espace vectoriel a au moins une base ([26]) et que toutes les bases ont le même cardinal.
Notation : Le cardinal d'une base d'une extension $L : K$ est noté $[L : K]$.

Définition 1.21. Compte tenu des hypothèses ci-dessus, $[L : K]$ est appelé **degré** de l'extension $L : K$ (ou **degré** de L sur K).
Si L est de dimension finie sur K, on dit que L est une extension de **degré fini** sur K et $[L : K] = dim_K L$.
Si L est de dimension infinie sur K, on dit que L est une extension de **degré infini** sur K.

On remarque que $L = K \iff [L : K] = 1$.

Théorème 1.22. *Quelles que soient les extensions de corps $L : K$ et $M : L$, on a*

$$[M : K] = [M : L][L : K]. \tag{1.3}$$

Démonstration. On suppose $K \subseteq L \subseteq M (Rem.\ 1.9, b))$.
Soit $\{x_i\}_{i\in I}$ une base de L sur K et $\{y_j\}_{j\in J}$ une base de M sur L, où I et J sont des ensembles non vides.
Montrons que $\{x_i y_j\}_{(i,j)\in I\times J}$ est une base de M sur K.
Soit $z \in M ; z = \sum_{j\in J} \alpha_j y_j$, où les α_j sont des éléments de L, nuls, sauf un nombre fini d'entre eux (ce que l'on exprime aussi, en disant que les α_j sont presque tous nuls dans L).
Pour tout $j \in J$, $\alpha_j = \sum_{i\in I} \beta_{ij} x_i$, les éléments β_{ij} étant presque tous nuls dans K ; alors

$$z = \sum_{(i,j)\in I\times J} \beta_{ij} x_i y_j, \text{ les } \beta_{ij} \text{ étant presque tous nuls dans } K.$$

On en déduit que la famille $\{x_i y_j\}_{(i,j)\in I\times J}$ est une partie génératrice de l'espace vectoriel M sur K ; montrons que c'est aussi une partie libre sur K.
Supposons $\sum_{(i,j)\in I\times J} c_{ij} x_i y_j = 0$, les c_{ij} étant presque tous nuls dans K.
On peut alors écrire

$$\sum_{j\in J} (\sum_{i\in I} c_{ij} x_i) y_j = 0.$$

Or $\{y_j\}_{j\in J}$ est une base de M sur L et pour tout $j \in J$, $\sum_{i\in I} c_{ij} x_i \in L$; par suite,

$$\sum_{i\in I} c_{ij} x_i = 0, \forall j \in J \Longrightarrow c_{ij} = 0, \forall (i,j) \in I \times J,$$

puisque $\{x_i\}_{i\in I}$ est une base de L sur K.
Ainsi la famille $\{x_i y_j\}_{(i,j)\in I\times J}$ est une partie libre et génératrice du K-espace vectoriel M, c'est donc une base de M sur K.
D'autre part, d'après la théorie des ensembles ([8]), on a

$$card(I \times J) = card(I) \times card(J);$$

on en déduit la relation (1.3). □

Remarque 1.23. a) On écrira souvent $[L : K] < \infty$, pour exprimer que l'extension $L : K$ est de *degré fini*.
b) Dans la relation (1.3),

$$[M : K] < \infty \Longrightarrow [M : L] < \infty \text{ et } [L : K] < \infty.$$

D'une façon générale, si deux des degrés qui figurent dans la relation (1.3) sont finis, le troisième est fini et dans ce cas, les entiers $[M : L]$ et $[L : K]$ divisent l'entier $[M : K]$.

Du théorème 1.22, on déduit facilement le résultat suivant.

Corollaire 1.24. *Soit $L : K$ une extension de corps, de degré fini ; si $\{K_i\}_{1\leq i\leq r}$, $r \geq 1$, est une famille finie, totalement ordonnée, de corps intermédiaires* (Déf. 1.20), *alors*

$$K \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_r \subseteq L \quad \textit{implique}$$

$$[L : K] = [L : K_r][K_r : K_{r-1}] \ldots [K_1 : K].$$

Remarque 1.25. Soit $L : K$ une extension d'un corps et $B = \{x_i\}_{i\in I}$ une base de L sur K ; alors L peut toujours être considéré comme *obtenu par l'adjonction de B à K*.
En effet, $B \subseteq L$ et $K \subseteq L$, donc l'extension $K(B)$, obtenue par l'adjonction de B à K, est un sous-corps de L. D'autre part, tout $x \in L$ s'écrit, de façon unique,

$$x = \sum_{i\in I} \alpha_i x_i, \text{ les } \alpha_i \text{ étant presque tous nuls dans } K.$$

Par suite, tout élément de L est dans $K(B)$, on en conclut que $L = K(B)$.
En particulier, si $[L : K] = n \in \mathbb{N}^*$ et si $\{x_i\}_{1\leq i\leq n}$ est une *base* de L sur K, alors

$$L = K(x_1, x_2, \ldots, x_n).$$

4. Isomorphismes d'extensions de corps

Rappels : a) Deux corps K et F sont dits isomorphes s'il existe un isomorphisme d'anneaux unitaires de K sur F.
b) Etant donné un corps K, une extension $L : K$ est définie par la donnée d'un couple (L, u), où u est un plongement de K dans L.

Définition 1.26. Soit K et F deux corps *isomorphes*. On dira que les **extensions** $L : K$ et $M : F$, respectivement définies par les couples (L, u) et (M, v), sont **isomorphes**, s'il existe un couple d'isomorphismes (λ, μ), respectivement, de K sur F et L sur M, tel que le diagramme suivant commute :

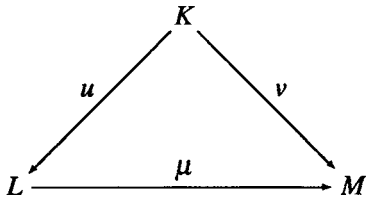
$$\begin{array}{ccc} K & \xrightarrow{\lambda} & F \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle v} \\ L & \xrightarrow{\mu} & M \end{array}$$

c'est-à-dire $\mu \circ u = v \circ \lambda$.
On dit alors, que le couple (λ, μ) est un **isomorphisme d'extensions de corps** de $L : K$ sur $M : F$.

Cas particuliers :
1) Si $K \subseteq L$ et $F \subseteq M$, u et v étant alors, respectivement, les injections canoniques de K dans L et F dans M, on a

$$\mu \circ u = v \circ \lambda \iff \mu_{/K} = \lambda.$$

2) Si $K = F$ et $\lambda = id_K$, le diagramme commutatif devient :



d'où $\mu \circ u = v$.
Si de plus, u et v sont les injections canoniques, alors

$$\mu \circ u = v \iff \mu_{/K} = id_K$$

et dans ce cas, on dit que μ est un **K-isomorphisme** de L sur M.
Les corps L et M sont alors **K-isomorphes** (dans certains ouvrages, on dit que les corps L et M sont *conjugués* sur K).

5. Exercices

1. Soit $K = \{0, 1, \alpha, \beta\}$ un ensemble de quatre éléments distincts, muni d'une addition et d'une multiplication, respectivement définies par les tables suivantes :

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

×	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Vérifier que K est un corps. Quelle est la caractéristique de K?
Δ désignant le sous-corps premier de K, quel est le degré de K sur Δ? Montrer que $K = \Delta(\alpha) = \Delta(\beta)$.

2. Un corps de cardinal infini peut-il contenir un sous-corps fini ?

3. Etant donné $\alpha \in \mathbb{C}$, que peut-on dire de l'extension $\mathbb{R}(\alpha)$ de $\mathbb{R}$?

4. Déterminer les sous-corps de $\mathbb{C}$, respectivement engendrés par :

$$\{0,1\}; \quad \{0\}; \quad \{i, \sqrt{2}\}; \quad \{\sqrt{2}, \sqrt{3}\}; \quad \mathbb{R}.$$

5. Soit A un domaine d'intégrité. On suppose que A contient un sous-corps F.
1°) Vérifier que A est un F-espace vectoriel.
2°) On suppose A de *dimension finie* sur F.
Soit $a \neq 0$ dans A ; montrer que l'application

$$t_a : A \longrightarrow A \text{ telle que } t_a(x) = ax, \text{ quel que soit } x \in A,$$

est un F-automorphisme de A.
En déduire que A est un corps.

6. Soit L une extension d'un corps K telle que $[L:K] = p \in \mathbb{N}^*$.
Montrer que si p est un nombre premier, alors L est une extension simple de K.

7. K étant un corps, on considère le groupe multiplicatif K^* et, quel que soit $n \in \mathbb{N}^*$, l'application

$$\begin{aligned} \phi_n : K^* &\longrightarrow K^* \\ x &\longmapsto x^n. \end{aligned}$$

1°) a) Vérifier que ϕ_n est un endomorphisme du groupe K^* et que

$$\phi_n \text{ est un automorphisme } \Longleftrightarrow K^* = K^{*n},$$

où $K^{*n} = \{x^n ; x \in K^*\}$.
b) Soit H un sous-groupe du groupe K^*; montrer que

$$\phi_n(H) = K^* \Longrightarrow H = K^*.$$

2°) Si $K = \mathbb{R}$, pour quelles valeurs de $n \in \mathbb{N}^*$, l'endomorphisme ϕ_n est-il un automorphisme du groupe $\mathbb{R}^*$?

8. Soit A un anneau unitaire ; une application $\partial : A \longrightarrow A$ est appelée une **dérivation** de A, si quels que soient a et b dans A,

$$\begin{aligned} &i) \quad \partial(a+b) = \partial(a) + \partial(b); \\ &ii) \quad \partial(ab) = a\partial(b) + \partial(a)b. \end{aligned}$$

1°) ∂ étant une dérivation d'un anneau unitaire A, calculer $\partial(0)$ et $\partial(1)$.
Vérifier que l'application nulle de A est une dérivation, que l'on appellera la *dérivation nulle* de A.
2°) Si K est un corps, vérifier que l'application

$$\begin{aligned} K[X] &\longrightarrow K[X] \\ f(X) &\longmapsto f'(X), \end{aligned}$$

où $f'(X)$ est le polynôme dérivé de $f(X)$, est une dérivation de l'anneau $K[X]$.
3°) A étant un anneau unitaire et commutatif, on pose

$$M(A) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \quad ; \quad (a,b) \in A \times A \right\}.$$

a) Vérifier que $M(A)$ est un sous-anneau unitaire de l'anneau $\mathcal{M}_2(A)$ des matrices carrées d'ordre 2 sur A.
b) Etant donné une application $\partial : A \longrightarrow A$, on considère

$$\begin{aligned} \mu : A &\longrightarrow M(A) \\ a &\longmapsto \begin{pmatrix} a & \partial(a) \\ 0 & a \end{pmatrix}. \end{aligned}$$

Démontrer que ∂ est une dérivation de A si et seulement si μ est un morphisme d'anneaux unitaires.

4°) On suppose que A est un domaine d'intégrité ([13], Déf. 1.21.) et on note F son corps de fractions ([13], Déf. 5.2.).
Etant donné une dérivation ∂ de A, on considère l'application

$$\lambda : A \longrightarrow M(F)$$
$$a \longmapsto \begin{pmatrix} a & \partial(a) \\ 0 & a \end{pmatrix}.$$

On note ε l'injection canonique de A dans F.
a) Prouver qu'il existe un unique morphisme d'anneaux unitaires
$\mu : F \longrightarrow M(F)$ tel que $\mu \circ \varepsilon = \lambda$.
En déduire qu'il existe une unique dérivation $\overline{\partial}$ de F qui prolonge ∂ (c'est-à-dire que $\overline{\partial}_{/A} = \partial$).
b) Pour tout $\frac{a}{s} \in F$, expliciter l'expression de $\overline{\partial}(\frac{a}{s})$ en fonction de $\partial(a)$ et $\partial(s)$.

9. *Construction de* $\mathbb{R}$ *à partir des suites de Cauchy de* $\mathbb{Q}$ (Voir un cours de 1^{er} cycle).
Rappel de définitions : $\mathbb{Q}_+^*$ désigne l'ensemble des nombres rationnels strictement positifs.
a) Une suite $u = (u_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ **converge** dans $\mathbb{Q}$ et $\lim_{n\to\infty} = a \in \mathbb{Q}$,
si $\quad \forall \varepsilon \in \mathbb{Q}_+^*, \exists N_\varepsilon \in \mathbb{N}\ t.q.\ n \geq N_\varepsilon \Longrightarrow | u_n - a | \leq \varepsilon.$
b) Une suite $u = (u_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ est une **suite de Cauchy** de $\mathbb{Q}$, si
$\forall \varepsilon \in \mathbb{Q}_+^*, \exists N_\varepsilon \in \mathbb{N}\ t.q.\ (m \geq N_\varepsilon, n \geq N_\varepsilon) \Longrightarrow | u_n - u_m | \leq \varepsilon.$
c) Une suite $u = (u_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ est dite **bornée** dans $\mathbb{Q}$, s'il existe $M \geq 0$ dans $\mathbb{Q}$ tel
$| u_n | \leq M, \quad \forall n \in \mathbb{N}.$
1°) a) Prouver que toute suite $u = (u_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ convergente dans $\mathbb{Q}$ est une suite de Cauchy de $\mathbb{Q}$.
La réciproque est fausse : voir 3°), c).
b) Montrer que toute suite de Cauchy de $\mathbb{Q}$ est bornée dans $\mathbb{Q}$.
2°) Soit $\mathcal{C}$ l'ensemble des suites de Cauchy de $\mathbb{Q}$; on a $\mathcal{C} \subset \mathbb{Q}^{\mathbb{N}}$.
a) Montrer que, quels que soient $u = (u_n)_{n\in\mathbb{N}}$ et $v = (v_n)_{n\in\mathbb{N}}$ dans $\mathcal{C}$, on a
$u + v := (u_n + v_n)_{n\in\mathbb{N}} \in \mathcal{C}$ et $uv := (u_n v_n)_{n\in\mathbb{N}} \in \mathcal{C}$.
En déduire que $\mathcal{C}$ est muni d'une structure d'anneau unitaire commutatif, dont on précisera l'élément nul et l'élément unité.
b) Prouver que l'ensemble $\mathcal{C}_0$ des suites de Cauchy de $\mathbb{Q}$ qui convergent vers 0 forme un idéal de l'anneau $\mathcal{C}$ ([13], Déf. 1.42).
3°) a) Démontrer que l'anneau quotient ([13], Déf. 2.27) $\mathcal{C}/\mathcal{C}_0$ est un corps. Ce corps est appelé **corps des nombres réels.**
b) En identifiant tout élément $q \in \mathbb{Q}$ à la suite constante égale à q, montrer que $\mathbb{Q}$ s'identifie à un sous-corps de $\mathbb{R}$.
c) Démontrer que la suite $u = (u_n)_n$ telle que $\forall\, n \in \mathbb{N}$, $u_n = \frac{1}{n!}$ est une suite de Cauchy *non convergente* dans $\mathbb{Q}$.
En conclure que le nombre réel e défini par la suite $(\frac{1}{n!})_{n\in\mathbb{N}}$ n'est pas un nombre rationnel ; on dit que e est **irrationnel.**
e est *le nombre de Néper.*

Chapitre 2
Extensions algébriques - Extensions transcendantes

Les notions de *racine* et *d'ordre de multiplicité d'une racine* d'un polynôme à une indéterminée sur un corps K sont supposées connues, ainsi que les propriétés de l'anneau $K[X]$ ([13], Ch. 4 et 5).

Remarque 2.1. Si $L : K$ est une extension de corps telle que $K \subseteq L$, alors tout polynôme de $K[X]$ peut être considéré comme un polynôme de $L[X]$.

1. Elément algébrique, élément transcendant

Définition 2.2. Soit L une extension d'un corps K, α un élément de L et $K(\alpha)$ l'extension de K obtenue par l'adjonction de α.
1) L'élément α est dit **algébrique sur** K, s'il existe un polynôme *non constant* $f(X)$, dans $K[X]$, tel que $f(\alpha) = 0$.
Dans ce cas, on dit que $K(\alpha)$ est une extension **simple, algébrique** de K.
2) L'élément α est dit **transcendant sur** K, si α n'est pas algébrique sur K, donc, si

$$\forall f(X) \in K[X] \setminus K,\ f(\alpha) \neq 0.$$

On dit alors que $K(\alpha)$ est une extension **simple, transcendante** de K.

Remarque 2.3. Les notations étant celles de la définition 2.2,
a) Tout élément α de K est algébrique sur K, puisqu'il est racine du polynôme $X - \alpha$.
b) Si α est algébrique sur K, alors α est algébrique sur tout corps F contenant K, puisque tout polynôme de $K[X]$ est un polynôme de $F[X]$.
c) $\alpha \neq 0$ dans L est algébrique sur K si et seulement s'il existe un nombre fini d'éléments dans K, $a_0, a_1, \ldots, a_n (n \geq 1)$ tels que $a_0 \neq 0$, les a_i non tous nuls, pour $1 \leq i \leq n$, et

$$\sum_{0 \leq i \leq n} a_i \alpha^i = 0.$$

Proposition 2.4. *Soit $L : K$ une extension de corps ; à tout $\alpha \in L$ on associe l'application*

$$\begin{aligned} \theta_\alpha : K[X] &\longrightarrow L \\ f(X) &\longmapsto f(\alpha). \end{aligned}$$

θ_α est un morphisme d'anneaux unitaires ; on pose $K[\alpha] := Im\,\theta_\alpha$; alors $K[\alpha]$ est un domaine d'intégrité et

$$\theta_\alpha \text{ est non injectif} \iff \alpha \text{ est algébrique sur } K. \tag{2.1}$$
$$\theta_\alpha \text{ est injectif} \iff \alpha \text{ est transcendant sur } K. \tag{2.2}$$

Démonstration. On vérifie facilement que θ_α est un morphisme d'anneaux unitaires ; $K[\alpha] = Im\,\theta_\alpha$ est un sous-anneau unitaire du corps L, c'est donc un domaine d'intégrité (D.I.).

$$\begin{aligned} \theta_\alpha \text{ non injectif} &\iff Ker\,\theta_\alpha \neq \{0\}, \\ &\iff \exists f(X) \in K[X] \setminus \{0\} \text{ tel que } f(\alpha) = 0, \\ &\iff \alpha \text{ algébrique sur } K. \end{aligned}$$

En prenant la contraposée de (2.1) on obtient le résultat (2.2), d'où

$$\alpha \text{ transcendant sur } K \iff K[\alpha] \simeq K[X]. \qquad \square$$

2. Extensions simples, transcendantes

Théorème 2.5. *Toute extension simple, transcendante $K(\alpha) : K$ est K-iso-morphe à l'extension $K(X) : K$, où $K(X)$ est le corps des fractions rationnelles à une indéterminée sur K.*
Plus précisément, il existe un isomorphisme μ de $K(X)$ sur $K(\alpha)$ tel que

$$\mu_{/K} = id_K \text{ et } \mu(X) = \alpha.$$

Démonstration. Par hypothèse, quel que soit $f(X) \in K[X] \setminus K$, on a $f(\alpha) \neq 0$. Or, d'après la proposition 1.18,

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} ; \frac{f(X)}{g(X)} \in K(X), g(\alpha) \neq 0 \right\};$$

par suite, l'hypothèse implique

$$K(\alpha) = \{q(\alpha) ; q(X) \in K(X)\}.$$

On vérifie alors facilement, que l'application

$$\begin{aligned} \mu : K(X) &\longrightarrow K(\alpha) \\ q(X) &\longmapsto q(\alpha) \end{aligned}$$

définit un isomorphisme du corps $K(X)$ sur le corps $K(\alpha)$, vérifiant $\mu_{/K} = id_K$ et $\mu(X) = \alpha$. $\square$

Corollaire 2.6. *Deux extensions simples, transcendantes d'un corps K sont K-isomorphes.*

Ce résultat est une conséquence directe du Th. 2.5.

Proposition 2.7. *Si $K(\alpha)$ est une extension simple transcendante d'un corps K, alors $K(\alpha)$ est le corps des fractions du domaine d'intégrité $K[\alpha]$* (Cf. Prop. 2.4).

Démonstration. L'élément α étant *transcendant* sur K, d'après la Prop. 2.4 et le Th. 2.5 on a

$$\begin{aligned} K[\alpha] &= \{f(\alpha) ; f(X) \in K[X]\} \simeq K[X]; \\ K(\alpha) &= \{q(\alpha) ; q(X) \in K(X)\} \simeq K(X). \end{aligned}$$

Or $K(X)$ est le corps des fractions du domaine d'intégrité $K[X]$ ([13], Ch. 5), on en déduit que $K(\alpha)$ est le corps des fractions du domaine d'intégrité $K[\alpha]$. $\square$

3. Extensions simples, algébriques

Rappel ([13], Ch. 4 et 5) : L'anneau $K[X]$ des polynômes à une indéterminée sur un corps K est *euclidien*, c'est donc un *domaine principal* (D.P.) et un anneau *factoriel*. De plus, pour tout idéal non nul I de $K[X]$, il existe un *unique* polynôme *unitaire* qui engendre I ([13], Cor. 4.37).

A. Caractérisation des extensions simples, algébriques

Théorème 2.8. *Etant donné une extension de corps $L : K$, si α est un élément de L, algébrique sur K, alors*
1) *Il existe un unique polynôme $p(X)$ unitaire et irréductible dans $K[X]$ tel que*

$$(f(X) \in K[X] \setminus \{0\} \text{ et } f(\alpha) = 0) \iff p(X) | f(X) \text{ dans } K[X]. \tag{2.3}$$

2) *L'extension simple $K(\alpha)$ vérifie l'égalité*

$$K(\alpha) = \{f(\alpha) ; f(X) \in K[X]\}. \tag{2.4}$$

3) $[K(\alpha) : K] = \deg p$.

Démonstration. 1) L'élément α étant fixé, considérons le morphisme θ_α défini dans la Prop. 2.4 et posons, pour cette démonstration, $\theta := \theta_\alpha$. On a

$$Ker\,\theta = \{f(X) \in K[X] ; f(\alpha) = 0\} \tag{2.5}$$
$$K[\alpha] := Im\,\theta = \{f(\alpha) ; f(X) \in K[X]\}. \tag{2.6}$$

$Ker\,\theta$ étant un idéal propre et non nul de $K[X]$ (Prop. 2.4), il existe un *unique* polynôme *unitaire* $p(X)$, non constant dans $K[X]$ qui engendre $Ker\,\theta$; on peut écrire $Ker\,\theta = (p(X))$. En appliquant le premier théorème d'isomorphisme relatifs aux anneaux unitaires, commutatifs ([13], Th. 2.34), on obtient

$$K[\alpha] \simeq \frac{K[X]}{(p(X))}. \tag{2.7}$$

$K[\alpha]$ est un domaine d'intégrité (Prop. 2.4)), par suite $p(X)$ est un élément *premier*, donc *irréductible* dans l'anneau factoriel $K[X]$ ([13], Ch. 5) ; alors

$$(f(X) \in Ker\,\theta\,(= (p(X))) \text{ et } f(X) \neq 0) \iff p(X) | f(X) \text{ dans } K[X]. \tag{2.8}$$

2) $K[X]$ étant un D.P., l'idéal premier, non nul, $Ker\,\theta = (p(X))$ est *maximal* ([13], Th. 2.66), par suite, l'isomorphisme (2.7) implique que $K[\alpha]$ est un corps, donc un sous-corps de L contenant K et α.
Or, par définition, l'extension simple $K(\alpha)$ est le plus petit sous-corps de L contenant K et α, d'où

$$K(\alpha) \subseteq K[\alpha].$$

D'autre part, pour tout $f(X)$ dans $K[X]$, on a $f(\alpha)$ dans $K(\alpha)$ (Prop. 1.18) ; on en déduit l'égalité

$$K(\alpha) = K[\alpha],$$

d'où le résultat 2) du théorème 2.8.

3) Posons $d := deg\, p$; dans $K[X] \setminus K$, $p(X)$ est le polynôme *unitaire, de plus petit degré* tel que $p(\alpha) = 0$ ([13], Cor. 4.37).
Il en résulte que, dans le K-espace vectoriel L, les éléments $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ sont linéairement indépendants.
En effet, puisqu'aucun polynôme de $K[X] \setminus K$, de degré strictement inférieur à d, n'est annulé par α, dans L, on a

$$(\sum_{0 \le i \le d-1} b_i \alpha^i = 0,\ b_i \in K, \forall i (0 \le i \le d-1)) \Longrightarrow (b_i = 0, \forall i (0 \le i \le d-1)).$$

D'autre part, soit $f(X)$ un polynôme de $K[X]$, tel que $f(\alpha) \neq 0$. La division euclidienne de $f(X)$ par $p(X)$ dans $K[X]$ ([13], Th. 4.33) entraîne l'existence de $q(X)$ et $r(X)$, uniques dans $K[X]$, tels que

$$f(X) = p(X)q(X) + r(X),\ deg\, r < deg\, p.$$

En tenant compte du résultat 1) obtenu précédemment, on a

$$f(\alpha) \neq 0 \Longrightarrow p(X) \nmid f(X),\ \text{donc } r(X) \neq 0.$$
$$f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) \Longrightarrow f(\alpha) = r(\alpha),\ \text{alors}$$
$$deg\, r \le d-1 \Longrightarrow f(\alpha) = \sum_{0 \le i \le d-1} b_i \alpha^i,\ \text{où } b_i \in K, \forall i (0 \le i \le d-1).$$

Ainsi, dans le K-espace vectoriel $K(\alpha) = K[\alpha]$, $\{\alpha^i, 0 \le i \le d-1\}$ forme une famille libre et génératrice, donc une base, d'où

$$[K(\alpha) : K] = d = deg\, p. \qquad \square$$

Définition 2.9. Etant donné une extension de corps $L : K$ et un élément $\alpha \in L$, algébrique sur K, l'unique polynôme $p(X)$, unitaire et irréductible de $K[X]$, associé à α dans le Th.2.8 est appelé le **polynôme irréductible de α sur K**. On écrira

$$p(X) = Irr_K(\alpha, X) \quad ou \quad p = Irr_K(\alpha).$$

Remarque 2.10. Les hypothèses étant celles du Th. 2.8 :
a) Dans certains ouvrages, le polynôme $Irr_K(\alpha)$ est appelé le polynôme *minimal* de α sur K.
b) La preuve du Th. 2.8 montre que tout $x \in K(\alpha)$ s'écrit de façon unique

$$x = \sum_{0 \le i \le d-1} b_i \alpha^i,\ \text{où } b_i \in K,\ \forall i (0 \le i \le d-1).$$

Le théorème suivant constitue une réciproque du Th. 2.8.

Théorème 2.11. *K étant un corps, soit $p(X)$ un polynôme* unitaire *et* irréductible *de $K[X]$; il existe alors une extension simple $K(\alpha) : K$ telle que α est algébrique sur K et $Irr_K(\alpha, X) = p(X)$.*

Démonstration. $K[X]$ étant un anneau factoriel ([13], Ch. 5), le polynôme irréductible $p(X)$ est un élément premier, non nul, de $K[X]$ ([13], Th. 5.89).
Mais $K[X]$ étant de plus un D.P. ([13], Th. 4.36), l'idéal premier, non nul, $(p(X))$ est *maximal* dans $K[X]$ ([13], Th. 2.66), par suite ([13], Th. 2.62),

$$F := \frac{K[X]}{(p(X))} \text{ est un corps.}$$

Soit u l'injection canonique de K dans $K[X]$ et π la surjection canonique de $K[X]$ sur F. $\pi \circ u$ est un morphisme d'anneaux unitaires de K dans F, donc un monomorphisme de K dans F. On en déduit que F est une extension de K telle que tout $a \in K$ peut être identifié à son image par $\pi \circ u$.
Dans F, posons $\alpha := \pi(X)$; alors

$$F = \{\pi(f(X)) ; f(X) \in K[X]\} = \{f(\alpha) ; f(X) \in K[X]\} \tag{2.9}$$

De plus, $\pi(p(X)) = 0 \Longrightarrow p(\alpha) = 0$,
donc l'élément α de F est *algébrique* sur K.
Compte tenu du Th. 2.8, la relation (2.9) implique $F = K(\alpha)$; ainsi F est une extension simple, algébrique de K et le polynôme $p(X)$ étant, par hypothèse, unitaire et irréductible dans $K[X]$,

$$p(\alpha) = 0 \Longrightarrow p(X) = Irr_K(\alpha, X). \qquad \square$$

Les théorèmes 2.8 et 2.11 ont pour conséquence le résultat suivant.

Corollaire 2.12. *Toute extension simple, algébrique d'un corps K est isomorphe à un corps de la forme $\dfrac{K[X]}{(p(X))}$, où $p(X)$ est un polynôme unitaire et irréductible de $K[X]$.*

B. Exemples d'extensions simples, algébriques

Exemple 2.13. $\mathbb{C} = \mathbb{R}(i)$ (Exemple 1.16) ; on a $Irr_K(i, X) = X^2 + 1$, donc $[\mathbb{C} : \mathbb{R}] = 2$ et $\mathbb{C} \simeq \dfrac{\mathbb{R}[X]}{(X^2+1)}$.
$[\mathbb{C} : \mathbb{R}] = 2$ implique que tout $z \in \mathbb{C}$ s'écrit de façon unique $z = a + bi$, où a, b sont dans $\mathbb{R}$.

Exemple 2.14. Soit $p(X) := X^3 - 2$ dans $\mathbb{Q}[X]$. On sait que le polynôme $p(X)$ est irréductible sur $\mathbb{Q}$; $\sqrt[3]{2}$ étant la racine cubique réelle de 2, on a

$$Irr_K(\sqrt[3]{2}, X) = X^3 - 2, \quad \mathbb{Q}(\sqrt[3]{2}) \simeq \frac{\mathbb{Q}[X]}{(X^3-2)} \quad \text{et} \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 ;$$

par suite, tout élément $x \in \mathbb{Q}(\sqrt[3]{2})$ s'écrit de façon unique :

$$x = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2,\ a, b, c \text{ dans } \mathbb{Q}.$$

Exemple 2.15. Soit $p(X) = X^2 + X + 1$ dans $\mathbb{Q}[X] \subset \mathbb{R}[X]$. Le polynôme $p(X)$ est irréductible sur $\mathbb{Q}$ et sur $\mathbb{R}$; ses racines dans $\mathbb{C}$ sont $\dfrac{-1 \pm i\sqrt{3}}{2}$, où $i^2 = -1$. Ce sont les racines cubiques complexes de 1, notées j et j^2 ; alors,

$$\mathbb{Q}(j) = \mathbb{Q}(j^2) \subsetneq \mathbb{C}, \quad \mathbb{Q}(j) \simeq \frac{\mathbb{Q}[X]}{(X^2+X+1)}, \quad [\mathbb{Q}(j) : \mathbb{Q}] = 2,$$

d'où $\mathbb{Q}(j) \simeq \mathbb{Q}(i)$;cependant, $\mathbb{Q}(j) = \{a + bj ;\ a, b \text{ dans } \mathbb{Q}\} \neq \mathbb{Q}(i)$.

$$\mathbb{R}(j) = \mathbb{R}(j^2) \simeq \frac{\mathbb{R}[X]}{(X^2+X+1)} ;\ [\mathbb{R}(j) : \mathbb{R}] = 2 \Longrightarrow \mathbb{R}(j) = \mathbb{R}(i) = \mathbb{C}.$$

C. Extensions simples, algébriques, isomorphes

Théorème 2.16. *Soit $L : K$ une extension de corps et α, β des éléments de L, algébriques sur K, tels que*

$$Irr_K(\alpha, X) = Irr_K(\beta, X);$$

alors les extensions $K(\alpha) : K$ et $K(\beta) : K$ sont isomorphes (Déf. 1.26).
Plus précisément, il existe un isomorphisme $\mu : K(\alpha) \longrightarrow K(\beta)$ tel que $\mu_{/K} = id_K$ et $\mu(\alpha) = \beta$.

Démonstration. Posons $p(X) := Irr_K(\alpha, X) = Irr_K(\beta, X)$; d'après la preuve du Th. 2.8, les corps $K(\alpha)$ et $K(\beta)$ sont K-isomorphes au corps $\frac{K[X]}{(p(X))}$, par suite les extensions $K(\alpha) : K$ et $K(\beta) : K$ sont isomorphes .
Posons $d = deg\, p$; tout $x \in K(\alpha)$ (resp. $y \in K(\beta)$) s'écrit de façon unique (Th. 2.8) :

$$x = \sum_{0 \leq i \leq d-1} a_i \alpha^i \quad (\text{resp.} \quad y = \sum_{0 \leq i \leq d-1} b_i \beta^i),$$

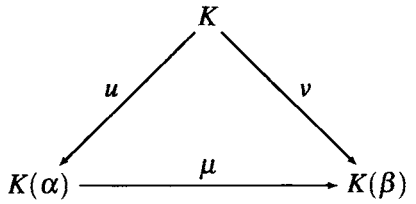
où pour tout $i\,(0 \leq i \leq d-1,)\, a_i$ et b_i sont dans K.
L'application

$$\mu : K(\alpha) \longrightarrow K(\beta)$$
$$\sum_{0 \leq i \leq d-1} a_i \alpha^i \longmapsto \sum_{0 \leq i \leq d-1} a_i \beta^i$$

est alors un morphisme d'anneaux unitaires, donc *injectif* ; la définition de μ implique sa *surjectivité*, par suite μ est un isomorphisme ; de plus,

$$\mu_{/K} = id_K \quad et \quad \mu(\alpha) = \beta. \qquad \square$$

Remarque 2.17. En notant, respectivement, u et v les injections canoniques de K dans $K(\alpha)$ et $K(\beta)$, le Th. 2.16 exprime que le diagramme suivant commute :



Définition 2.18. Etant donnés des éléments α et β appartenant à une extension d'un corps K et algébriques sur K, on dira que α et β sont **conjugués** sur K, si

$$Irr_K(\alpha) = Irr_K(\beta).$$

Exemple 2.19. On considère le polynôme $p(X) = X^3 - 2$, unitaire et irréductible sur $\mathbb{Q}$ (Exemple 2.13).
Ses racines $\sqrt[3]{2} \in \mathbb{R}$, $j\sqrt[3]{2}$, et $j^2\sqrt[3]{2}$, où $j^3 = 1$ dans $\mathbb{C}$, sont deux à deux conjuguées sur $\mathbb{Q}$ (Déf. 2.18).
Les trois extensions simples de $\mathbb{Q}$, obtenues par l'adjonction de chacune des racines de $p(X)$, sont deux à deux $\mathbb{Q}$-isomorphes (Th. 2.16). On note cependant que $\mathbb{Q}(\sqrt[3]{2})$ est un sous-corps de $\mathbb{R}$, alors que $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$ sont dans $\mathbb{C}$ et de plus

$$j^3 = 1 \Longrightarrow \mathbb{Q}(j\sqrt[3]{2}) = \mathbb{Q}(j^2\sqrt[3]{2}).$$

Remarque 2.20. D'après le Th. 2.16, si des éléments α et β sont conjugués sur un corps K (Déf. 2.18.), alors les extensions simples $K(\alpha)$ et $K(\beta)$ sont K-isomorphes, mais la réciproque de cette propriété est fausse (Voir Exemple 2.15 et les Ex. **4.**, **5.**, **6.** de ce chapitre).

La définition suivante est justifiée par les théorèmes 2.11 et 2.16.

Définition 2.21. K étant un corps et $p(X)$ un polynôme *irréductible* et *unitaire* de $K[X]$, on appellera **corps de rupture** de $p(X)$ sur K, toute extension simple $K(\alpha)$ de K telle que $Irr_K(\alpha,X) = p(X)$.

Remarque 2.22. :
a) Un corps de rupture d'un polynôme irréductible et unitaire de $K[X]$ est défini à un K-isomorphisme près (Cf. Th. 2.11 et 2.16).
b) Etant donné un polynôme $q(X)$, *irréductible* de $K[X]$, on pourra toujours supposer qu'il est *unitaire*.
En effet, si $q(X)$ a un coefficient directeur $a \neq 1$, comme a est non nul, il est inversible dans K et le polynôme $p(X) = a^{-1}q(X)$ est unitaire et irréductible sur K ; de plus, pour α appartenant à une extension de K, on a

$$p(\alpha) = 0 \iff q(\alpha) = 0.$$

Rappel ([13], Ch. 4) : Pour une extension de corps $L : K$, tout plongement $\lambda : K \longrightarrow L$ se prolonge en un morphisme *injectif* d'anneaux unitaires $\hat{\lambda}$ tel que

$$\begin{aligned} \hat{\lambda} : K[X] &\longrightarrow L[X] \\ \sum_{0\leq i\leq n} a_i X^i &\longmapsto \sum_{0\leq i\leq n} \lambda(a_i)X^i \end{aligned}$$

De plus, si λ est un isomorphisme, il en est de même pour $\hat{\lambda}$.

Le théorème suivant généralise le théorème 2.16.

Théorème 2.23. *Soit $L : K$ et $L' : K'$ des extensions de corps, où l'on suppose que K et K' sont isomorphes.*
Etant donné un isomorphisme λ de K sur K', si $\alpha \in L$ et $\beta \in L'$ sont, respectivement, algébriques sur K et sur K' et tels que

$$\hat{\lambda}(Irr_K(\alpha,X)) = Irr_{K'}(\beta,X),$$

alors les extensions $K(\alpha) : K$ et $K'(\beta) : K'$ sont isomorphes et il existe un isomorphisme μ de $K(\alpha)$ sur $K'(\beta)$ tel que

$$\mu_{/K} = \lambda \ \text{ et } \ \mu(\alpha) = \beta.$$

Démonstration. Soit u et v les injections canoniques, respectivement, de K dans $K(\alpha)$ et de K' dans $K'(\beta)$.
λ étant un isomorphisme de K sur K', $\hat{\lambda}$ est un isomorphisme de $K[X]$ sur $K'[X]$, par suite les polynômes $Irr_K(\alpha,X)$ et $Irr_{K'}(\beta,X)$ ont le même degré, que l'on notera d ; on vérifie alors, que l'application

$$\begin{aligned} \mu : K(\alpha) &\longrightarrow K'(\beta) \\ \sum_{0\leq i\leq d-1} a_i\alpha^i &\longmapsto \sum_{0\leq i\leq d-1} \lambda(a_i)\beta^i \end{aligned}$$

est un isomorphisme tel que $\mu_{/K} = \lambda$ et $\mu(\alpha) = \beta$. □

Remarque 2.24. a) En prenant $K' = K$ et $\lambda = id_{/K}$ dans le Th. 2.23, on retouve le Th. 2.16.
b) Compte tenu du Th. 2.23, si u et v sont les injections canoniques, respectivement, de K dans $K(\alpha)$ et de K' dans $K'(\beta)$, alors le diagramme suivant commute.

$$\begin{array}{ccc} K & \xrightarrow{\lambda} & K' \\ \downarrow u & & \downarrow v \\ K(\alpha) & \xrightarrow{\mu} & K'\beta) \end{array}$$

4. Extensions algébriques, extensions transcendantes

Définition 2.25. Une **extension** L d'un corps K est dite **algébrique** sur K, si tout élément de L est algébrique sur K (Déf. 2.2).

Dans ce cas, on dit que l'extension $L : K$ est algébrique.

Théorème 2.26. *Toute extension L de* degré fini *sur un corps K est algébrique sur K.*

Démonstration. Posons $[L : K] = n \in \mathbb{N}^*$ et soit $\alpha \in L$.
Dans le cas où $\alpha \in K$, alors α est algébrique sur K (Rem. 2.3).
Supposons $n > 1$ et $\alpha \in L \setminus K$; l'ensemble $\{\alpha^i ; i \in \mathbb{N}\}$ forme nécessairement une famille liée dans le K-espace vectoriel L ; par suite il existe un entier $r > 1$ et des éléments $a_i, 0 \leq i \leq r$, non tous nuls dans K tels que

$$\sum_{0 \leq i \leq r} a_i \alpha^i = 0.$$

L'élément α est donc algébrique sur K (Rem. 2.3). □

Corollaire 2.27. *Toute extension simple, algébrique d'un corps K* (Déf. 2.2) *est une extension algébrique de K.*

Démonstration. Si $K(\alpha)$ est une extension simple, algébrique de K, alors $K(\alpha)$ est de degré fini sur K (Th. 2.8), donc est une extension algébrique de K (Th. 2.26). □

Remarque 2.28. La réciproque du Th. 2.26 est fausse (Voir Ex. **14.** à la fin du chapitre).

Théorème 2.29. *Une extension $L : K$ est algébrique et de degré fini si et seulement si L est obtenu par l'adjonction à K d'un nombre fini d'éléments algébriques sur K.*

Démonstration. Supposons L algébrique sur K et $[L : K] = n \in \mathbb{N}^*$. Soit $\{x_1, x_2, \ldots, x_n\}$ une base de L sur K ; alors, d'après la Rem. 1.25, on a $L = K(x_1, x_2, \ldots, x_n)$ et l'extension $L : K$ étant algébrique, chaque $x_i, 1 \leq i \leq n$, est algébrique sur K.
Réciproquement, considérons $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, où $n \in \mathbb{N}^*$ et chaque α_i, $1 \leq i \leq n$, est algébrique sur K.
D'après la Prop. 1.14, L peut être obtenu par les adjonctions successives des $\alpha_i, 1 \leq i \leq n$.

$$\begin{aligned} \alpha_1 \text{ algébrique sur } K &\Longrightarrow [K(\alpha_1) : K] < \infty. \\ \alpha_2 \text{ algébrique sur } K &\Longrightarrow \alpha_2 \text{ algébrique sur } K(\alpha_1) \\ &\Longrightarrow [K(\alpha_1, \alpha_2) : K(\alpha_1)] < \infty. \end{aligned}$$

Raisonnons alors, par récurrence sur n, en supposant, pour tout $i(2 \leq i \leq n-1)$,

$$[K(\alpha_1,\ldots,\alpha_i) : K(\alpha_1,\ldots,\alpha_{i-1})] < \infty;$$

$$\text{alors, } \alpha_n \text{ algébrique sur } K \Longrightarrow \alpha_n \text{ algébrique sur } K(\alpha_1,\ldots,\alpha_{n-1}),$$

$$\text{d'où} \quad [K(\alpha_1,\ldots,\alpha_n) : K(\alpha_1,\ldots,\alpha_{n-1})] < \infty;$$

et en appliquant le Cor. 1.24, on obtient :

$$[L : K] = [K(\alpha_1,\ldots,\alpha_n) : K(\alpha_1,\ldots,\alpha_{n-1})]\ldots[K(\alpha_1) : K] < \infty. \quad \square$$

Théorème 2.30. *Soit $L : K$ une extension de corps de* degré fini *; alors L est une extension* simple *de K, si et seulement si l'extension $L : K$ n'a qu'un nombre fini de corps intermédiaires* (Déf. 1.20).

Démonstration. 1^{er} cas : le corps K est de *cardinal infini.*
a) Posons $[L : K] = n > 1$ et supposons qu'il n'existe qu'un nombre fini de corps intermédiaires. Pour tout $a \in L$, on a $1 \leq [K(a) : K] \leq n$; considérons $\alpha \in L$ tel que $[K(\alpha) : K]$ soit *maximal* et montrons que $L = K(\alpha)$.
Supposons $K(\alpha) \subsetneq L$; il existe alors $\beta \in L$ tel que $\beta \notin K(\alpha)$.
Pour tout $x \in K$, $K(\alpha + \beta x)$ est un corps intermédiaire pour l'extension $L : K$; mais le corps K étant, par hypothèse, de cardinal infini, nécessairement, certains de ces corps coincident. Supposons x et y dans K tels que

$$x \neq y \quad \text{et} \quad K(\alpha+\beta x) = K(\alpha+\beta y),$$

$$\text{alors} \quad \big((\alpha+\beta x) \text{ et } (\alpha+\beta y) \text{ dans } K(\alpha+\beta x)\big) \Longrightarrow \beta(x-y) \in K(\alpha+\beta x).$$

$$\text{Par suite,} \quad (x \text{ et } y \text{ dans } K(\alpha+\beta x) \text{ et } x \neq y) \Longrightarrow \beta \in K(\alpha+\beta x),$$

$$\big(\alpha \text{ et } \beta \text{ dans } K(\alpha+\beta x) \text{ et } \beta \notin K(\alpha)\big) \Longrightarrow [K(\alpha+\beta x) : K] > [K(\alpha) : K],$$

ce qui contredit la maximalité de $[K(\alpha) : K]$, donc $L = K(\alpha)$.

b) Supposons L extension simple de K ; soit $L = K(\alpha)$. D'après le Th. 2.26,

$$[L : K] < \infty \Longrightarrow \alpha \text{ algébrique sur } K.$$

Soit F un corps intermédiaire pour l'extension $L : K$; on a

$$K \subseteq F \subseteq L = K(\alpha)$$

$$\text{et} \quad [K(\alpha) : K] < \infty \Longrightarrow [K(\alpha) : F] < \infty \Longrightarrow \alpha \text{ algébrique sur } F.$$

Posons $q(X) := Irr_F(\alpha, X)$ et $r := deg\, q$; alors,

$$K \subseteq F \subseteq K(\alpha) \Longrightarrow F(\alpha) = K(\alpha),$$

$$\text{d'où} \quad r = deg\, q \Longrightarrow r = [F(\alpha) : F] = [K(\alpha) : F].$$

En supposant $q(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_1 X + a_0$ dans $F[X]$, on a

$$K \subseteq K(a_0, a_1, \ldots, a_{r-1}) \subseteq F \quad \text{et} \quad q(X) \in K(a_0, a_1, \ldots, a_{r-1})[X].$$

Le polynôme $q(X)$, unitaire et irréductible dans $F[X]$, est encore unitaire et irréductible dans $K(a_0, a_1, \ldots, a_{r-1})[X] \subseteq F[X]$, par suite

$$q(\alpha) = 0 \Longrightarrow [K(a_0, a_1, \ldots, a_{r-1})(\alpha) : K(a_0, a_1, \ldots, a_{r-1})] = r.$$

$$K \subseteq K(a_0, a_1, \ldots, a_{r-1}) \subseteq F \subseteq K(\alpha) \Longrightarrow K(a_0, a_1, \ldots, a_{r-1})(\alpha) = K(\alpha),$$

d'où $[K(\alpha) : K(a_0, a_1, \ldots, a_{r-1})] = r$; alors l'égalité

$$[K(\alpha) : K(a_0, a_1, \ldots, a_{r-1})] = [K(\alpha) : F][F : K(a_0, a_1, \ldots, a_{r-1})],$$

entraîne $[F : K(a_0,a_1,\ldots,a_{r-1})] = 1$, donc $F = K(a_0,a_1,\ldots,a_{r-1})$.
Ainsi, le corps F est *déterminé* par le polynôme $q(X) = Irr_F(\alpha,X)$.
Soit $p(X) := Irr_K(\alpha,X)$ considéré dans $F[X]$; on a alors,

$$p(\alpha) = 0 \Longrightarrow q(X) \mid p(X) \text{ dans } F[X] \ ;$$

et le polynôme $p(X)$ n'ayant qu'un nombre fini de diviseurs irréductibles dans $F[X]$, on en conclut qu'il n'existe qu'un nombre fini de corps intermédiaires F, pour l'extension simple donnée $K(\alpha) : K$.

$2^{ème}$ cas : K est un corps *fini* (voir, Ch. 4).
Le Th. 2.30 est vrai car, d'une part (Th. 4.1),

$$(|\, K \,| < \infty \text{ et } [L : K] = n < \infty) \Longrightarrow |\, L \,| = |\, K \,|^n,$$

donc L est un corps fini et l'extension $L : K$ n'admet qu'un nombre fini de corps intermédiaires (Th. 4.8).
Nous verrons d'autre part, que toute extension de degré fini d'un corps fini est une extension simple (Th. 4.12, Rem. 4.14). □

Théorème 2.31. *Soit $L : K$ et $M : L$ des extensions de corps ; alors*

$$(L : K \text{ et } M : L \text{ } \textit{algébriques}) \Longrightarrow M : K \text{ } \textit{algébrique}.$$

Démonstration. Les extensions $L : K$ et $M : L$ étant algébriques, démontrons que tout élément β de M est algébrique sur K.
Par hypothèse, β est algébrique sur L, donc il existe un nombre fini d'éléments, non tous nuls dans L, $b_0,b_1,\ldots,b_m$, tels que

$$\sum_{0 \le i \le m} b_i \beta^i = 0. \tag{2.10}$$

Or, pour tout i, $1 \le i \le m$, b_i est algébrique sur K, donc $F := K(b_0,b_1,\ldots,b_m)$ est une extension algébrique et de degré fini sur K (Th. 2.29). On déduit de la relation (2.10), que l'élément β est algébrique sur F, d'où $[F(\beta) : F]$ fini, et

$$[F(\beta) : F][F : K] = [F(\beta) : K] < \infty,$$

entraîne β algébrique sur K (Th. 2.26). □

Remarque 2.32. La preuve du Th. 2.31 montre qu'étant donné des extensions de corps $L : K$ et $M : L$, pour β dans M, on a

$$(L : K \text{ algébrique et } \beta \text{ algébrique sur } L) \Longrightarrow \beta \text{ algébrique sur } K.$$

Définition 2.33. Une **extension** L d'un corps K est dite **transcendante** sur K, si elle n'est pas algébrique sur K; autrement dit, s'il existe au moins un élément $\alpha \in L$ transcendant sur K (Déf. 2.2).

Exemple 2.34. Il est connu que les nombres réels π et e sont transcendants sur $\mathbb{Q}$ (en voir une preuve dans l'App. B de ce livre) ; on en conclut que les corps $\mathbb{R}$ et $\mathbb{C}$ sont *transcendants* sur $\mathbb{Q}$.

Remarque 2.35. Les nombres π et e ne sont pas les seuls nombres réels transcendants sur $\mathbb{Q}$ ([28]).

Proposition 2.36. *Soit $L : K$ une extension de corps.*
1) *($\alpha \in L$ et α transcendant sur K)* $\iff [K(\alpha) : K]$ *infini.*
2) *L transcendant sur K* $\implies [L : K]$ *infini.*

Démonstration. 1) D'après les théorèmes 2.26 et 2.8,

$$[K(\alpha) : K] < \infty \iff \alpha \text{ algébrique sur } K.$$

La contraposée de cette relation donne le résultat 1) de la Prop. 2.36.
2) Si L est transcendant sur K, alors il existe un élément $\alpha \in L$ transcendant sur K, donc $[K(\alpha) : K]$ est infini, par suite (Th. 1.22),

$$[L : K] = [L : K(\alpha)][K(\alpha) : K] \implies [L : K] \text{ infini.} \qquad \square$$

Remarque 2.37. La réciproque de la propriété 2) de la Prop. 2. 36 est fausse. Il existe des extensions algébriques de degré infini (Ex. **14.** à la fin du chapitre.).

5. Construction par la règle et le compas

Nous abordons le problème de la *construction par la règle et le compas,* comme application des propriétés élémentaires des extensions de corps.
Cette question préoccupait déjà les Grecs de l'Antiquité. En effet, la droite et le cercle étaient, selon Platon, les seules figures géométriques *parfaites*. Aussi, les géomètres de son époque accordèrent une grande importance aux constructions géométriques *possibles* avec la règle et le compas.
Certes, ces deux instruments permettent d'effectuer de nombreuses constructions, les plus fondamentales étant : la construction de la médiatrice d'un segment, de la bissectrice d'un angle, de droites parallèles à une droite donnée, d'où la division d'un segment en un nombre quelconque de segments égaux.
Cependant, trois célèbres problèmes résistèrent à l'ingéniosité des géomètres de la Grèce Antique :
1) *la duplication du cube* : construire un cube ayant un volume double de celui d'un cube donné.
2) *la trisection de l'angle* : partager un angle quelconque en trois angles égaux.
3) *la quadrature du cercle* : construire un carré ayant une aire égale à celle d'un cercle donné.
Grâce à leurs connaissances déjà très étendues, les géomètres grecs avaient bien pressenti *l'impossibilité* d'effectuer, par la règle et le compas, les trois constructions en question, mais ils n'avaient pas à leur disposition, la méthode de *formulation algébrique* permettant d'en donner une preuve rigoureuse.

A. Méthode de formulation algébrique

La méthode consiste à traduire algébriquement le problème géométrique de la construction par la règle et le compas.
On suppose connues les propriétés élémentaires de la géométrie affine euclidienne classique ([25]).

1 / Point constructible par la règle et le compas

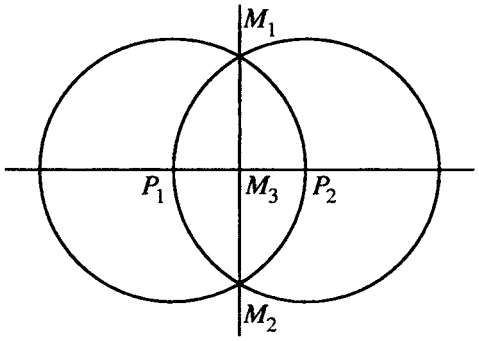
Nous considérons le problème de la construction par la règle et le compas dans le plan affine euclidien $\mathbb{R}^2$, muni d'un repère orthonormé Oxy. Tout point de $\mathbb{R}^2$ est alors déterminé par ses coordonnées (x,y).
D'une façon générale, résoudre un tel problème consiste à construire un certain nombre de points à partir d'un ensemble $\mathcal{P}_0$ de points donnés, dans le plan $\mathbb{R}^2$.
Exemple : Construire le milieu d'un segment P_1P_2; l'ensemble des points donnés est alors $\mathcal{P}_0 = \{P_1, P_2\}$.

La construction, par la règle et le compas, d'un point M à partir de $\mathcal{P}_0$, résulte d'un nombre fini d'opérations 1 ou 2, dites *élémentaires* et définies comme suit :
Opération 1 : Tracer la droite passant par deux points de $\mathcal{P}_0$.
Opération 2 : Tracer le cercle dont le centre est un point de $\mathcal{P}_0$ et dont le rayon est égal à la distance de deux points de $\mathcal{P}_0$.

Définition 2.38. Tout point d'intersection de deux *droites ou cercles* obtenus par les opérations élémentaires 1 ou 2 sera dit **construit en une étape à partir de** $\mathcal{P}_0$.

Définition 2.39. Un point M du plan $\mathbb{R}^2$ sera dit **constructible à partir de** $\mathcal{P}_0$, s'il existe une suite finie de points $M_1, M_2, \ldots, M_n = M$ tels que, pour tout $i\,(1 \leq i \leq n)$, le point M_i est construit en une étape à partir de l'ensemble des points de $\mathcal{P}_0 \cup \{M_1, M_2, \ldots, M_{i-1}\}$.

Exemple 2.40. Construction du milieu d'un segment P_1P_2.



On a $\mathcal{P}_0 = \{P_1, P_2\}$. Les opérations élémentaires sont les suivantes :
1) Tracer la droite P_1P_2 (op. 1).
2) Tracer le cercle de centre P_1, de rayon égal à la distance des points P_1, P_2 (op. 2).
3) Tracer le cercle de centre P_2, de rayon égal à la distance des points P_1, P_2 (op. 2).
Soit M_1 et M_2 les points d'intersection des deux cercles précédents.
4) Tracer la droite M_1M_2 (op. 1)
Le point d'intersection M_3 des droites P_1P_2 et M_1M_2 est alors le milieu du segment P_1P_2, puisque la droite M_1M_2 est la médiatrice du segment P_1P_2.

2 / Formulation algébrique

On conserve les mêmes notations que précédemment.
On désigne par K_0 le sous-corps de $\mathbb{R}$ engendré par l'ensemble des coordonnées (x, y) des points de $\mathcal{P}_0$. Le corps K_0 est nécessairement de caractéristique 0, donc contient $\mathbb{Q}$; par suite, K_0 est l'extension de $\mathbb{Q}$ obtenue par l'adjonction des coordonnées des points de $\mathcal{P}_0$.
Etant donné un point M du plan $\mathbb{R}^2$, résultant des constructions successives de points $M_1, M_2, \ldots, M_n = M$, pour tout $i\,(1 \leq i \leq n)$ on note (x_i, y_i) les coordonnées de M_i et on

définit le corps K_i tel que

$$K_i = K_{i-1}(x_i, y_i).$$

On obtient ainsi la chaîne d'extensions de corps

$$\mathbb{Q} \subseteq K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subset \mathbb{R}. \tag{2.11}$$

Lemme 2.41. *Avec les notations précédentes, pour tout $i (1 \leq i \leq n)$, les nombres réels x_i et y_i sont racines de polynômes de $K_{i-1}[X]$, de degré 1 ou 2.*

Démonstration. Trois cas sont à considérer pour la construction du point M_i à partir de l'ensemble $\mathcal{P}_0 \cup \{M_1, M_2, \ldots, M_{i-1}\}$. En effet, le point M_i est l'intersection, soit de deux droites, soit d'une droite et d'un cercle, soit de deux cercles.
Etant donné deux points distincts A et B dans le plan affine $\mathbb{R}^2$, dont les coordonnées respectives $(a, a'), (b, b')$ sont dans K_{i-1}, l'équation de la droite AB, dans le repère $0xy$, est ([25])

$$\frac{x-a}{b-a} = \frac{y-a'}{b'-a'}. \tag{2.12}$$

Etant donné un point C dont les coordonnées (c, c') sont dans K_{i-1}, si r est la distance de deux points de $\mathcal{P}_0 \cup \{M_1, M_2, \ldots, M_{i-1}\}$, alors $r^2 \in K_{i-1}$ et l'équation du cercle de centre C et de rayon r est

$$(x-c)^2 + (y-c')^2 = r^2. \tag{2.13}$$

L'équation (2.12) montre que si M_i est l'intersection de deux droites, alors ses coordonnées x_i et y_i sont, chacune, solution d'une équation de degré 1, à coefficients dans K_{i-1} et dans ce cas, on a $K_i = K_{i-1}$.
Examinons les cas où M_i est un point d'intersection d'une droite et d'un cercle ou de deux cercles.
a) M_i est un point d'intersection d'une droite AB, d'équation (2.12) et d'un cercle Γ, d'équation (2.13).
Les équations (2.12) et (2.13) entraînent successivement :

$$y = \frac{b'-a'}{b-a}(x-a) + a'; \tag{2.14}$$

$$(x-c)^2 + \left(\frac{b'-a'}{b-a}(x-a) + a' - c'\right)^2 = r^2. \tag{2.15}$$

Les points d'intersection M_i et M_i' de la droite AB et du cercle Γ (qui existent, par hypothèse) ont pour coordonnées (x_i, y_i) et (x_i', y_i'), où x_i et x_i' sont les racines (nécessairement réelles) du polynôme du second degré défini par la relation (2.15) ; y_i et y_i' étant obtenus en substituant, successivement, x_i et x_i' à x dans la relation (2.14). On en déduit que

$$K_i = K_{i-1}(x_i, y_i) = K_{i-1}(x_i) = K_{i-1}(y_i) \tag{2.16}$$

$$\text{et} \quad [K_i : K_{i-1}] = [K_{i-1}(x_i) : K_{i-1}] = 1 \text{ ou } 2. \tag{2.17}$$

b) On considère le cas où M_i est un point d'intersection de deux cercles Γ_1 et Γ_2 d'équations respectives :

$$(x-c_1)^2 + (y-c_1')^2 = r_1^2 \tag{2.18}$$

$$(x-c_2)^2 + (y-c_2')^2 = r_2^2. \tag{2.19}$$

En explicitant les équations (2.18) et (2.19), on obtient ensuite, par soustraction, l'équation de la droite joignant les points M_i et M_i' d'intersection des deux cercles :

$$2x(c_1 - c_2) + 2y(c_1' - c_2') - {c_1}^2 + {c_2}^2 - {c_1'}^2 + {c_2'}^2 + {r_1}^2 - {r_2}^2 = 0. \tag{2.20}$$

Les points M_i et M_i' peuvent alors être considérés comme points d'intersection de la droite d'équation (2.20) et de l'un des cercles Γ_1 ou Γ_2.
On est ainsi ramené au cas a) précédent ; par suite, les conclusions (2.16) et (2.17) sont valables dans le cas b). □

Théorème 2.42. *Si un point M de coordonnées* (x,y) *est* constructible *à partir d'un ensemble* $\mathcal{P}_0$ *de points de l'espace affine euclidien* $\mathbb{R}^2$ *et si* K_0 *est le sous-corps de* $\mathbb{R}$ *engendré par les coordonnées des points de* $\mathcal{P}_0$, *alors*

$$[K_0(x) : K_0] \text{ et } [K_0(y) : K_0]$$

sont des puissances de 2.

Démonstration. On suppose, selon la Déf. 2.39, que M résulte des constructions successives des points $M_1, M_2, \ldots, M_n = M$. En reprenant les notations et les conclusions du lemme 2.41, on a pour tout $i (1 \leq i \leq n)$,

$$K_i = K_{i-1}(x_i) = K_{i-1}(y_i) \quad \text{et} \quad [K_i : K_{i-1}] = 1 \text{ ou } 2.$$

On en déduit que

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \ldots [K_1 : K_0]$$

est une puissance de 2 (sachant que $1 = 2^0$).
Or, d'après les hypothèses, $M = M_n$, donc $x = x_n$ et $y = y_n$, ; alors

$$[K_n : K_0] = [K_n : K_0(x)][K_0(x) : K_0] \Longrightarrow [K_0(x) : K_0] \text{ est une puissance de 2.}$$

De même, $[K_0(y) : K_0]$ est une puissance de 2. □

B. Les trois fameuses constructions impossibles

C'est le Th. 2.42 qui permet de prouver l'impossibilité de résoudre, par la règle et le compas, les trois fameux problèmes cités au début de ce paragraphe.
On conservera les notations telles que $\mathcal{P}_0$, K_0, définies dans le paragraphe précédent.

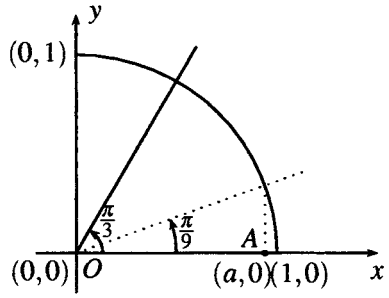
Proposition 2.43. *Il est impossible de construire, par la règle et le compas, un cube ayant un volume double de celui d'un cube donné.*

Démonstration. Désignons par C_0 un cube donné dans l'espace affine $\mathbb{R}^3$, rapporté à un repère orthonormé $Oxyz$. On suppose que O est un sommet du cube et que l'une de ses arêtes est sur l'axe Ox.
On choisit, comme unité de longueur, la longueur de l'arête de C_0, dont le volume est alors $1^3 = 1$.
L'ensemble $\mathcal{P}_0$ des points donnés dans le plan Oxy est ici formé par les points de coordonnées $(0,0)$ et $(1,0)$. On en déduit que $K_0 = \mathbb{Q}$.
Résoudre le problème de la duplication du cube revient à construire un point A sur l'axe Ox de coordonnées $(a,0), a > 0$ dans $\mathbb{R}$, tel que le cube d'arête a ait pour volume 2 ; ce qui implique $a^3 = 2$.

Si le point A était constructible par la règle et le compas, alors le degré de l'extension $\mathbb{Q}(a) : \mathbb{Q}$ serait une puissance de 2 (Th. 2.42).
Or a est la racine réelle du polynôme $X^3 - 2$, irréductible sur $\mathbb{Q}$, on a donc
$[\mathbb{Q}(a) : \mathbb{Q}] = 3$, d'où une contradiction qui prouve l'impossibilité de la duplication du cube, par la règle et le compas. □

Proposition 2.44. *L'angle de mesure $\frac{\pi}{3}$ ne peut être divisé en trois angles égaux, par la règle et le compas.*

Démonstration. On suppose choisie une unité de longueur dans le plan affine euclidien $\mathbb{R}^2$, rapporté à un repère orthonormé Oxy; alors l'ensemble $\mathcal{P}_0$ est formé des points $(0,0)$ et $(1,0)$, d'où $K_0 = \mathbb{Q}$.
Effectuer la trisection de l'angle $\frac{\pi}{3}$ dans le plan $\mathbb{R}^2$ revient à construire le point A de coordonnées $(a,0)$, où $a = \cos\frac{\pi}{9}$.



Si le point A était *constructible* (Déf. 2.39), il en serait de même du point $B = (b,0)$, où $b = 2a = 2\cos\frac{\pi}{9}$, et réciproquement.
Appliquons la formule de trigonométrie

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$

en prenant $\theta = \frac{\pi}{9}$. On a $\cos 3\theta = \frac{1}{2}$, par suite,

$$\cos\frac{\pi}{9} = \frac{b}{2} \Longrightarrow b^3 - 3b - 1 = 0.$$

Or le polynôme $f(X) = X^3 - 3X - 1$ est irréductible sur $\mathbb{Q}$ (à vérifier en appliquant le Critère d'Eisenstein au polynôme $f(X+1)$ ([13], Ch. 5)), d'où

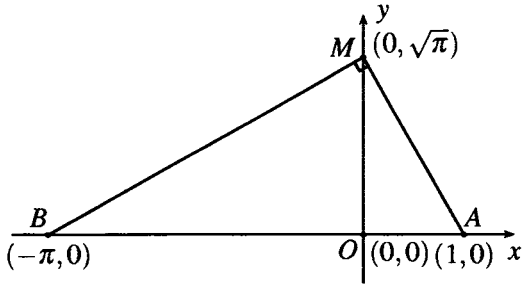
$$[\mathbb{Q}(b) : \mathbb{Q}] = 3.$$

On en conclut (Th. 2.42) que le point $B = (b,0)$ et par suite, le point $A = (a,0)$, où $a = \frac{b}{2}$, n'est pas constructible par la règle et le compas. □

Remarque 2.45. La proposition 2.44 fournit un exemple permettant d'affirmer qu'étant donné un angle de mesure α quelconque, $0 < \alpha < 2\pi$, la trisection de cet angle, par la règle et le compas, est impossible, en général.
On rappelle cependant que l'on sait construire, par la règle et le compas, un angle de mesure $\frac{\pi}{3}$, donc la trisection de l'angle de mesure π est possible ; il en est alors de même pour les angles de mesure $\frac{\pi}{2}$ ou 2π.

Proposition 2.46. *La quadrature du cercle est impossible par la règle et le compas.*

Démonstration. On considère, dans le plan $\mathbb{R}^2$ rapporté au repère orthonormé Oxy, le cercle de centre O et de rayon 1 ; son aire est donc égale à π.
Résoudre la quadrature du cercle, revient à construire le point $M = (0, \sqrt{\pi})$ à partir de l'ensemble $\mathcal{P}_0 = \{(0,0),(1,0)\}$; comme dans les problèmes précédents, on a $K_0 = \mathbb{Q}$.
Si le point M était constructible (Déf. 2.39), alors, à partir de $\mathcal{P}_0$ et du point M, on pourrait construire, par la règle et le compas, le triangle AMB rectangle en M, où $A = (1,0)$ et $B = (-\pi,0)$.



En effet, dans ce triangle rectangle, la hauteur relative à l'hypothénuse est MO, d'où (en utilisant un résultat de géométrie élémentaire connu)

$$OM^2 = OA.OB \Longrightarrow \pi = OB.$$

Le point B étant constructible, on aurait $[\mathbb{Q}(\pi) : \mathbb{Q}]$ égal à une puissance de 2 (Th. 2.42), ce qui est en contradiction avec la transcendance de π sur $\mathbb{Q}$ (Cf. App. B). □

C. Caractérisation des constructions possibles

Nous reprenons les notations du paragraphe **A.**

Dans les énoncés qui suivent, $\mathcal{P}_0$ désigne un ensemble de points du plan affine orthonormé $\mathbb{R}^2$ contenant les points $(0,0)$ et $(1,0)$; K_0 est le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points de $\mathcal{P}_0$.

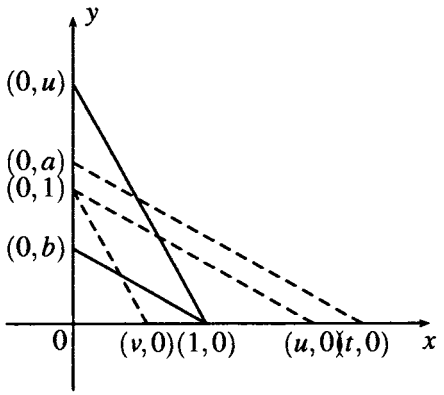
Lemme 2.47. *Un point $(a,b) \in \mathbb{R}^2$ est constructible à partir de $\mathcal{P}_0$, si a et b appartiennent au sous-corps K_0 de $\mathbb{R}$.*

Démonstration. On remarque qu'étant donné un point (a,b) du plan $\mathbb{R}^2$, il est facile de construire les points $(0,a)$ et $(0,b)$.
Inversement, la donnée des points $(0,a)$, $(0,b)$ permet de construire le point (a,b) dans $\mathbb{R}^2$.
Pour démontrer le lemme 2.47, il suffit donc de prouver qu'étant donné des points $(0,a)$ et $(0,b)$ de $\mathcal{P}_0$, alors les points

$$(0,a+b),\ (0,a-b),\ (0,ab),\ (0,\frac{a}{b}),\ \text{si } b \neq 0.$$

sont constructibles.
Pour les deux premiers points, la construction est immédiate ; pour les deux autres, on suppose a et b non nuls et on procède comme suit.
Par le point $(0,a)$ on construit la parallèle à la droite joignant les points $(0,b)$ et $(1,0)$, qui coupe l'axe $0x$ en $(t,0)$. En utilisant les propriétés des triangles semblables (voir la figure) on obtient

$$\frac{t}{a} = \frac{1}{b} \Longrightarrow t = \frac{a}{b}, \quad \text{d'où le point } (0,\frac{a}{b}).$$



En prenant $a = 1$, on construit, par le même procédé, le point $(u,0)$ où $u = \frac{1}{b}$; puis en remplaçant le point $(0,b)$ par $(0,\frac{1}{b})$, on obtient $(v,0)$, où $v = ab$. □

Lemme 2.48. *On considère une extension $K_0(\alpha) : K_0$ telle que*

$$K_0(\alpha) \subset \mathbb{R} \quad et \quad [K_0(\alpha) : K_0] = 2 ;$$

alors, tout point (x,y) du plan $\mathbb{R}^2$, tel que $(x,y) \in K_0(\alpha) \times K_0(\alpha)$ est constructible à partir d'un ensemble fini de points dont les coordonnées sont dans K_0.

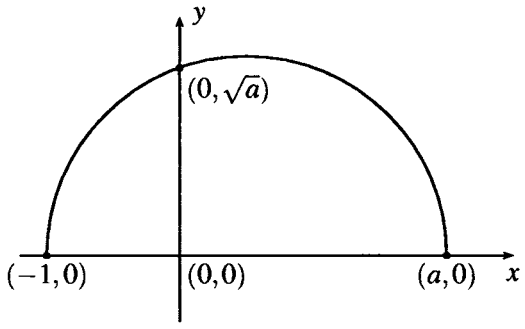
Démonstration. L'hypothèse $[K_0(\alpha) : K_0] = 2$ implique que α est algébrique sur K_0 et que $p_\alpha(X) := Irr_{K_0}(\alpha, X)$ est de degré 2. Posons

$$p_\alpha(X) = X^2 + bX + c, \quad \text{dans} \quad K_0[X] \subset \mathbb{R}[X].$$

$$\alpha \in \mathbb{R} \Longrightarrow b^2 - 4c \geq 0 \quad \text{et} \quad \alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Compte tenu du lemme 2.47, pour prouver le lemme 2.48, il suffit de montrer que le point $(0, \sqrt{b^2 - 4c})$ est constructible à partir d'un nombre fini de points dont les coordonnées sont dans K_0.

Cela revient à montrer que, quel que soit $a > 0$ dans K_0, le point $(0, \sqrt{a})$ est constructible, à partir d'un nombre fini de points dont les coordonnées sont dans K_0. La construction est indiquée par la figure ci-dessous. □



Théorème 2.49. *Soit L une extension de K_0, contenue dans $\mathbb{R}$, et x, y des éléments de L ; alors le point (x,y) du plan $\mathbb{R}^2$, est constructible si et seulement s'il existe un nombre fini de corps intermédiaires entre K_0 et $K_0(x,y)$ tels que*

$$K_0 \subset K_1 \subset \cdots \subset K_r = K_0(x,y), \quad r \geq 1 \quad et \quad [K_i : K_{i-1}] = 2, \forall i (1 \leq i \leq r).$$

Démonstration. 1°) Si $M(x,y)$ est constructible à partir des points de $\mathcal{P}_0$ (Déf. 2.39), alors, d'après le lemme 2.41, et la peuve du Th. 2.42, il existe une chaîne croissante finie de corps, $\{K_i\}_{0\leq i\leq n}$, $n\in\mathbb{N}$, telle que

$$\mathbb{Q}\subseteq K_0\subseteq K_1\subseteq\cdots\subseteq K_n=K_0(x,y)\subset\mathbb{R}$$
$$\text{et}\quad \forall i(1\leq i\leq n),\ [K_i:K_{i-1}]=1\ \text{ ou }\ 2.$$

Si $n\geq 1$, en éliminant les cas où deux corps consécutifs sont égaux, on peut extraire de la chaîne précédente une chaîne finie strictement croissante
$\{K_j\}_{0\leq j\leq r}$, $0\leq r\leq n$, que l'on écrira, moyennant un éventuel changement d'indexation :

$$K_0\subset K_1\subset\cdots\subset K_r=K_0(x,y),\quad [K_j:K_{j-1}]=2,\ 1\leq j\leq r. \tag{2.21}$$

2°) Réciproquement, supposons qu'il existe une chaîne finie strictement croissante de corps intermédiaires entre K_0 et $K_0(x,y)\subset\mathbb{R}$ vérifiant les conditions (2.21), montrons qu'alors, le point $M(x,y)$ est constructible.
Pour $r=0$ et $r=1$, le résultat est donné, respectivement, par le lemme 2.47 et le lemme 2.48.
Pour $r>1$, on raisonne par récurrence sur r.
Pour tout j, $1\leq j\leq r$, soit $\alpha_j\in K_j\setminus K_{j-1}$. On a $[K_j:K_{j-1}]=2$ donc α_j est algébrique sur K_{j-1} et le degré du polynôme $Irr_{K_{j-1}}(\alpha_j,X)$ est 2 ; on en déduit que $K_{j-1}(\alpha_j)=K_j$.
D'après le lemme 2.48, tout point (x,y) dont les coordonnées sont dans K_j est constructible à partir d'un nombre fini de points dont les coordonnées sont dans K_{j-1}.
L'hypothèse de récurrence et le raisonnement précédent, appliqué au cas $j=r$, donnent le résultat énoncé. □

Remarque 2.50. Une droite étant déterminée par deux points, il a été prouvé qu'en fait, toute construction par *la règle et le compas* pouvait s'effectuer en utilisant, uniquement, *le compas*. Cette propriété est généralement attribuée à Mascheroni (1797).
Pour davantage de résultats, concernant les problèmes de constructions par la règle et le compas, voir par exemple [14] ou [32].

Nous étudierons, dans le Ch. 7, *le problème de la construction des polygones réguliers, en utilisant, à la fois, les* Th. 2.42, 2.49 *et la Théorie de Galois.*

6. Exercices

1. Soit L une extension d'un corps K, obtenue par l'adjonction d'un nombre fini d'éléments :

$$L=K(\alpha_1,\alpha_2,\ldots,\alpha_n),\ n>1 \text{ dans } \mathbb{N}.$$

1°) Démontrer que $[L:K]$ est fini si et seulement si α_1 est algébrique sur K et, pour tout $i\,(2\leq i\leq n)$, α_i est algébrique sur $K(\alpha_1,\ldots\alpha_{i-1})$.
2°) Soit $K[X_1,X_2,\ldots,X_n]$ l'anneau des polynômes à n indéterminées sur K. Montrer que si $[L:K]$ est fini, alors

$$L=\{f(\alpha_1,\alpha_2,\ldots,\alpha_n);f\in K[X_1,X_2,\ldots,X_n]\}.$$

2. Soit $\alpha\in\mathbb{C}$; que peut-on dire du degré du polynôme $Irr_{\mathbb{R}}(\alpha,X)$?

3. On considère l'extension $\mathbb{Q}(\sqrt{5}):\mathbb{Q}$.
1°) Vérifier que tout élément $\alpha\in\mathbb{Q}(\sqrt{5})$ s'écrit, de façon unique,

$$\alpha=a+b\sqrt{5},\ \text{où } a \text{ et } b \text{ sont } \mathbb{Q}.$$

2°) Pour α donné dans $\mathbb{Q}(\sqrt{5})$, déterminer le polynôme $Irr_{\mathbb{Q}}(\alpha, X)$.

4. K étant un corps, soit $f(X) \in K[X]$ tel que $deg\, f = k > 1$ et L une extension de K telle que $[L : K] = n > 1$.
Montrer que si le polynôme f est irréductible sur K et $k \wedge n = 1$, alors $f(X)$ n'a aucune racine dans L.

5. Soit $\mathbb{Q}(i, \sqrt{2})$, où $i^2 = -1$ dans $\mathbb{C}$.
1°) On pose $\alpha := i + \sqrt{2}$; vérifier que

$$\frac{\alpha^2 - 3}{2\alpha} = i; \quad \frac{\alpha^2 + 3}{2\alpha} = \sqrt{2}.$$

En déduire que $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\alpha)$.
2°) Soit $\beta \in \mathbb{C}$ tel que $\beta^2 = i$.
Exprimer β sous la forme $a + ib$, où a et b sont réels.
En déduire que $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\beta)$.
3°) Déterminer $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}]$; trouver alors, deux polynômes, $p_1(X), p_2(X)$, unitaires et irréductibles dans $\mathbb{Q}[X]$, tels que

$$\mathbb{Q}(i, \sqrt{2}) \simeq \frac{\mathbb{Q}[X]}{(p_1(X))}; \quad \mathbb{Q}(i, \sqrt{2}) \simeq \frac{\mathbb{Q}[X]}{(p_2(X))}.$$

6. Justifier l'irréductibilité sur $\mathbb{Q}$, des polynômes

$$p(X) = X^2 - 2 \quad \text{et} \quad q(X) = X^2 - 4X + 2.$$

Vérifier qu'il existe des corps de rupture $\mathbb{Q}(\alpha)$ de $p(X)$ et $\mathbb{Q}(\beta)$ de $q(X)$ contenus dans $\mathbb{R}$.
Comparer les corps $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(\beta)$.

7. Etant donné une extension de corps $L : K$, pour tout élément $\alpha \in L$, algébrique sur K, on pose

$$p_\alpha(X) := Irr_K(\alpha, X).$$

On considère les cas suivants :

$$a)\, L = \mathbb{R},\ K = \mathbb{Q},\ \alpha = \sqrt{3}; \qquad b)\, L = \mathbb{R},\ K = \mathbb{Q},\ \alpha = \frac{1 + \sqrt{5}}{2};$$

$$c)\, L = \mathbb{C},\ K = \mathbb{Q},\ \alpha = \frac{i\sqrt{3} - 1}{2}.$$

1°) Dans chacun de ces cas, justifier l'existence du polynôme $p_\alpha(X)$ en le calculant et préciser le degré $[K(\alpha) : K]$.
2°) Dans le cas b) (resp. c)) trouver un élément $\beta \in \mathbb{R}$ (resp. $\beta \in \mathbb{C}$) tel que $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$ et $p_\beta(X) \neq p_\alpha(X)$.

8. Dans chacun des cas envisagés ci-dessous, existe-t-il un élément α, appartenant à une extension de K, tel que $Irr_K(\alpha, X) = p(X)$?

$$a)\, K = \mathbb{Z}/3\mathbb{Z},\ p(X) = X^2 + 1; \qquad b)\, K = \mathbb{Z}/5\mathbb{Z},\ p(X) = X^2 + 1;$$

$$c)\, K = \mathbb{R},\ p(X) = X^7 - 3X^6 + 4X^3 - X - 1.$$

9. Déterminer le degré de l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ et trouver une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbb{Q}$.

10. Soit $f(X) \in K[X]$, où K est un corps. On suppose $deg f = n > 1$.

1°) Prouver que pour $n = 2$ et $n = 3$, $f(X)$ est irréductible sur K si et seulement si $f(X)$ n'a pas de racine dans K.

2°) Montrer, par un exemple, qu'un polynôme $f(X)$ de degré $n > 3$, qui n'a pas de racine dans K, n'est pas nécessairement irréductible sur K.

11. On considère le polynôme $p(X) = X^3 + X - 1$ dans $\mathbb{Q}[X]$.

1°) Vérifier que $p(X)$ est irréductible sur $\mathbb{Q}$.

$\mathbb{Q}(\alpha)$ étant un corps de rupture de $p(X)$ sur $\mathbb{Q}$, comment s'écrivent les éléments de $\mathbb{Q}(\alpha)$?

2°) Soit $\lambda = 6 + 3\alpha + 4\alpha^2$. Déterminer le degré $[\mathbb{Q}(\lambda) : \mathbb{Q}]$; en déduire que

$$\mathbb{Q}(\lambda) = \mathbb{Q}(\alpha).$$

3°) On pose

$$\alpha\lambda = a_0 + a_1\alpha + a_2\alpha^2; \qquad \alpha^2\lambda = b_0 + b_1\alpha + b_2\alpha^2.$$

a) Calculer les nombres rationnels a_i, b_i, $0 \leq i \leq 2$.

b) On considère le système d'équations linéaires suivant

$$(S) = \begin{cases} (6-\lambda)X_1 + 3X_2 + 4X_3 = 0 \\ a_0X_1 + (a_1 - \lambda)X_2 + a_2X_3 = 0 \\ b_0X_1 + b_1X_2 + (b_2 - \lambda)X_3 = 0 \end{cases}$$

(S) est un système linéaire homogène de trois équations à trois inconnues, à coefficients dans le corps $\mathbb{Q}(\lambda)$.

- Ecrire le système (S) en remplaçant les a_i et b_i $(0 \leq i \leq 2)$, par les valeurs trouvées dans la question a).
- Que peut-on dire du déterminant du système (S) ?
- Calculer le déterminant de (S) ; en déduire le polynôme irréductible de λ sur $\mathbb{Q}$.

12. Soit $Aut(K)$ le groupe des automorphismes d'un corps K. On appelle **involution** de K, tout élément $\sigma \in Aut(K)$ tel que $\sigma^2 = id_K$.

On note $\mathfrak{I}_K$ l'ensemble des *involutions* de K.

1°) Soit $\sigma \in \mathfrak{I}_K \setminus \{id_K\}$; on pose

$$L := \{x \in K \,;\, \sigma(x) = x\},$$
$$M := \{x \in K \,;\, \sigma(x) = -x\}.$$

Vérifier que L et M sont non vides. Montrer que L est un sous-corps de K et que M est un sous-groupe de $(K, +)$.

2°) On suppose $car K \neq 2$; montrer que pour tout $\sigma \in \mathfrak{I}_K \setminus \{id_K\}$, on a les propriétés suivantes.

a) $K = L \oplus M$ (somme directe de sous-groupes de $(K, +)$).

b) $\forall a \in M \setminus \{0\}$, $M = La = \{xa \,;\, x \in L\}$.

c) $\forall a \in M \setminus \{0\}$, $a^2 \in L$; en déduire que

$$K = L(a) \;;\; [K : L] = 2 \;;\; Irr_L(a, X) = X^2 - a^2.$$

d) Si $\tau \in \mathfrak{I}_K \setminus \{id_K\}$ et $\tau_{/L} = \sigma$, alors $\tau = \sigma$.

3°) On suppose $car K = 2$; soit $\sigma \in \mathfrak{I}_K \setminus \{id_K\}$.

a) Soit $a \in K$ tel que $\sigma(a) \neq a$; on pose $b = a(a - \sigma(a))^{-1}$. Vérifier que $\sigma(b) = b + 1$.

On pose $\beta := b\sigma(b)$; montrer que

$$\beta \in L \text{ et } b^2+b+\beta = 0.$$

b) Soit $x \in K \setminus L$ et $y := (x-\sigma(x))^{-1}$.
Montrer que $(y+b) \in L$; en déduire que

$$K = L(b)\ ;\ Irr_L(b,X) = X^2+X+\beta\ ;\ [K:L] = 2.$$

c) Soit $\tau \in \mathfrak{I}_K \setminus \{id_K\}$ tel que $\tau_{/L} = \sigma$; prouver que $\tau = \sigma$.

13. Soit $K(\alpha)$ et $K(\beta)$ deux extensions simples algébriques d'un corps K telles que

$$[K(\alpha):K] = m > 0, \quad [K(\alpha):K] = n > 0.$$

1°) a) Vérifier que l'extension $K(\alpha,\beta)$ de K est de degré fini sur K, sur $K(\alpha)$ et sur $K(\beta)$.
b) On pose $t := [K(\alpha,\beta):K]$. Démontrer que t est un multiple de m et de n tel que $1 \leq t \leq mn$.
En conclure que si m et n sont premiers entre eux (c'est-à-dire $m \wedge n = 1$), alors $t = mn$.
2°) On suppose, dans cette question,

$$m > 1, \quad n > 1 \quad \text{et} \quad m \wedge n = 1.$$

Etant donné $a \neq 0$ dans K, on considère le polynôme $X^{mn} - a$.
Le but de cette question est de prouver que $X^{mn} - a$ est irréductible dans $K[X]$ si et seulement si $X^m - a$ et $X^n - a$ le sont.
a) Montrer que, dans $K[X]$,

$$X^{mn} - a \text{ irréductible } \Longrightarrow X^m - a \text{ et } X^n - a \text{ irréductibles.}$$

b) On suppose $X^m - a$ et $X^n - a$ irréductibles dans $K[X]$.
Soit α une racine du polynôme $X^{mn} - a$ dans une extension de K.
– Déterminer les polynômes $Irr_K(\alpha^n,X)$ et $Irr_K(\alpha^m,X)$.
– Montrer, à l'aide du 1 °) b), que $\alpha \in K(\alpha^m, \alpha^n)$; en déduire que $X^{mn} - a$ est irréductible dans $K[X]$.

14. Soit $\mathcal{P}$ l'ensemble des nombres premiers (Cf. [13], App.A, Déf. 0.5).
1°) Soit $p \in \mathcal{P}$, $\sqrt{p}$ désignant la racine carrée positive de p dans $\mathbb{R}$, montrer que $\sqrt{p} \notin \mathbb{Q}$ et que $[\mathbb{Q}(\sqrt{p}):\mathbb{Q}] = 2$.
2°) On rappelle que $\mathcal{P}$ est une partie infinie de $\mathbb{N}$ ([13], App.A, Th. 0.12) et on considère la suite croissante des nombres premiers :

$$p_1 < p_2 < \cdots < p_{n-1} < p_n < \ldots$$

où $p_1 = 2, p_2 = 3, p_3 = 5, \ldots ; p_n$ désigne le $n^{ème}$ nombre premier. On pose

$$F := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}, \sqrt{p_{n+1}}, \ldots)$$

et $\quad \forall n \in \mathbb{N}, F_n := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$, avec $F_0 := \mathbb{Q}$.

a) Démontrer, par récurrence sur n, que

$$\forall n \in \mathbb{N},\ [F_{n+1} : F_n] = 2.$$

En déduire que, pour tout $n \in \mathbb{N}$, $[F_n : \mathbb{Q}] = 2^n$.
b) Prouver que $F = \bigcup_{n\in\mathbb{N}} F_n$; en déduire que F est une extension *algébrique* de $\mathbb{Q}$, de *degré infini* sur $\mathbb{Q}$.

15. Soit $K(\alpha)$ une extension *simple transcendante* de K (Déf. 2.2). On pose

$$K[\alpha] = \{f(\alpha);\ f(X) \in K[X]\}.$$

1°) a) L'élément α étant transcendant sur K, justifier la propriété suivante :

$K[\alpha]$ est un anneau factoriel.

Quelles sont les *unités* de l'anneau $K[\alpha]$? ([13], Ch. 1)

b) Montrer que tout polynôme non constant $f(X) \in K(\alpha)[X]$ peut s'écrire

$$f(X) = c(\alpha) f_1(X),$$

où $c(\alpha) \in K(\alpha)$ et $f_1(X)$ est *primitif* dans $K[\alpha][X]$ ([13], Déf. 5.102).

c) Si, dans $K(\alpha)[X]$, on a

$$c(\alpha) f_1(X) = d(\alpha) g_1(X),$$

avec $c(\alpha), d(\alpha)$ non nuls dans $K(\alpha)$ et $f_1(X), g_1(X)$ primitifs dans $K[\alpha][X]$, prouver qu'il existe $k \in K^*$ tel que

$$f_1(X) = k g_1(X).$$

2°) Soit $\beta \in K(\alpha) \setminus K$. On pose $\beta = \dfrac{u(\alpha)}{v(\alpha)}$; où $\dfrac{u(X)}{v(X)} \in K(X)$ et $u(X) \wedge v(X) = 1$ dans $K[X]$. Soit

$$p(X) := \beta v(X) - u(X) \text{ dans } K[\beta][X].$$

a) Montrer que α est algébrique sur $K(\beta)$. En déduire que β est transcendant sur K.

b) Si, dans $K[\beta][X]$, on a une égalité de la forme

$$p(X) = q(X) f(X), \text{ où } q(X) \in K[X] \text{ et } f(X) \in K[\beta][X],$$

démontrer que $deg\, q = 0$.

[Supposer $deg\, q > 0$ et montrer que cette hypothèse conduit à une contradiction, en considérant une racine de $q(X)$ dans une extension de K.]

En déduire que $p(X)$ est irréductible dans $K[\beta][X]$. [Considérer le degré de $p(X)$ en β.]

c) Démontrer que $p_1(X) = u(\alpha)v(X) - v(\alpha)u(X)$ est primitif dans $K[\alpha][X]$.

3°) Soit F une extension de K telle que

$$K \subsetneq F \subseteq K(\alpha).$$

a) Montrer que α est algébrique sur F.

b) On pose $f(X) := Irr_F(\alpha, X)$. Compte tenu du 1°), on a

$$f(X) = c(\alpha) f_1(X),$$

où $c(\alpha) \in K(\alpha)$ et $f_1(X)$ est primitif dans $K[\alpha][X]$. Ecrivons

$$f(X) = \sum_{0 \le i \le n} a_i(\alpha) X^i, \quad f_1(X) = \sum_{0 \le i \le n} b_i(\alpha) X^i,$$

où quel que soit $i\ (0 \le i \le n)$, $a_i(X) \in K(X)$ et $b_i(X) \in K[X]$.

Soit $m = max\{deg\, b_i\ ;\ 0 \le i \le n\}$.

Justifier l'existence d'au moins un indice $j\ (0 \le j \le n)$ tel que $a_j(\alpha) \in K(\alpha) \setminus K$. Pour un tel indice j, on pose $\beta := a_j(\alpha)$.

On écrit $\beta = \dfrac{u(\alpha)}{v(\alpha)}$, avec $u(X) \wedge v(X) = 1$ dans $K[X]$.

Calculer β en fonction de $b_j(\alpha)$ et $b_n(\alpha)$. En déduire les inégalités

$$deg\, u \le m,\ deg\, v \le m.$$

c) On pose $p(X) := \beta v(X) - u(X)$.

- Prouver que $f(X)$ divise $p(X)$, dans $F[X]$.

On écrit alors, $p(X) = f(X)q(X)$, dans $F[X]$.

- Vérifier que les résultats des questions 1°), 2°) et 3°) a) permettent d'écrire

$$p(X) = a(\alpha) p_1(X), \quad q(X) = b(\alpha) q_1(X), \quad f(X) = c(\alpha) f_1(X),$$

avec $a(\alpha) = \dfrac{1}{v(\alpha)}$, $b(\alpha), c(\alpha)$ dans $K(\alpha)$ et p_1, q_1, f_1 primitifs dans $K[\alpha][X]$.

- Justifier l'existence d'un élément d, non nul dans K, tel que

$$p_1(X) = d f_1(X) q_1(X). \tag{2.22}$$

- En comparant les degrés en α des deux membres de (2.22), prouver qu'il existe d_1, non nul dans K, tel que

$$p_1(X) = d_1 f_1(X).$$

d) Montrer que les résultats précédents entraînent $F = K(\beta)$.

16. Montrer que la trisection d'un angle, de mesure θ, est possible par la règle et le compas si et seulement si le polynôme

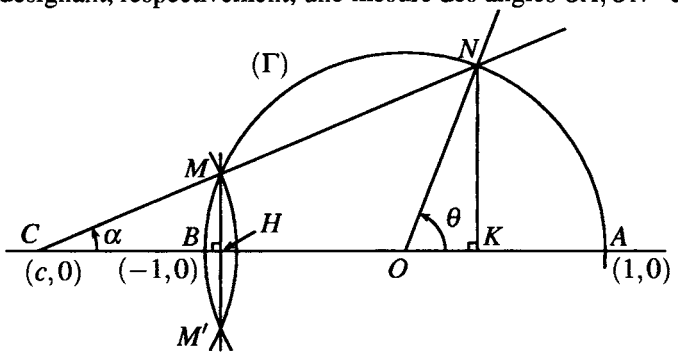
$$4X^3 - 3X - \cos\theta$$

est *réductible* sur $\mathbb{Q}(\cos\theta)$.

17. Dans le plan euclidien orthonormé Oxy ([25]), on considère le cercle trigonométrique (Γ) coupant l'axe Ox en $A = (1,0)$ et $B = (-1,0)$.
Soit $C = (c,0)$, un point de Ox tel que (par exemple) $-2 < c < -1$, dans $\mathbb{R}$. Le cercle de centre C et de *rayon 1* coupe (Γ) en deux points distincts, M et M', où l'on suppose M d'ordonnée positive. Soit N le second point d'intersection de la droite CM avec (Γ) ; on pose

$$\theta := \widehat{\overrightarrow{OA}, \overrightarrow{ON}}, \qquad \alpha := \widehat{\overrightarrow{CA}, \overrightarrow{CN}},$$

θ et α désignant, respectivement, une mesure des angles $\widehat{\overrightarrow{OA}, \overrightarrow{ON}}$ et $\widehat{\overrightarrow{CA}, \overrightarrow{CN}}$.



Compte tenu du choix de la position du point C sur l'axe Ox, démontrer que $\theta = 3\alpha$. (On pourra considérer les triangles semblables CMH et CNK, où H et K sont, respectivement, les projections orthogonales de M et N sur Ox).

Chapitre 3
Extensions normales - Extensions séparables

Dans tout le chapitre, K désigne un corps et $K^* = K \setminus \{0\}$.

1. Corps de décomposition d'un polynôme

A. Préliminaires

a) On rappelle qu'un polynôme $f(X) \in K[X]$, de degré $n > 0$, a au plus n racines, « distinctes ou confondues », dans K ([13], Cor. 4.48).

b) Dans le Ch. 2, nous avons défini la notion de *corps de rupture* pour un polynôme irréductible et unitaire de $K[X]$ (Déf. 2.21).
Afin d'étendre cette définition à un polynôme non constant, quelconque de $K[X]$, rappelons que, l'anneau $K[X]$ étant factoriel ([13], Ch. 4), tout polynôme $f(X) \in K[X] \setminus K$ s'écrit de façon unique (à l'ordre près des facteurs)

$$f(X) = a(p_1(X))^{n_1}(p_2(X))^{n_2} \dots (p_r(X))^{n_r}, \tag{3.1}$$

où $a \in K^*$, $r \in \mathbb{N}^*$ et pour $1 \leq i \leq r$, les $p_i(X)$ sont des polynômes irréductibles et unitaires, deux à deux distincts dans $K[X]$, les n_i étant dans $\mathbb{N}^*$.
Les polynômes $p_i(X)$, $1 \leq i \leq r$, sont les *facteurs* ou *diviseurs* irréductibles et unitaires de $f(X)$ dans $K[X]$.

Le polynôme $f(X)$ est dit *scindé sur* K si, dans la relation (3.1), pour tout i, $1 \leq i \leq r$, le polynôme $p_i(X)$ est de degré 1 ([13], Déf. 4.46) ; autrement dit :

$$f(X) = a(X - \alpha_1)^{n_1} \dots (X - \alpha_r)^{n_r} \quad \text{et} \quad \sum_{1 \leq i \leq r} n_i = \deg f. \tag{3.2}$$

Dans ce cas, le polynôme f a n racines dans K et les α_i, $1 \leq i \leq r$, sont les racines *distinctes* de f dans K.

Rappelons qu'un corps K est dit *algébriquement clos* ([13], Déf. 4.42), si tout polynôme non constant de $K[X]$ a au moins une racine dans K.
On en déduit ([13], Prop. 4.44) que si K est un corps algébriquement clos, alors tout polynôme non constant de $K[X]$ est scindé sur K.

La notion de corps algébriquement clos sera reprise dans le Ch. 5, où l'on démontrera, en particulier, que le corps $\mathbb{C}$ est algébriquement clos.

Définition 3.1. Etant donné un polynôme $f(X)$, non constant dans $K[X]$, on appellera **corps de rupture** de f sur K, tout corps de rupture d'un facteur irréductible quelconque de $f(X)$ dans $K[X]$.

Remarque 3.2. On sait qu'un corps de rupture d'un polynôme irréductible et unitaire $p(X)$ de $K[X]$ contient au moins une racine de $p(X)$, mais pas nécessairement toutes les racines de $p(X)$ (Cf. Exemple 2.19) ; compte tenu de la Déf. 3.1, il en est de même pour un corps de rupture d'un polynôme quelconque, non constant dans $K[X]$.
Le but du paragraphe suivant est de prouver que, pour tout polynôme non constant $f(X)$ de $K[X]$, il existe un corps, extension de K, sur lequel f est scindé et nous construirons la plus petite extension de K satisfaisant à cette propriété (Th. 3.3).

B. Notion de corps de décomposition d'un polynôme

Théorème 3.3. *Soit $f(X)$ un polynôme non constant de $K[X]$; alors il existe une extension E de K telle que*
1) $K \subseteq E$ et $f(X)$ est scindé sur E.
2) ($K \subseteq E' \subseteq E$ et $f(X)$ scindé sur E') $\Longrightarrow E' = E$.

Démonstration. On note que si K est algébriquement clos, alors $E = K$.
On suppose donc que K n'est pas algébriquement clos.
Posons $n := deg\, f \geq 1$ et raisonnons par récurrence sur n.
- Si $n = 1$, $f(X) = a(X - \alpha)$, où $a \in K^*$ et $\alpha \in K$, donc $E = K$.
- Supposons $n > 1$ et le théorème vrai pour tout polynôme de degré $n - 1$ sur un corps quelconque.

Soit $p_1(X)$ un diviseur irréductible et unitaire de $f(X)$ dans $K[X]$. Un corps de rupture de $p_1(X)$ est de la forme $K(\alpha_1)$, où α_1 appartient à une extension de K et $p_1(\alpha_1) = 0$. C'est aussi un corps de rupture de $f(X)$ sur K (Déf. 3.1).
α_1 étant une racine de $f(X)$ dans $K(\alpha_1)$, $(X - \alpha_1)$ divise $f(X)$ dans $K(\alpha_1)[X]$ ([13], Ch.4), d'où

$$f(X) = (X - \alpha_1)g(X), \text{ où } g(X) \in K(\alpha_1)[X] \text{ et } deg\, g = n - 1.$$

L'hypothèse de récurrence implique qu'il existe une extension E de $K(\alpha_1)$ satisfaisant aux propriétés 1) et 2) du Th. 3.3, pour le polynôme $g(X)$.
On a donc $K(\alpha_1) \subseteq E$ et $g(X)$ scindé sur E ; de plus, si E' est une extension de $K(\alpha_1)$ telle que $K(\alpha_1) \subseteq E' \subseteq E$ et $g(X)$ scindé sur E', alors $E' = E$.
Montrons que l'extension E de $K(\alpha_1)$, définie ci-dessus, est une extension de K satisfaisant au Th. 3.3 pour le polynôme $f(X)$. On a en effet,

$$K(\alpha_1) \subseteq E \Longrightarrow K \subseteq E ;$$
$$(f(X) = (X - \alpha_1)g(X) \text{ et } g(X) \text{ scindé sur } E) \Longrightarrow f(X) \text{ scindé sur } E.$$

D'autre part, si E' est une extension de K telle que

$$K \subseteq E' \subseteq E \text{ et } f(X) \text{ scindé sur } E',$$

alors, nécessairement, $\alpha_1 \in E'$, d'où $K(\alpha_1) \subseteq E' \subseteq E$. De plus,

$$f(X) \text{ scindé sur } E' \Longrightarrow g(X) \text{ scindé sur } E' ;$$

d'où $E' = E$, d'après l'hypothèse de récurrence formulée pour $g(X)$. □

Définition 3.4. Etant donné un polynôme $f(X)$ non constant dans $K[X]$, on appellera **corps de décomposition** de f sur K, toute extension E de K vérifiant les propriétés 1) et 2) du Th. 3.3.

Proposition 3.5. *Soit E un corps de décomposition d'un polynôme $f(X)$ non constant de $K[X]$; si $n = \deg f > 0$ et $\alpha_1, \ldots, \alpha_n$ sont les racines distinctes ou confondues de f dans E, alors*

$$E = K(\alpha_1, \ldots, \alpha_n),$$

donc E est une extension algébrique, de degré fini sur K.

Démonstration. On a

$$(K \subseteq E \text{ et } \forall i (1 \leq i \leq n), \alpha_i \in E) \Longrightarrow K(\alpha_1, \ldots, \alpha_n) \subseteq E. \tag{3.3}$$

Le polynôme f étant scindé sur E (Th. 3.3), dans $E[X]$, $f(X)$ s'écrit :

$$f(X) = a(X - \alpha_1) \ldots (X - \alpha_n), \quad \text{où } a \in K^*.$$

Cette égalité exprime que f est scindé sur $K(\alpha_1, \ldots, \alpha_n)$; alors, la relation (3.3) et la propriété 2) du Th. 3.3 impliquent

$$E = K(\alpha_1, \ldots, \alpha_n),$$

donc l'extension $E : K$ est algébrique, de degré fini (Th. 2.29). □

Remarque 3.6. a) Si, dans la preuve précédente, $\alpha_1, \ldots, \alpha_m$, $m \leq n$, sont les racines distinctes de $f(X)$ dans E, alors $E = K(\alpha_1, \ldots, \alpha_m)$.
b) La preuve du Th. 3.3 montre que la construction d'un corps de décomposition E d'un polynôme non constant $f(X)$ de $K[X]$ n'est pas unique, a priori ; cependant, nous allons démontrer que deux corps de décomposition d'un polynôme $f(X)$ sont K-isomorphes.

Lemme 3.7. *Soit λ un isomorphisme d'un corps K sur un corps K' et $f(X)$ non constant dans $K[X]$. On pose*

$$\hat{f}(X) := \hat{\lambda}(f(X)).$$

E étant un corps de décomposition de f sur K, soit L une extension de K' telle que $\hat{f}(X)$ est scindé sur L. Il existe alors un monomorphisme $\mu : E \longrightarrow L$ tel que $\mu_{/K} = \lambda$.

Démonstration. $\hat{\lambda}$ désigne le prolongement canonique de λ ([13], Ch. 4) ; $\hat{\lambda}$ est donc un isomorphisme de $K[X]$ sur $K'[X]$.
On suppose $K' \subseteq L$ et on raisonne par récurrence sur $n := \deg f > 0$.
– Si $n = 1$, alors $E = K$, on en déduit que $\mu = \lambda$.
– Supposons $n > 1$ et la propriété vérifiée pour tout polynôme de degré $n - 1$, sur un corps quelconque.
Soit $p_1(X)$ un diviseur irréductible et unitaire de $f(X)$ dans $K[X]$; le polynôme $f(X)$ étant scindé sur E, il en est de même de $p_1(X)$.
Puisque $\hat{\lambda}$ est un isomorphisme, $\hat{p}_1(X) := \hat{\lambda}(p_1(X))$ est un diviseur irréductible et unitaire de $\hat{f}(X)$ dans $K'[X]$ et $\deg \hat{p}_1 = \deg p_1$.
De plus, $\hat{f}(X)$ étant scindé sur L, il en est de même de $\hat{p}_1(X)$. Ecrivons

$$p_1(X) = (X - \alpha_1) \ldots (X - \alpha_d), \quad \text{dans } E[X],$$
$$\hat{p}_1(X) = (X - \beta_1) \ldots (X - \beta_d), \quad \text{dans } L[X].$$

Les extensions $K(\alpha_1)$ et $K'(\beta_1)$ sont, respectivement, corps de rupture de p_1 sur K et de $\hat{p}_1$ sur K'. D'après le Th. 2.23, il existe un isomorphisme μ_1 de $K(\alpha_1)$ sur $K'(\beta_1)$ tel que $\mu_{1/K} = \lambda$ et $\mu_1(\alpha_1) = \beta_1$.
α_1 étant une racine de $f(X)$, $X - \alpha_1$ divise $f(X)$ dans $K(\alpha_1)[X]$, d'où

$$f(X) = (X - \alpha_1)g(X), \text{ où } g(X) \in K(\alpha_1)[X], deg\, g = n - 1.$$

Soit $\hat{\mu}_1$ l'isomorphisme de $K(\alpha_1)[X]$ sur $K'(\beta_1)[X]$ prolongeant μ_1 ;

$$\hat{\mu}_1(f(X)) = (X - \beta_1)\hat{\mu}_1(g(X)) ;$$
$$\text{or,} \quad \mu_{1/K} = \lambda \Longrightarrow \hat{\mu}_1(f(X)) = \hat{\lambda}(f(X)) = \hat{f}(X).$$

Par hypothèse, $\hat{f}(X)$ est scindé sur L; or $\beta_1 \in L$, donc $\hat{\mu}_1(g(X))$ est scindé sur L. L'hypothèse de récurrence, appliquée au polynôme g de degré $n-1$, entraîne alors l'existence d'un monomorphisme

$$\mu : E \longrightarrow L \text{ tel que } \mu_{/K(\alpha_1)} = \mu_1 \quad \text{et} \quad \mu_{1/K} = \lambda \Longrightarrow \mu_{/K} = \lambda. \quad \square$$

Théorème 3.8. *Soit λ un isomorphisme d'un corps K sur un corps K' et $f(X)$ un polynôme non constant de $K[X]$. Si E est un corps de décomposition de f sur K et E' un corps de décomposition de $\hat{f} := \hat{\lambda}(f)$ sur K', alors les extensions $E : K$ et $E' : K'$ sont isomorphes et il existe un isomorphisme $\mu : E \longrightarrow E'$, tel que $\mu_{/K} = \lambda$.*

Démonstration. Soit u et u' les injections canoniques, respectivement, de K dans E et de K' dans E'. D'après le lemme 3.7, il existe un monomorphisme $\mu : E \longrightarrow E'$, tel que $\mu_{/K} = \lambda$, donc le diagramme suivant commute

$$\begin{array}{ccc} K & \xrightarrow{\lambda} & K' \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u'} \\ E & \xrightarrow{\mu} & E' \end{array}$$

On a $\mu \circ u = u' \circ \lambda$, d'où $K' = \lambda(K) = \mu(K) \subseteq \mu(E) \subseteq E'$.

$$f(X) = a \prod_{1 \le i \le n} (X - \alpha_i), \quad \text{dans } E[X],$$
$$\text{implique} \qquad \hat{f}(X) = \mu(a) \prod_{1 \le i \le n} (X - \mu(\alpha_i)), \quad \text{dans } E'[X],$$

d'où $\hat{f}$ scindé sur $\mu(E)$. Mais E' est, par hypothèse, un corps de décomposition de $\hat{f}$ sur K', par suite (Th. 3.3)

$$K' \subseteq \mu(E) \subseteq E' \Longrightarrow \mu(E) = E',$$

donc μ est un isomorphisme. $\square$

Corollaire 3.9. *Deux corps de décomposition sur K d'un polynôme $f(X) \in K[X] \setminus K$, sont K-isomorphes.*

Il suffit d'appliquer le Th. 3.8, dans le cas où $K' = K$ et $\lambda = id_K$.

Remarque 3.10. Les résultats précédents (Th. 3.3, Cor. 3.9) montrent qu'un corps de décomposition d'un polynôme non constant $f(X)$ de $K[X]$ est, à un K-isomorphisme près, la plus petite extension de K sur laquelle $f(X)$ est scindé.

Corollaire 3.11. *$f(X)$ étant un polynôme non constant de $K[X]$, si $f(X)$ est scindé sur un corps L, extension de K, alors L contient un corps de décomposition de f sur K.*

Démonstration. Soit E un corps de décomposition de $f(X)$ sur K. Les hypothèses du corollaire impliquent, d'après le lemme 3.7, qu'il existe un plongement $\mu : E \longrightarrow L$ tel que $\mu_{/K} = id_K$; donc $\mu(E)$ est un sous-corps de L, K-isomorphe à E. □

Exemple 3.12. (à vérifier)
1) Le corps $\mathbb{Q}(\sqrt[3]{2}, j) \subset \mathbb{C}$ est corps de décomposition sur $\mathbb{Q}$ du polynôme $X^3 - 2$.
2) $\mathbb{C}$ est corps de décomposition sur $\mathbb{R}$, du même polynôme $X^3 - 2$.

2. Extensions normales - Clôture normale

A. Extensions normales

Définition 3.13. Une extension L de K est dite **normale** sur K, si
i) L est algébrique sur K.
ii) Tout polynôme irréductible de $K[X]$, qui a une racine dans L, est scindé sur L.

Exemple 3.14. 1) On remarque que tout corps K est extension normale de lui-même ; en effet, K est algébrique sur K et de plus, tout polynôme irréductible de $K[X]$, qui a une racine dans K, est nécessairement de degré 1, donc est (trivialement) scindé sur K.
2) $\mathbb{C}$ est une extension normale de $\mathbb{R}$ (une justification rigoureuse en sera donnée dans le Ch. 5).
3) $\mathbb{Q}(\sqrt[3]{2})$ n'est pas une extension normale de $\mathbb{Q}$ (Cf. Exemple 2.19).

Théorème 3.15. *L étant une extension de K, alors L est* normale et de degré fini *sur K si et seulement si L est corps de décomposition sur K d'un polynôme de $K[X]$.*

Démonstration. – Supposons $L : K$ normale et de degré fini ; alors L est algébrique et de degré fini sur K, donc il existe un nombre fini d'éléments $\alpha_1, \ldots, \alpha_r$ dans L tels que (Th. 2.29)

$$L = K(\alpha_1, \ldots, \alpha_r), \quad r \in \mathbb{N}^*.$$

Chaque α_i, $1 \leq i \leq r$, est algébrique sur K ; posons $p_i(X) := Irr_K(\alpha_i, X)$.
Pour tout $i (1 \leq i \leq r)$, le polynôme irréductible p_i a une racine $\alpha_i \in L$; alors, L étant normale sur K, p_i est scindé sur L (Déf. 3.13). On en déduit que le polynôme

$$f(X) := p_1(X)p_2(X)\ldots p_r(X)$$

est scindé sur L, donc il existe un corps de décomposition E de f sur K tel que $K \subseteq E \subseteq L$ (cor. 3.11).
Mais $\alpha_1, \ldots, \alpha_r$ étant des racines de f dans L, on a (Prop. 3.5)

$$L = K(\alpha_1, \ldots, \alpha_r) \subseteq E, \quad \text{d'où } E = L.$$

– Réciproquement, soit L un corps de décomposition sur K d'un polynôme non constant $f(X)$ de $K[X]$. D'après la Prop. 3.5, L est une extension algébrique et de degré fini sur K et si $\beta_1, \ldots, \beta_s \, (s \in \mathbb{N}^*)$ sont les racines distinctes de f dans L, alors

$$L = K(\beta_1, \ldots, \beta_s). \tag{3.4}$$

Pour prouver que L est normale sur K, considérons un polynôme $p(X)$ irréductible dans $K[X]$, ayant une racine $\alpha \in L$ et démontrons que $p(X)$ est scindé sur L (Cf. Déf. 3.13). On peut supposer $p(X)$ unitaire (Rem. 2.22).
- Si $deg\, p = 1$, alors $p(X) = X - \alpha$ et la propriété est vérifiée.
- Supposons $deg\, p > 1$ et considérons le polynôme

$$g(X) := f(X)p(X), \quad \text{dans } K[X].$$

Par hypothèse, $f(X)$ est scindé sur L; désignons par M un corps de décomposition de $g(X)$ sur K contenant L.
Le polynôme $p(X)$, irréductible sur K, est alors scindé sur M et a au moins deux racines distinctes γ_1 et γ_2 dans M.
- Montrons que $[L(\gamma_1) : L] = [L(\gamma_2) : L]$. Pour $i = 1, 2$, on a

$$K \subseteq K(\gamma_i) \subseteq L(\gamma_i) \subseteq M \quad \text{et} \quad K \subseteq L \subseteq L(\gamma_i) \subseteq M, \tag{3.5}$$

$$\text{d'où} \quad [L(\gamma_i) : K] = [L(\gamma_i) : K(\gamma_i)][K(\gamma_i) : K] \tag{3.6}$$

$$= [L(\gamma_i) : L][L : K]. \tag{3.7}$$

Or, par hypothèse, $p(X)$ est irréductible et unitaire dans $K[X]$, donc

$$p(X) = Irr_K(\gamma_1, X) = Irr_K(\gamma_2, X),$$

ce qui entraîne (Th. 2.8 et 2.16)

$$[K(\gamma_1) : K] = [K(\gamma_2) : K] = deg\, p. \tag{3.8}$$

D'autre part, compte tenu de la relation (3.4), on a, pour $i = 1, 2$,

$$L(\gamma_i) = K(\beta_1, \ldots, \beta_s, \gamma_i) = K(\gamma_i)(\beta_1, \ldots, \beta_s) \quad \text{(Prop. 1.14)}.$$

Par suite, $L(\gamma_1)$ et $L(\gamma_2)$ sont corps de décomposition de $f(X)$, respectivement, sur les corps isomorphes $K(\gamma_1)$ et $K(\gamma_2)$ (Th. 2.16). On en déduit (Th. 3.8) que les extensions $L(\gamma_1) : K(\gamma_1)$ et $L(\gamma_2) : K(\gamma_2)$ sont isomorphes et en particulier

$$[L(\gamma_1) : K(\gamma_1)] = [L(\gamma_2) : K(\gamma_2]).$$

Cette dernière égalité, jointe aux relations (3.6), (3.7) et (3.8), donne

$$[L(\gamma_1) : L] = [L(\gamma_2) : L]. \tag{3.9}$$

Mais, par hypothèse, $p(X)$ a une racine α dans $L \subseteq M$, et d'après l'égalité (3.9), quelle que soit la racine γ de $p(X)$ dans M, on a

$$[L(\gamma) : L] = [L(\alpha) : L] = 1,$$

donc $\gamma \in L$. Ainsi $p(X)$ est scindé sur L, d'où L normale sur K (Déf. 3.13). □

B. Clôture normale

Définition 3.16. On appelle **clôture normale** d'une extension de corps $L : K$, une extension N de L telle que $K \subseteq L \subseteq N$ et
i) N est une extension normale de K ;
ii) ($L \subseteq M \subseteq N$ et M extension normale de K) $\Longrightarrow M = N$.

Théorème 3.17. *Pour toute extension de corps $L : K$, de degré fini, il existe une clôture normale, N, de degré fini sur K et unique à un K-isomorphisme près.*

Démonstration. Si $L : K$ est de degré fini, alors L est algébrique sur K et obtenu par l'adjonction à K d'un nombre fini d'éléments, algébriques sur K (Th. 2.29) ; supposons $[L : K] > 1$ et écrivons

$$L = K(\alpha_1, \ldots, \alpha_m),\ m \in \mathbb{N}^*, \alpha_i \text{ algébrique sur } K, \forall i, 1 \leq i \leq m.$$

Posons $\forall i, 1 \leq i \leq m,\ p_i(X) := Irr_K(\alpha_i, X)$ et $f(X) := \prod_{1 \leq i \leq m} p_i(X)$.

Les α_i, $1 \leq i \leq m$ étant des racines de $f(X)$, il existe un corps de décomposition N de $f(X)$ sur K contenant L, et l'extension $N : K$ est normale et de degré fini (Th. 3.15).
Supposons que M soit une extension de L telle que $L \subseteq M \subseteq N$ et M normale sur K, alors chaque polynôme $p_i(x)$, ayant une racine α_i dans M, est scindé sur M. Par suite, $f(X)$ est scindé sur M. On en conclut (Th. 3.3) que $M = N$.
Si N' est une clôture normale de $L : K$ telle que $N' \neq N$, alors

$$L = K(\alpha_1, \ldots, \alpha_m) \subseteq N'$$

implique l'existence d'un corps de décomposition E, de $f(X)$ sur K, vérifiant $L \subseteq E \subseteq N'$.
L'extension $E : K$ est normale et de degré fini, d'où $E = N'$ (Déf. 3.16).
Ainsi, N et N' sont deux corps de décomposition de $f(X)$ sur K, donc N et N' sont K-isomorphes (Cor. 3.9). □

Remarque 3.18. a) Pour une extension de degré fini $L : K$, une clôture normale est, à un K-isomorphisme près, la plus petite extension de L normale et de degré fini sur K.
b) La preuve du Th. 3.17 montre que si $L = K(\alpha)$, alors N est une clôture normale de $K(\alpha)$ sur K si et seulement si N est corps de décomposition sur K du polynôme $Irr_K(\alpha, X)$.

Exemple 3.19. Soit $\alpha := \sqrt[3]{2}$ dans $\mathbb{R}$; alors $\mathbb{Q}(\alpha)$ n'est pas une extension normale de $\mathbb{Q}$, car le polynôme $X^3 - 2$, irréductible sur $\mathbb{Q}$, n'a qu'une seule racine dans $\mathbb{Q}(\alpha)$.
Cependant, si j et j^2 désignent les racines cubiques non réelles de l'unité, dans $\mathbb{C}$, alors $N := \mathbb{Q}(\alpha, \alpha j, \alpha j^2) = \mathbb{Q}(\alpha, j)$ est corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$, donc N est la clôture normale de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$, contenue dans $\mathbb{C}$.

3. Extensions séparables

A. Polynômes irréductibles séparables

Définition 3.20. 1) On dit qu'un polynôme irréductible de $K[X]$ est **séparable** sur K s'il n'a que des racines simples ([13], Déf. 4.41) dans un corps de décomposition sur K.
2) Un polynôme irréductible de $K[X]$, qui n'est pas séparable sur K, sera dit **inséparable** sur K.

Exemple 3.21. 1) Soit $X^5 - 1$ dans $\mathbb{Q}[X]$; on a

$$X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1).$$

Le polynôme $p(X) := X^4 + X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{Q}$ (Cf. [13]) et ses racines sont les $\exp\frac{2k\pi i}{5}$, $1 \leq k \leq 4$, deux à deux distinctes dans $\mathbb{C}$.

Le polynôme irréductible $p(X)$ est donc séparable sur $\mathbb{Q}$.

2) Il s'agit d'un exemple de polynôme irréductible inséparable.
Soit p un nombre premier *impair* ; posons $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
Soit t un élément appartenant à une extension de $\mathbb{F}_p$ et *transcendant* sur $\mathbb{F}_p$. On considère l'extension simple transcendante de $\mathbb{F}_p$ obtenue par l'adjonction de t et on pose

$$K := \mathbb{F}_p(t).$$

Soit $f(X) := X^p - t$ dans $K[X]$.
Désignons par E un corps de décomposition de f sur K et soit α une racine de f dans E ; donc $\alpha^p = t$.
Or, d'après la définition de K, on a $car K = p > 2$; par suite, dans $K[X]$ ([13], Prop. 1.72) :

$$(X-\alpha)^p = X^p - \alpha^p = X^p - t = f(X).$$

Quelle que soit la racine β de $f(X)$ dans E, on a

$$0 = \beta^p - t = \beta^p - \alpha^p = (\beta - \alpha)^p.$$

Un corps n'a pas de diviseur de zéro, donc

$$(\beta - \alpha)^p = 0 \Longrightarrow \beta = \alpha.$$

On en conclut que le polynôme f a p racines égales à α dans E.

Démontrons, maintenant, que le polynôme f est irréductible sur K.
Supposons f réductible sur K, donc dans $K[X]$,

$$f(X) = g(X)h(X), \quad \text{avec} \quad 1 \leq deg\, g < p, \ 1 \leq deg\, h < p.$$

Compte tenu de l'unicité de la factorisation de $f(X)$ dans $E[X]$,

$$f(X) = (X-\alpha)^p \Longrightarrow g(X) = (X-\alpha)^s, \ 1 \leq s < p.$$

$g(X)$ est un polynôme de $K[X]$, donc son terme constant $(-1)^s\alpha^s$ est dans K ; montrons qu'alors, $\alpha \in K$. En effet, p étant un nombre premier,

$$1 \leq s < p \Longrightarrow p \wedge s = 1.$$

D'après le théorème de Bezout ([13], App. A, Th. 0.31), il existe a et b dans $\mathbb{Z}$ tels que $as + bp = 1$, d'où

$$(\alpha = \alpha^{(as+bp)} = (\alpha^s)^a(\alpha^p)^b \quad \text{et} \quad \alpha^s \in K, \ \alpha^p = t \in K) \Longrightarrow \alpha \in K.$$

Montrons que ce résultat conduit à une contradiction.
Par hypothèse, t est transcendant sur $\mathbb{F}_p$, d'où (Th. 2.5)

$$K = \mathbb{F}_p(t) = \left\{ \frac{v(t)}{w(t)} \, ; \, \frac{v(X)}{w(X)} \in \mathbb{F}_p(X) \right\}.$$

$\alpha \in K$, donc il existe $\dfrac{v(X)}{w(X)} \in \mathbb{F}_p[X]$ tel que $\alpha = \dfrac{v(t)}{w(t)}$.

$$\alpha^p = t \iff \big(v(t)\big)^p - t\big(w(t)\big)^p = 0.$$

L'élément t est transcendant sur $\mathbb{F}_p$, donc t n'est annulé par aucun polynôme non nul de $\mathbb{F}_p[X]$; vérifions que $(v(X))^p - X(w(X))^p$ n'est pas le polynôme nul.
Dans l'anneau factoriel $\mathbb{F}_p[X]$, X est un élément irréductible et les polynômes $v(X)$ et $w(X)$ s'écrivent de façon unique, à l'ordre près des facteurs :

$$v(X) = q_1(X)\dots q_k(X); \qquad w(x) = r_1(X)\dots r_l(X);$$

les $q_i, 1 \le i \le k$, et les $r_j, 1 \le j \le l$, étant irréductibles dans $\mathbb{F}_p[X]$ et définis à une unité multiplicative près ([13], Ch. 5).
Si $(v(X))^p - X(w(X))^p = 0$, alors,

$$(q_1(X))^p \dots (q_k(X))^p = X(r_1(X))^p \dots (r_l(X))^p.$$

On en déduit que ([13], Prop. 5.26) $kp = 1 + lp$, d'où $p(k-l) = 1$, ce qui est impossible, puisque p est premier dans $\mathbb{Z}$.
On en conclut que que le polynôme $f(X) = X^p - t$ est irréductible et inséparable sur $K = \mathbb{F}_p(t)$.

Remarque 3.22. Dans tout ce qui suit, K désigne, de nouveau, un corps quelconque.
On rappelle qu'un polynôme f, non constant de $K[X]$, n'a que des racines simples dans un corps de décomposition sur K si et seulement si son polynôme dérivé f' vérifie ([13], Cor. 8.49) :

$$f' \neq 0 \quad \text{et} \quad f \wedge f' = 1.$$

Proposition 3.23. *Soit $f(X) \in K[X] \setminus K$ et $f'(X)$ son polynôme dérivé ; alors,*
1) $car K = 0 \Longrightarrow f'(X) \neq 0$.
2) $car K = p \neq 0 \Longrightarrow (f'(X) = 0 \iff f(X) = g(X^p))$,
où $g(X)$ est un polynôme de $K[X]$.

Démonstration. Posons $n := deg\, f > 0$; alors dans $K[X]$,

$$\Big(f(X) = \sum_{0 \le i \le n} a_i X^i,\ a_n \neq 0\Big) \Longrightarrow f'(X) = \sum_{1 \le i \le n} i a_i X^{i-1}.$$

1) $car K = 0$; alors, $a_n \neq 0 \Longrightarrow n a_n \neq 0 \Longrightarrow f'(X) \neq 0$.
2) $car K$ est un nombre premier p ; l'expression de $f'(X)$ implique

$$\begin{aligned} f'(X) = 0 &\iff \forall i (1 \le i \le n),\ i a_i = 0 \\ &\iff \forall i (1 \le i \le n),\ (a_i = 0 \text{ ou } p \mid i). \end{aligned}$$

On en déduit que

$$\begin{aligned} f'(X) = 0 &\iff f(X) = \sum_{0 \le k \le r} b_k X^{kp}, \text{ où } r \in \mathbb{N}^*,\ b_k \in K,\ \forall k (0 \le k \le r) \\ &\iff f(X) = g(X^p), \quad \text{où} \quad g(X) = \sum_{0 \le k \le r} b_k X^k. \end{aligned}$$

□

Théorème 3.24. *K étant un corps,*
– Si $car K = 0$, alors tout polynôme irréductible de $K[X]$ est séparable *sur K.*
– Si $car K = p \neq 0$, alors un polynôme irréductible $f(X)$ de $K[X]$ est inséparable *sur K si et seulement si*

$$f(X) = g(X^p), \quad \text{où} \quad g(X) \in K[X].$$

Démonstration. – Si $carK = 0$ et si $f(X)$ est un polynôme irréductible de $K[X]$, alors f est non constant, donc f' est non nul (Prop. 3.23) et

$$deg\, f' < deg\, f \Longrightarrow f \nmid f', \text{ dans } K[X].$$

L'irréductibilité du polynôme f implique alors : $f \wedge f' = 1$ ([13], Prop. 5.47). On en conclut que f est séparable sur K (Rem. 3.22).
– Si $carK = p \neq 0$, pour un polynôme $f(X)$ irréductible de $K[X]$, deux cas sont possibles :
a) $f'(X) \neq 0$, alors comme dans le cas de la caractéristique nulle, $f \wedge f' = 1$,
donc f est séparable sur K.
b) $f'(X) = 0$, alors le polynôme irréductible f a au moins une racine multiple dans un corps de décomposition sur K (Rem. 3.22.), donc est inséparable sur K et (Prop. 3.23) $f'(X) = 0$ si et seulement si

$$f(X) = g(X^p), \quad \text{où} \quad g(X) \in K[X]. \qquad \square$$

B. Notion d'extension séparable – Corps parfaits

Définition 3.25. :
1) Un **polynôme** $f(X) \in K[X] \setminus K$ sera dit **séparable** sur K si tous ses diviseurs irréductibles sont séparables sur K.
2) Etant donné une extension L de K, on dit qu'un **élément** $\alpha \in L$ est **séparable** sur K si α est algébrique sur K et le polynôme $Irr_K(\alpha, X)$ est séparable sur K.
3) On dit qu'une **extension** L de K est **séparable** sur K(ou que l'extension $L : K$ est séparable) si tout $\alpha \in L$ est séparable sur K.
4) Un corps K est dit **parfait** si toute extension algébrique de K est séparable sur K.

Remarque 3.26. :
a) D'après la Déf. 3.25., 1), un polynôme séparable, qui n'est pas irréductible, n'a pas nécessairement que des racines simples dans un corps de décomposition.
b) Dans la Déf. 3.25., 2), 3) impliquent que toute extension séparable sur K est algébrique sur K.

Théorème 3.27. *Un corps K est* parfait *si et seulement si*

$$carK = 0 \quad ou \quad carK = p \neq 0 \quad et \quad K = \{a^p \,;\, a \in K\}.$$

Démonstration. Soit L une extension algébrique de K.
– Si $carK = 0$, alors tout élément de L est séparable sur K (Th. 3.24), donc $L : K$ est séparable et K est un corps parfait.
– Si $carK = p > 0$, posons $K^p := \{a^p \,;\, a \in K\}$ et supposons $K = K^p$; soit $\alpha \in L$ et $q(X) := Irr_K(\alpha, X)$.
Si $q(X)$ est inséparable sur K, alors $q(X)$ est de la forme (Th. 3.24)

$$q(X) = \sum_{0 \leq k \leq r} b_k X^{kp}, \text{ où } r \in \mathbb{N}^*,\ b_k \in K,\ \forall k (0 \leq k \leq r). \tag{3.10}$$

$$K = K^p \Longrightarrow \forall k (0 \leq k \leq r),\ \exists c_k \in K, \text{ tel que } b_k = {c_k}^p, \tag{3.11}$$

$$\text{d'où} \quad q(X) = \sum_{0 \leq k \leq r} {c_k}^p (X^k)^p = \Big(\sum_{0 \leq k \leq r} c_k X^k \Big)^p, \tag{3.12}$$

puisque $carK = p$ ([13], Prop. 1.72). Le résultat (3.12) est alors en contradiction avec l'irréductibilité de $q(X)$ dans $K[X]$, donc $q(X)$ est séparable sur K; par suite, L est séparable sur K et K est un corps parfait.
Réciproquement, considérons un corps parfait K; alors, $carK = 0$ ou $carK = p$ non nul. Montrons que, dans le second cas, on a $K = K^p$.
Soit $b \in K$; si $b = 0$, alors $b = 0^p$; on suppose donc $b \neq 0$ et on considère le polynôme $X^p - b$.
Dans l'anneau factoriel $K[X]$, il existe au moins un polynôme *irréductible* $q(X)$ divisant $X^p - b$ et on peut supposer $q(X)$ unitaire.
Soit a, appartenant à une extension de K, tel que $q(a) = 0$; alors a est aussi une racine du polynôme $X^p - b$ et dans $K(a)[X]$, on a

$$X^p - b = X^p - a^p = (X-a)^p, \quad \text{puisque } carK = p.$$
$$q(X) \mid X^p - b \Longrightarrow q(X) = (X-a)^m,\ 1 \leq m \leq p.$$

Mais K étant parfait par hypothèse, $q(X)$ est séparable sur K, d'où nécessairement, $m = 1$, donc $a \in K$ et $a^p = b$; par suite, $K = K^p$. □

Remarque 3.28. Si K est un corps tel que $carK = p \neq 0$ et $K = K^p$, alors
$K = K^{p^n} := \{a^{p^n}\ ;\ a \in K\}$, quel que soit l'entier $n > 0$.

Théorème 3.29. *Etant donné des extensions de corps $L : K$ et $M : L$, on a*

$$M : K \text{ séparable} \Longrightarrow M : L \text{ et } L : K \text{ séparables.}$$

Démonstration. On peut supposer $K \subseteq L \subseteq M$. Il est immédiat que

$$(L \subseteq M \text{ et } M \text{ séparable sur } K) \Longrightarrow L \text{ séparable sur } K.$$

Montrons que M est séparable sur L.
Soit $\alpha \in M$; par hypothèse $M : K$ est séparable, donc α est algébrique sur K. Posons $p_\alpha(X) := Irr_K(\alpha, X)$.

$$\big(p_\alpha(X) \in K[X] \text{ et } K \subseteq L\big) \Longrightarrow p_\alpha(X) \in L[X]$$
$$\text{et} \qquad p_\alpha(\alpha) = 0 \Longrightarrow \alpha \text{ algébrique sur } L.$$

Posons $q_\alpha(X) := Irr_L(\alpha, X)$; dans $L[X]$, on a (Th. 2.8)

$$\big(q_\alpha(X) = Irr_L(\alpha, X) \text{ et } p_\alpha(\alpha) = 0\big) \Longrightarrow q_\alpha(X) \mid p_\alpha(X).$$

$\alpha \in M$ et M est séparable sur K, donc $p_\alpha(X)$ est un polynôme irréductible séparable sur K. On en déduit que

$$\big(q_\alpha(X) \mid p_\alpha(X) \text{ dans } L[X]\big) \Longrightarrow q_\alpha(X) \text{ séparable sur } L,$$

d'où α séparable sur L, et par suite, $M : L$ est séparable. □

Proposition 3.30. *Soit $L : K$ une extension de degré fini, normale et séparable, alors L est corps de décomposition sur K d'un polynôme séparable.*

Démonstration. On suppose $[L : K] > 1$; L est normal et de degré fini sur K, donc L est corps de décomposition d'un polynôme non constant, $f(X)$, de $K[X]$ (Th. 3.15).
De plus, L est séparable sur K, par suite, tout facteur irréductible de $f(X)$ étant scindé sur L, est séparable sur K. On en conclut que $f(X)$ est séparable sur K (Déf. 3.25). □

La réciproque de la Prop. 3.30 *sera démontrée au* Ch. 7 (Th. 7.20).

Théorème 3.31. Théorème de l'élément primitif
Soit L une extension d'un corps K telle que

$$[L:K] < \infty \quad et \quad L : K \text{ séparable},$$

alors L est une extension simple de K.

Démonstration. Dans cette preuve, nous supposons K de *cardinal infini* ; dans le cas d'un corps fini, le théorème résulte de propriétés qui seront vues au Ch. 4. (Rem. 4.14).
Posons $[L:K] = n > 1$.
– Etudions le cas où $n = 2$. Soit $\{\alpha, \beta\}$ une base de L sur K, alors $L = K(\alpha, \beta)$ (Rem. 1.25).
Les hypothèses impliquent que L est algébrique sur K; posons

$$p_\alpha(X) := Irr_K(\alpha, X) \; ; \; p_\beta(X) := Irr_K(\beta, X) \quad \text{et} \quad f(X) := p_\alpha(X)\, p_\beta(X).$$

Soit M un corps de décomposition sur K du polynôme $f(X)$ contenant L.
Posons $deg\, p_\alpha = r > 0$ et $deg\, p_\beta = s > 0$; soit

$$\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r \text{ les racines de } p_\alpha(X) \text{ dans } M,$$
$$\beta_1 = \beta, \beta_2, \ldots, \beta_s \text{ les racines de } p_\beta(X) \text{ dans } M.$$

L est séparable sur K, donc les $\alpha_i, 1 \le i \le r$, (resp. $\beta_j, 1 \le j \le s$) sont deux à deux distincts dans M et (Prop. 3.5)

$$M = K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s).$$

Montrons qu'il existe $t \in K^*$ tel que

$$\forall (i,j)\, (2 \le i \le r,\, 2 \le j \le s),\; \alpha_i + t\beta_j \neq \alpha + t\beta. \tag{3.13}$$

En effet, l'ensemble

$$\Phi = \left\{ -\frac{\alpha - \alpha_i}{\beta - \beta_j} ;\, 2 \le i \le r,\, 2 \le j \le s \right\} \tag{3.14}$$

est une partie *finie*, non vide de $M^* = M \setminus \{0\}$; or le corps K étant de cardinal infini, il existe nécessairement $t \in K^*$ tel que $t \notin \Phi$ et

$$t \notin \Phi \Longrightarrow \alpha + t\beta \neq \alpha_i + t\beta_j,\; \forall (i,j)\, (2 \le i \le r,\, 2 \le j \le s).$$

Pour t fixé dans K et vérifiant la condition (3.13), posons $\theta := \alpha + t\beta$; on a alors

$$\theta - t\beta_j \neq \alpha_i,\; \forall (i,j)\, (2 \le i \le r,\, 2 \le j \le s).$$

Considérons le polynôme composé ([13], Ch. 4) $h(X) := p_\alpha(\theta - tX)$ dans $K(\theta)[X]$; alors

$$h(\beta) = p_\alpha(\alpha) = 0 \quad \text{et} \quad \forall j (2 \le j \le s),\; h(\beta_j) = p_\alpha(\theta - t\beta_j) \neq 0.$$

On en déduit que β est algébrique sur $K(\theta)$ et que β est la seule racine commune aux polynômes $h(X)$ et $p_\beta(X)$ de $K(\theta)[X]$. On pose $\mu(X) := Irr_{K(\theta)}(\beta, X)$.

$$p_\beta(\beta) = 0 \Longrightarrow \mu(X) \mid p_\beta(X), \text{ dans } K(\theta)[X],$$
$$h(\beta) = 0 \Longrightarrow \mu(X) \mid h(X), \text{ dans } K(\theta)[X].$$

Toute racine de $\mu(X)$ est donc une racine commune aux polynômes $h(X)$ et $p_\beta(X)$. D'autre part, L est séparable sur K, donc séparable sur $K(\theta)$, par suite, nécessairement, $\mu(X) = X - \beta$. On en déduit que $\beta \in K(\theta)$; alors,

$$\big(\theta = \alpha + t\beta \quad \text{et} \quad t \in K^*\big) \Longrightarrow \alpha \in K(\theta),$$

d'où $K(\alpha,\beta) = K(\theta)$; ainsi le théorème est démontré pour $n = 2$.

– Pour $n > 2$, on peut écrire $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, où $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ est une base de L sur K et on raisonne par récurrence sur n.
On suppose la propriété vraie pour toute extension séparable de K, de degré $n-1$; en particulier, il existe un élément $\theta \in K(\alpha_1, \ldots, \alpha_{n-1})$ tel que

$$K(\alpha_1, \ldots, \alpha_{n-1}) = K(\theta);$$

alors $L = K(\theta, \alpha_n)$ et d'après l'étude du cas « $n = 2$ », il existe un certain $\lambda \in L$ tel que $L = K(\lambda)$. □

Définition 3.32. Pour une extension $L : K$ séparable et de degré fini, on dit que $\lambda \in L$ est un **élément primitif**, si $L = K(\lambda)$.

Exemple 3.33. Dans la remarque 1.19., on a montré que

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}),$$

donc $\sqrt{2} + \sqrt{3}$ est un élément primitif pour l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$.

4. Extensions purement inséparables

Définition 3.34. Soit $L : K$ une extension de corps ;
1) Un **élement** $\alpha \in L$ est dit **purement inséparable** sur K si
i) α est algébrique sur K,
ii) il existe $m \in \mathbb{N}^*$ tel que $Irr_K(\alpha, X) = (X - \alpha)^m$, dans $L(X)$.
2) L' **extension** L de K est **purement inséparable** sur K si tout $\alpha \in L$ est purement inséparable sur K.

Remarque 3.35. Compte tenu du 1) de la Déf. 3.34, toute extension $L : K$ purement inséparable est une extension algébrique.

Proposition 3.36. *Etant donné une extension de corps $L : K$, un élément $\alpha \in L$ est à la fois,* purement inséparable *et* séparable *sur K, si et seulement si $\alpha \in K$.*

Démonstration. Les Déf. 3.34. et 3.20., impliquent que $\alpha \in L$ est à la fois, purement inséparable et séparable sur K, si et seulement si

$$\alpha \text{ est algébrique sur } K \text{ et } Irr_K(\alpha, X) = X - \alpha,$$

c'est-à-dire $\alpha \in K$. □

Remarque 3.37. Si K est un corps *parfait* (Déf. 3.25, 4)), toute extension algébrique L de K est séparable, donc les seuls éléments de L purement inséparables sur K sont les éléments de K, ce qui ne présente pas un grand intérêt.

En conséquence, nous supposerons, dans tout ce paragraphe, que *K n'est pas un corps parfait*, autrement dit (Th. 3.27),

$$car K = p \neq 0 \quad \text{et} \quad K \neq K^p \quad (K^p = \{a^p \,;\, a \in K\}). \tag{3.15}$$

Proposition 3.38. *Soit L une extension d'un corps K vérifiant* (3.15), *et un élément $\alpha \in L$ algébrique sur K ; il existe alors $k \in \mathbb{N}$ tel que α^{p^k} est séparable sur K.*

Démonstration. Posons $f_\alpha(X) := Irr_K(\alpha, X)$ et $n := deg\, f_\alpha$.
- Si $n = 1, f_\alpha(X) = X - \alpha$, donc $\alpha \in K$ est séparable sur K.
- Pour $n > 1$, raisonnons par récurrence sur n.

Si α est séparable sur K, la propriété est vérifiée avec $k = 0$.
Si α est inséparable sur K, alors (Th. 3.24)

$$f_\alpha(X) = g(X^p), \text{ où } g(X) \in K[X].$$

On en déduit que, dans $K[X]$, on a $deg\, g < deg\, f_\alpha$ et $f_\alpha(X)$ irréductible et unitaire implique $g(X)$ irréductible et unitaire. Par suite,

$$g(\alpha^p) = 0 \Longrightarrow g(X) = Irr_K(\alpha^p, X)$$

et l'hypothèse de récurrence implique qu'il existe $k' \in \mathbb{N}$ tel que

$$(\alpha^p)^{p^{k'}} \text{ est séparable sur } K,$$

d'où α^{p^k} séparable sur K, pour $k = k' + 1$. □

Théorème 3.39. *Etant donné une extension L d'un corps K vérifiant* (3.15), *un élément $\alpha \in L$ est* purement inséparable *sur K si et seulement s'il existe $r \in \mathbb{N}$ et $a \in K$ tels que*

$$f_\alpha(X) := Irr_K(\alpha, X) = X^{p^r} - a.$$

Démonstration. Supposons α purement inséparable sur K ; il existe $m \in \mathbb{N}^*$, tel que

$$f_\alpha(X) = (X - \alpha)^m, \quad \text{dans } L[X].$$

L' entier m s'écrit de façon unique

$$m = sp^r, \quad \text{où} \quad r \in \mathbb{N} \quad \text{et} \quad p \nmid s, \text{ dans } \mathbb{N}^*, \quad \text{d'où}$$

$$f_\alpha(X) = (X - \alpha)^{sp^r} = (X^{p^r} - \alpha^{p^r})^s, \quad \text{dans } L[X].$$

Or, les coefficients du polynôme $f_\alpha(X)$ sont dans K, donc en particulier, le coefficient de $X^{(s-1)p^r}$, c'est-à-dire $\pm s\alpha^{p^r}$, appartient à K ; alors

$$p \wedge s = 1 \Longrightarrow s1_K \neq 0 \Longrightarrow \alpha^{p^r} \in K;$$
$$(X - \alpha)^m = (X^{p^r} - \alpha^{p^r})^s \text{ irréductible sur } K \Longrightarrow s = 1,$$
$$\text{d'où} \quad f_\alpha(X) = (X - \alpha)^m = X^{p^r} - a, \text{ où } a := \alpha^{p^r} \in K.$$

Réciproquement, si $\alpha \in L$ et $f_\alpha(X) = X^{p^r} - a$, dans $K[X]$, alors $a = \alpha^{p^r}$; par suite

$$f_\alpha(X) = X^{p^r} - \alpha^{p^r} = (X - \alpha)^{p^r},$$

donc α est purement inséparable sur K. □

Théorème 3.40. *K étant un corps vérifiant* (3.15), *si $L : K$ est une extension purement inséparable, de degré fini, alors $[L : K]$ est une puissance de p.*

Démonstration. L'hypothèse $[L : K] < \infty$ implique que L est obtenue par l'adjonction à K d'un nombre fini d'éléments algébriques sur K (Th. 2.29) :

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_n), \quad n \in \mathbb{N}^*.$$

Posons $K_1 := K(\alpha_1), K_2 := K_1(\alpha_2), \ldots, K_n := K_{n-1}(\alpha_n) = L$.
Par hypothèse α_1 est purement inséparable sur K ; montrons que pour tout $j (2 \leq j \leq n)$, α_j est purement inséparable sur K_{j-1}.
Etant donné $j (2 \leq j \leq n)$, posons

$$f_j(X) := Irr_K(\alpha_j, X) \quad \text{et} \quad g_j(X) := Irr_{K_{j-1}}(\alpha_j, X).$$

α_j est purement inséparable sur K, donc dans $K_j[X]$, on a

$$f_j(X) = (X - \alpha_j)^{m_j}, \quad \text{où} \quad m_j \in \mathbb{N}^*.$$

D'autre part, dans $K_{j-1}[X]$,

$$\big(g_j(X) = Irr_{K_{j-1}}(\alpha_j, X) \text{ et } f_j(\alpha_j) = 0\big) \Longrightarrow g_j(X) \mid f_j(X),$$

$$\text{d'où,} \quad g_j(X) = (X - \alpha_j)^{m'_j}, \quad 1 \leq m'_j \leq m_j, \text{ dans } \mathbb{N}.$$

Par suite, α_j est purement inséparable sur K_{j-1}.

Posons $K_0 := K$; d'après le Th. 3.39, pour tout $j\,(1 \leq j \leq n)$, il existe $r_j \in \mathbb{N}$ et $a_j \in K_{j-1}$ tels que

$$g_j(X) = X^{p^{r_j}} - a_j.$$

On en déduit que

$$\forall j (1 \leq j \leq n),\ [K_j : K_{j-1}] = [K_{j-1}(\alpha_j) : K_{j-1}] = p^{r_j}.$$

Par suite,

$$[L : K] = [K_n : K] = \prod_{1 \leq j \leq n} [K_j : K_{j-1}] = \prod_{1 \leq j \leq n} p^{r_j},$$

donc $[L : K]$ est une puissance de p. □

Théorème 3.41. *K étant un corps vérifiant* (3.15), *soit $a \in K \setminus K^p$; alors, pour tout entier $n \geq 0$, le polynôme $f(X) := X^{p^n} - a$ est irréductible sur K.*

Démonstration. Soit $q(X)$ un diviseur irréductible et unitaire de $f(X)$ dans $K[X]$ et soit $K(\alpha)$ un corps de rupture de $q(X)$ (Déf. 2.21).

$$q(\alpha) = 0 \Longrightarrow f(\alpha) = 0 = \alpha^{p^n} - a.$$

Dans $K(\alpha)[X]$, on a

$$f(X) = X^{p^n} - \alpha^{p^n} = (X - \alpha)^{p^n}, \text{ puisque } car K = p.$$

Par suite, tout diviseur, irréductible et unitaire $h(X)$ de $f(X)$ dans $K[X]$ s'écrit, dans $K(\alpha)[X]$,

$$h(X) = (X - \alpha)^{p^m},\ 0 \leq m \leq n \quad \text{dans } \mathbb{N};$$

$$\text{alors} \quad h(\alpha) = 0 \Longrightarrow q(X) \mid h(X) \quad \text{dans } K[X].$$

Les polynômes $q(X)$ et $h(X)$ étant irréductibles et unitaires dans $K[X]$, on en déduit que $q(X) = h(X)$. Ainsi $f(X)$ est nécessairement une puissance de $q(X)$:

$$f(X) = \big(q(X)\big)^k,\ k \in \mathbb{N}^*, \quad \text{et} \quad deg\, f = p^n \Longrightarrow k\, deg\, q = p^n.$$

Par suite, les entiers k et $deg\, q$ sont des puissances de p ; d'où

$$f(X) = \big(q(X)\big)^{p^r}, \quad \text{pour un certain } r \in \mathbb{N}.$$

Soit $c \in K$, le terme constant de $q(X)$; le terme constant de $f(X)$ est alors

$$a = (\pm c)^{p^r}, \quad \text{où} \quad r \in \mathbb{N}.$$

En supposant $r > 0$, on aurait $a \in K^p$, ce qui est contraire à l'hypothèse, donc $r = 0$ et $f(X) = X^{p^n} - a = q(X)$ est irréductible dans $K[X]$. □

Théorème 3.42. *Soit L une extension d'un corps K vérifiant* (3.15), *alors $\alpha \in L$ est purement inséparable sur K si et seulement s'il existe $r \in \mathbb{N}$ tel que $\alpha^{p^r} \in K$.*

Démonstration. D'après le Th. 3.39, si α est un élément de L purement inséparable sur K, alors il existe un entier $r \geq 0$ et $a \in K$ tels que

$$f_\alpha(X) = Irr_K(\alpha, X) = X^{p^r} - a,$$

donc $\alpha^{p^r} = a \in K$.

On remarque que r est alors le plus petit élément de $\mathbb{N}$ tel que $\alpha^{p^r} \in K$.

En effet, s'il existait un entier r' tel que $0 \leq r' < r$ et $\alpha^{p^{r'}} = b \in K$, α serait racine du

polynôme $g(X) := X^{p^r} - b \in K[X]$, de degré strictement inférieur à celui $f_\alpha(X)$, ce qui est impossible.

Réciproquement, soit $\alpha \in L$ tel que $\alpha^{p^r} \in K$, pour un certain entier $r \geq 0$. On peut supposer que r est le plus petit élément de $\mathbb{N}$ satisfaisant à cette condition.
Si $r = 0$, alors $\alpha \in K$, donc α est purement inséparable sur K.
Si $r > 0$ et $\alpha^{p^r} \in K$, supposons que $\alpha^{p^r} \in K^p$; il existe alors $b \in K$ tel que $\alpha^{p^r} = b^p$, ce qui implique $\alpha^{p^{r-1}} = b \in K$, d'où une contradiction avec l'hypothèse de minimalité faite sur r. On en déduit que

$$(r > 0 \quad \text{et} \quad \alpha^{p^r} \in K) \Longrightarrow \alpha^{p^r} \notin K^p.$$

D'après le Th. 3.41., le polynôme $X^{p^r} - \alpha^{p^r}$ est irréductible sur K, et nécessairement

$$Irr_K(\alpha, X) = X^{p^r} - \alpha^{p^r} = (X - \alpha)^{p^r},$$

donc α est purement inséparable sur K. □

5. Exercices

1. Soit $f(X) = X^4 + X^2 + 1$ dans $\mathbb{Q}[X]$.
1°) $f(X)$ est-il irréductible dans $\mathbb{Q}[X]$?
2°) Existe-t-il des racines de f(X) dans $\mathbb{Q}$? ou dans $\mathbb{R}$?
3°) Vérifier qu'il existe un corps de décomposition F, de $f(X)$ sur $\mathbb{Q}$, contenu dans $\mathbb{C}$. Déterminer $[F : \mathbb{Q}]$.

2. K étant un corps, soit $f(X) \in K[X]$ tel que $deg\, f = n \geq 1$.
Démontrer que $f(X)$ est irréductible dans $K[X]$ si et seulement s'il n'a aucune racine dans les extensions L de K telles que

$$[L : K] \leq [\frac{n}{2}], \quad \text{où } [\frac{n}{2}] \text{ désigne la partie entière de } \frac{n}{2}.$$

3. Soit $f(X) \in K[X]$ où K est un corps ; on suppose $deg\, f = n \geq 1$.
1°) Soit $p_1(X)$ un diviseur irréductible et unitaire de $f(X)$ dans $K[X]$.
a) On note L_1 un corps de rupture de $p_1(X)$ sur K ; montrer que

$$1 \leq [L_1 : K] \leq n.$$

b) Soit F un corps de décomposition de $f(X)$ sur K. Démontrer que

$$1 \leq [F : K] \leq n!.$$

2°) On suppose que le polynôme f est irréductible sur K ; prouver que l'on a alors,

$$n \leq [F : K] \leq n! \quad \text{et} \quad n \text{ divise } [F : K].$$

3°) Vérifier que les polynômes

$$f(X) = X^3 - 2 \quad \text{et} \quad g(X) = X^4 - 2$$

sont irréductibles sur $\mathbb{Q}$.
F (resp. E) désignant un corps de décomposition de f (resp. g) sur $\mathbb{Q}$, déterminer

$$[F : \mathbb{Q}] \quad \text{et} \quad [E : \mathbb{Q}].$$

4. Soit $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ le corps à 2 éléments ; on pose $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$.
Dans $\mathbb{F}_2[X]$, on considère le polynôme $f(X) := X^2 + X + 1$.
1°) Vérifier que $f(X)$ est irréductible sur $\mathbb{F}_2$. Etant donné une racine α de $f(X)$ dans une extension de $\mathbb{F}_2$, préciser le degré de $\mathbb{F}_2(\alpha)$ sur $\mathbb{F}_2$.
2°) a) Montrer que $\mathbb{F}_2(\alpha)$ est corps de décomposition de $f(X)$ sur $\mathbb{F}_2$ et écrire la factorisation de $f(X)$ dans $\mathbb{F}_2(\alpha)[X]$.

b) Soit $K := \{0, 1, \alpha, \alpha + 1\}$. En écrivant les tables d'addition et de multiplication des éléments de K, montrer que K est un sous-corps de $\mathbb{F}_2(\alpha)$; en déduire l'égalité $\mathbb{F}_2(\alpha) = K$.

5. Soit $\gamma := \sqrt{2+\sqrt{2}}$ dans $\mathbb{R}$.
1°) Déterminer $p(X) := Irr_{\mathbb{Q}}(\gamma, X)$.
2°) Montrer que le polynôme $p(X)$ a un corps de décomposition K sur $\mathbb{Q}$ tel que

$$\mathbb{Q} \subset K \subset \mathbb{R}.$$

Préciser le corps K et déterminer $[K : \mathbb{Q}]$.

6. Soit $f(X) = X^4 + 4X^2 + 2$ dans $\mathbb{Q}[X]$.
1°) Vérifier que $f(X)$ est irréductible sur $\mathbb{Q}$ ([13], Prop. 5.112 et 5.108) et réductible (c'est-à-dire non irréductible) sur $\mathbb{Q}(\sqrt{2})$.
2°) Trouver un corps de décomposition F de $f(X)$ sur $\mathbb{Q}$ tel que

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset F \subset \mathbb{C}.$$

– Préciser les degrés $[F : \mathbb{Q}]$ et $[F : \mathbb{Q}(\sqrt{2})]$.
– F est-il corps de décomposition de $f(X)$ sur $\mathbb{Q}(\sqrt{2})$?

7. Soit $K := \mathbb{Q}(i, j, \sqrt{2})$, où $i^2 = -1$, $j^3 = 1, j \neq 1$, dans $\mathbb{C}$.
1°) a) Vérifier que K est une extension algébrique, de degré fini sur $\mathbb{Q}$. Calculer $[K : \mathbb{Q}]$.
b) Justifier l'existence d'un élément $\lambda \in K$ tel que $K = \mathbb{Q}(\lambda)$.
2°) a) En tenant compte de la Rem. 1.19.b) (Cf. Exemple 3.33.), prouver que

$$K = \mathbb{Q}(i, \sqrt{2} + \sqrt{3}).$$

b) Déterminer le polynôme $Irr_{\mathbb{Q}}(\sqrt{2} + \sqrt{3}, X)$.
c) En suivant la démonstration du *Théorème de l'élément primitif* (Th. 3.31), trouver un élément $\lambda \in K$ tel que $K = \mathbb{Q}(\lambda)$.

8. Soit K un corps de caractéristique $p \neq 0$ et $K(\alpha)$ une extension simple, *transcendante* de K (Déf. 2.2).
1°) Démontrer que le polynôme $X^p - \alpha^p$ est irréductible sur $K(\alpha^p)$; en déduire que $[K(\alpha) : K(\alpha^p)] = p$.
2°) Soit $K(\beta)$ une extension simple, *transcendante* de K, telle que

$$\alpha \notin K(\beta) \text{ et } \beta \notin K(\alpha).$$

a) Prouver que $[K(\alpha, \beta) : K(\alpha^p, \beta^p)] = p^2$.
b) Vérifier que $u \in K(\alpha, \beta) \Longrightarrow u^p \in K(\alpha^p, \beta^p)$;
en conclure que $K(\alpha, \beta)$ n'est pas une extension simple de $K(\alpha^p, \beta^p)$.

9. Soit K un corps, p un nombre premier et a un élément donné dans K, tel que

$$a \neq 0, a \neq 1.$$

On suppose, dans toutes les questions qui suivent, que le polynôme $X^p - a$ est *irréductible* sur K et on note α une racine de ce polynôme dans une extension de K.
1°) Donner l'expression d'un élément quelconque de $K(\alpha)$ en fonction de α.
2°) On suppose $\underline{car K = p}$.
Démontrer que le polynôme $X^p - \alpha$ n'a pas de racine dans $K(\alpha)$.
3°) On suppose $\underline{p = 2}$ et $\underline{car K \neq 2}$.
Démontrer que le polynôme $X^p - \alpha$ a une racine dans $K(\alpha)$ si et seulement si $-4a$ est une puissance $4^{ème}$ dans K (c'est-à-dire qu'il existe $x \in K$ tel que $-4a = x^4$).
4°) On suppose $\underline{p \neq 2}$ et $\underline{car K \neq p}$.

Soit L un corps de décomposition sur K du polynôme $X^p - 1$.
a) Vérifier que $X^p - 1$ n'a que des racines simples dans L.
b) On note Γ l'ensemble des p racines de $X^p - 1$ dans L.
– Vérifier que Γ forme un sous-groupe *cyclique* du groupe multiplicatif $L^* = L \setminus \{0\}$.
– En déduire que, pour tout $\varepsilon \neq 1$ dans Γ, on a $L = K(\varepsilon)$.
– Déterminer le produit $\varepsilon\,\varepsilon^2\,\varepsilon^3 \ldots \varepsilon^{p-1}$.
5°) On suppose toujours $p \neq 2$ et $car K \neq p$.
Soit $\varepsilon \neq 1$ dans le groupe Γ défini dans la question précédente.
On suppose que le polynôme $X^p - a$, irréductible sur K, par hypothèse, est , de plus, irréductible sur $K(\varepsilon)$.
On pose $M = K(\alpha, \varepsilon)$.
a) Vérifier que le polynôme $X^p - a$ est séparable sur K et que, pour $0 \leq i \leq p-1$, les éléments $\alpha\varepsilon^i$ sont les racines de $X^p - a$ dans M.
En conclure que M est une extension de degré fini, normale et séparable sur K.
b) Montrer que, pour tout entier i, $0 \leq i \leq p-1$, il existe un automorphisme σ_i du corps M tel que

$$\sigma_i(\alpha) = \alpha\varepsilon^i \text{ et } \sigma_{i/K(\varepsilon)} = id_{K(\varepsilon)}.$$

(On remarquera que $M = K(\varepsilon)(\alpha) = K(\varepsilon)(\varepsilon^i\alpha)$, $\forall i (0 \leq i \leq p-1)$).
c) Le but de cette question est de prouver que le polynôme $X^p - \alpha$ n'a pas de racine dans $K(\alpha)$.
On suppose qu'il existe $\beta \in K(\alpha)$ tel que $\beta^p = \alpha$, il s'agit alors de montrer que cette hypothèse conduit à une contradiction avec l'irréductibilité sur K du polynôme $X^p - a$.
– Vérifier que $\beta^p = \alpha$ implique $K(\beta) = K(\alpha)$. En déduire que β est algébrique sur K.
– On pose $g(X) := Irr_K(\beta, X)$. Quel est le degré du polynôme g(X) ?
Montrer que $g(X)$ est scindé sur M.
– Les σ_i, $0 \leq i \leq p-1$, étant les automorphismes de M définis dans la question 5°)b), on pose, pour tout i,

$$\sigma_i(\beta) = \beta_i.$$

– Prouver que les β_i, $0 \leq i \leq p-1$, sont exactement les racines de $g(X)$ dans M. On pose

$$b := \beta_0\beta_1 \ldots \beta_{p-1}.$$

Comparer b au terme constant de $g(X)$.
Calculer b^p ; en conclure que $X^p - \alpha$ n'a pas de racine dans $K(\alpha)$.

10. Soit ∂ une *dérivation* d'un corps K (Ex. **8.**, Ch. 1). Pour tout $f(X) = \sum_{0 \leq i \leq n} a_i X^i$, dans $K[X]$, on pose

$$f^{\partial}(X) := \sum_{0 \leq i \leq n} \partial(a_i) X^i.$$

1°) Calculer $(f+g)^{\partial}$ et $(fg)^{\partial}$ pour f et g dans $K[X]$.
2°) Soit $K(\alpha)$ une extension simple de K.
a) On suppose qu'il existe une dérivation ∂_1 de $K(\alpha)$ prolongeant ∂ (c'est-à-dire que $\partial_{1/K} = \partial$).
Pour tout $n \in \mathbb{N}$, calculer $\partial_1(\alpha^n)$; en déduire $\partial_1(f(\alpha))$, pour tout $f(X) \in K[X]$.
b) On considère le morphisme

$$\begin{aligned} \theta : K[X] &\longrightarrow K(\alpha) \\ f(X) &\longmapsto f(\alpha). \end{aligned}$$

On pose $K[\alpha] := Im\,\theta$ et on note θ_1 la *restriction surjective* de θ ; autrement dit :

$$\theta_1 : K[X] \longrightarrow K[\alpha] \text{ et pour tout } f(X) \in K[X],\ \theta_1(f(X)) = f(\alpha).$$

Comme dans l'Ex. **8.**, Ch. 1, on définit l'anneau de matrices

$$M(K(\alpha)) := \left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \quad ; \quad (x,y) \in K(\alpha) \times K(\alpha) \right\}.$$

Soit $\beta \in K(\alpha)$; on considère l'application

$$\begin{aligned} \varphi : K[X] &\longrightarrow M(K(\alpha)) \\ f(X) &\longmapsto \begin{pmatrix} f(\alpha) & f^{\partial}(\alpha) + f'(\alpha)\beta \\ 0 & f(\alpha) \end{pmatrix}. \end{aligned}$$

où $f'(X)$ désigne le polynôme dérivé de $f(X)$.

Vérifier que φ est un morphisme d'anneaux unitaires.

3°) Comme précédemment, soit $K(\alpha)$ une extension simple de K.

a) On suppose α *transcendant* sur K et, comme ci-dessus, on note θ_1 la *restriction surjective* de θ. Justifier les propriétés suivantes :

θ_1 est un isomorphisme et $K(\alpha)$ est le corps des fractions du domaine d'intégrité $K[\alpha]$.

On pose $\varphi_1 = \varphi \circ {\theta_1}^{-1}$ et on note ε l'injection canonique de $K[\alpha]$ dans $K(\alpha)$. Prouver qu'il existe un unique morphisme d'anneaux unitaires ψ de $K[\alpha]$ dans $M(K(\alpha))$ tel que $\psi \circ \varepsilon = \varphi_1$.

En déduire que, pour tout $\beta \in K(\alpha)$, il existe une unique dérivation ∂_1 de $K(\alpha)$ qui prolonge ∂ et telle que $\partial_1(\alpha) = \beta$ (Cf. Ex. 8, Ch. 1).

b) On suppose α *algébrique* sur K et $\beta \in K(\alpha)$; on considère $p(X) := Irr_K(\alpha, X)$ et on note π la surjection canonique de $K[X]$ sur $\dfrac{K[X]}{(p(X))}$.

En identifiant $K(\alpha)$ à $\dfrac{K[X]}{(p(X))}$ (voir la preuve du Th. 2.11), montrer qu'il existe un unique morphisme d'anneaux unitaires

$$\psi \text{ de } K(\alpha) \text{ dans } M(K(\alpha)) \text{ tel que } \psi \circ \pi = \varphi$$

si et seulement si on a

$$(p(X)) \subseteq Ker\,\varphi. \tag{3.16}$$

Montrer que la condition (3.15) équivaut à la condition

$$p^{\partial}(\alpha) + p'(\alpha)\beta = 0. \tag{3.17}$$

En déduire que la condition (3.16) équivaut à l'existence d'une dérivation ∂_β de $K(\alpha)$ prolongeant ∂ et telle que $\partial_\beta(\alpha) = \beta$.

Vérifier que si la dérivation ∂_β existe, alors elle est unique.

– Si α est *séparable* sur K, prouver que ∂_β existe pour une seule valeur de $\beta \in K(\alpha)$.

– Si α est *inséparable* sur K et si $p(X) = \sum_{0 \le i \le d} c_i X^i$, démontrer que ∂_β existe, pour tout $\beta \in K(\alpha)$, si et seulement si $\partial(c_i) = 0$, quel que soit $i\,(0 \le i \le d)$.

Chapitre 4
Corps finis

Signalons que les corps finis sont encore appelés « *champs de Galois* », mais nous n'utiliserons pas ce vocable.

1. Cardinal d'un corps fini

Rappels :
a) Tout corps fini (c'est-à-dire de cardinal fini) est nécessairement de caractéristique non nulle (Rem. 1.7).
b) Pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est de cardinal p et de caractéristique p (Ch. 1).
c) Si V est un espace vectoriel sur un corps K, alors (voir un cours d'Algèbre Linéaire)

$$dim_K V = n < \infty \iff V \simeq K^n. \tag{4.1}$$

Notations :
a) p étant nombre premier, on notera $\mathbb{F}_p$, le corps $\mathbb{Z}/p\mathbb{Z}$.
b) Le cardinal d'un ensemble X sera noté $card(X)$ ou $|X|$.

Théorème 4.1. *Si K est un corps fini de caractéristique p, il existe alors un entier $n \geq 1$ tel que $|K| = p^n$.*

Démonstration. K est un corps de caractéristique $p \neq 0$, donc K est une extension de $\mathbb{F}_p$ (Ch. 1) ; on peut supposer $\mathbb{F}_p \subseteq K$, alors,

$$(\mathbb{F}_p \subseteq K \quad \text{et} \quad |K| < \infty) \Longrightarrow [K : \mathbb{F}_p] < \infty.$$

Posons $n := [K : \mathbb{F}_p]$; ainsi K est un espace vectoriel de dimension finie, n, sur $\mathbb{F}_p$; d'où $K \simeq \mathbb{F}_p{}^n$ (Rappel c), ci-dessus), ce qui implique $|K| = p^n$. □

2. Groupe des éléments non nuls d'un corps fini

A tout corps K on peut associer le groupe multiplicatif abélien K^*.
Si K est un corps fini de cardinal p^n (Th. 4.1), alors K^* est un groupe abélien fini de cardinal $p^n - 1$.

Théorème 4.2. *Le groupe multiplicatif des éléments non nuls d'un corps fini est cyclique.*

Démonstration. 1°) **Rappels** ([12], Ch. III)
Un groupe fini G est *cyclique* s'il est engendré par un élément x et dans ce cas (en supposant que G est un groupe multiplicatif),

$$|G| = m \Longrightarrow G = < x > = \{x^k\,;\, 0 \leq k \leq m-1\}.$$

L'élément x est alors un *générateur* de G.
Le nombre des générateurs d'un groupe cyclique G d'ordre m est $\varphi(m)$, où φ est la fonction d'Euler ([12], Prop. 3.21).
De plus, pour tout diviseur d de m dans $\mathbb{N}^*$, le nombre des éléments de G, d'ordre d, est $\varphi(d) > 0$ et

$$m = \sum_{d|m} \varphi(d), \quad 1 \leq d \leq m. \tag{4.2}$$

2°) Le Th. 4.2 résultera du **lemme** suivant ([12], Ex. 19, Ch. III).

Lemme 4.3. *Soit G un groupe (multiplicatif) fini d'ordre m ; si pour tout diviseur d de m dans $\mathbb{N}$, le nombre d'éléments x de G vérifiant l'égalité $x^d = 1$, est au plus égal à d, alors G est cyclique* (1 *désigne l'élément unité de* G).

Démonstration. On remarque que l'hypothèse du lemme ne suppose pas G abélien.
Quel que soit le diviseur d de m dans $\mathbb{N}^*$, désignons par $\lambda(d)$ le nombre des éléments de G, *d'ordre* d. On a alors

$$\lambda(d) \geq 0 \quad \text{et} \quad m = \sum_{d|m} \lambda(d), \quad 1 \leq d \leq m. \tag{4.3}$$

φ étant la fonction d'Euler, montrons que

$$\big(1 \leq d \leq m,\ d \mid n \text{ et } \lambda(d) \neq 0\big) \Longrightarrow \lambda(d) = \varphi(d).$$

En effet, $\lambda(d) \neq 0$ implique qu'il existe au moins un élément $y \in G$ d'ordre d ; le sous-groupe cyclique de G engendré par y, noté $< y >$, est alors d'ordre d et tout $x \in < y >$ vérifie : $x^d = 1$.
Compte tenu de l'hypothèse du lemme, on en déduit que les seuls éléments x de G, vérifiant $x^d = 1$, sont les éléments du groupe $< y >$. Par suite, les seuls éléments de G, *d'ordre* d, sont les *générateurs* du groupe $< y >$, d'où

$$\lambda(d) = \varphi(d).$$

Pour prouver que le groupe G est cyclique il suffit de montrer que $\lambda(m)$ est non nul. En tenant compte des résultats (4.2) et (4.3), on obtient

$$\lambda(m) = m - \sum_{d|m,d\neq m} \lambda(d) \geq m - \sum_{d|m,d\neq m} \varphi(d) = \varphi(m) > 0,$$

d'où $\lambda(m) \neq 0$. □

3°) **Preuve** du Th. 4.2.
Pour un corps K fini, de caractéristique p et de cardinal p^n (Th. 4.1), le groupe K^* est d'ordre $p^n - 1$.
Pour tout diviseur d de $p^n - 1$ dans $\mathbb{N}^*$, le polynôme $X^d - 1$ a au plus d racines dans K ([13], Cor. 4.48) et plus précisément, dans K^*, puisque 0 n'est pas l'une de ses racines.
On en déduit que le groupe fini K^* satisfait aux hypothèses du lemme 4.3, donc K^* est cyclique. □

En particulier, le groupe $\mathbb{F}_p{}^*$ est cyclique d'ordre $p-1$.

Corollaire 4.4. *Quel que soit le corps K (fini ou non), tout sous-groupe* fini *du groupe K^* est cyclique.*

Démonstration. En effet, si G est un sous-groupe *fini* de K^*, le raisonnement fait pour la preuve du Th. 4.2 montre que le groupe G vérifie les hypothèses du lemm 4.3, donc G est cyclique. □

3. Caractérisation des corps finis

Théorème 4.5. *Etant donné $n \in \mathbb{N}^*$, un corps K, fini et de caractéristique p, est de cardinal p^n si et seulement si K est corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^{p^n} - X$.*

Démonstration. Soit K un corps fini tel que $carK = p$ et $|K| = p^n$; alors K est une extension de $\mathbb{F}_p$ et $[K : \mathbb{F}_p] = n$ (voir la preuve du Th. 4.1).
De plus (Th. 4.2), le groupe K^* est cyclique d'ordre $p^n - 1$, donc tout $\alpha \in K^*$ vérifie : $\alpha^{p^n-1} = 1$.
Considérons le polynôme $f(X) := X^{p^n} - X = X(X^{p^n-1} - 1)$ dans $\mathbb{F}_p[X]$; alors tout élément α de K est racine du polynôme $f(X)$.
D'autre part, $car\mathbb{F}_p = p$ implique $f'(X) = -1$, d'où $f \wedge f' = 1$.
On en déduit ([13], Cor. 8.49) que le polynôme $f(X)$ a p^n racines simples dans un corps de décomposition sur $\mathbb{F}_p$; ce sont donc les p^n éléments de K. Par suite, K est corps de décomposition du polynôme $X^{p^n} - X$ sur $\mathbb{F}_p$.

Réciproquement, soit K un corps de décomposition sur $\mathbb{F}_p$, du polynôme $f(X) = X^{p^n} - X$.
Comme on l'a vérifié précédemment, $f(X)$ n'a que des racines simples dans K.
Soit $R = \{\alpha_1, \alpha_2, \ldots, \alpha_{p^n}\}$ l'ensemble des racines distinctes de $f(X)$ dans K. Montrons que R est un sous-corps de K.
On remarque que $\{0, 1\} \subseteq R$; posons $[1, p^n] := \{i \in \mathbb{N} \,;\, 1 \leq i \leq p^n\}$.
Pour tout $i \in [1, p^n]$, on a $\alpha_i = \alpha_i{}^{p^n}$, donc quels que soient i et j dans $[1, p^n]$:

$$\alpha_i - \alpha_j = \alpha_i{}^{p^n} - \alpha_j{}^{p^n} = (\alpha_i - \alpha_j)^{p^n}, \text{ puisque } carK = p.$$
$$\alpha_i \alpha_j{}^{-1} = \alpha_i{}^{p^n}(\alpha_j{}^{p^n})^{-1} = (\alpha_i \alpha_j{}^{-1})^{p^n}, \text{ en supposant } \alpha_j \neq 0.$$

On en conclut que R est un sous-corps de K. On a $\mathbb{F}_p \subseteq R$ et $f(X)$ scindé sur R ; or par hypothèse, K est corps de décomposition de $f(X)$ sur $\mathbb{F}_p$, par suite (Th. 3.3), $R = K$, d'où $|K| = p^n$. □

Corollaire 4.6. *Quels que soient le nombre premier p et l'entier $n \geq 1$, il existe un corps fini de cardinal p^n, défini à un $\mathbb{F}_p$-isomorphisme près.*

Ce résultat se déduit des théorèmes 3.3 et 4.5 et du Cor. 3.9.

Notation : Un corps fini de caractéristique p et de cardinal $p^n, n > 0$, étant unique à un $\mathbb{F}_p$-isomorphisme près (Cor. 4.6), nous utiliserons couramment, la notation $\mathbb{F}_{p^n}$ pour désigner un tel corps et nous supposerons $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$.

4. Sous-corps d'un corps fini

Rappel ([13], App. A, Prop. 0.37) :
Quels que soient les entiers $a > 1, n > 0, s > 0$, on a, dans $\mathbb{N}^*$,

$$(a^s - 1) \mid (a^n - 1) \iff s \mid n. \tag{4.4}$$

Lemme 4.7. *Etant donné un corps K et un entier $n > 1$, alors pour $s \in \mathbb{N}^*$,*

$$X^s - 1 \mid X^n - 1, \text{ dans } K[X] \iff s \mid n, \text{ dans } \mathbb{N}^*. \tag{4.5}$$

Démonstration. 1^{er} *cas* : $car K = 0$ ou $car K = p$ et $p \nmid n$.
Supposons $s \mid n$; il existe alors un entier $d \geq 1$ tel que $n = sd$, donc dans le cas où $car K = p$ et $p \nmid n$, on a $p \nmid s$. On en déduit que

$$X^n - 1 = (X^s)^d - 1 = (X^s - 1)(X^{s(d-1)} + X^{s(d-2)} + \cdots + X + 1),$$

d'où $X^s - 1 \mid X^n - 1$, dans $K[X]$.

Réciproquement, supposons $X^s - 1 \mid X^n - 1$, dans $K[X]$; on a alors, $0 < s \leq n$, dans $\mathbb{N}$. On en déduit qu'il existe des entiers q et r tels que

$$n = sq + r, \quad q > 0, \quad 0 \leq r < s.$$

Par suite,

$$X^n - 1 = X^{sq}X^r - 1 = (X^{sq} - 1)X^r + X^r - 1;$$
$$\text{alors,} \quad X^s - 1 \mid X^{sq} - 1 \Longrightarrow (X^s - 1 \mid X^n - 1 \iff X^s - 1 \mid X^r - 1).$$

Compte tenu de la condition $0 \leq r < s$, on en déduit que

$$X^s - 1 \mid X^n - 1 \Longrightarrow r = 0 \Longrightarrow s \mid n.$$

$2^{ème}$ *cas* : $car K = p \neq 0$ et $p \mid n$.
Dans $\mathbb{N}$, on peut écrire $n = kp^\alpha$, avec $\alpha > 0, k > 0, p \nmid k$, alors la condition $car K = p$ implique

$$X^n - 1 = (X^k)^{p^\alpha} - 1 = (X^k - 1)^{p^\alpha}. \tag{4.6}$$

Si $s \mid n$ dans $\mathbb{N}$, on a $s = k'p^\beta$, où $k' \mid k$, donc $p \nmid k'$, et $0 \leq \beta \leq \alpha$, d'où,

$$X^s - 1 = (X^{k'p^\beta} - 1) = (X^{k'} - 1)^{p^\beta};$$
$$\text{par suite,} \quad (k' \mid k,\ p \nmid k,\ 0 \leq \beta \leq \alpha) \Longrightarrow (X^{k'} - 1)^{p^\beta} \mid (X^k - 1)^{p^\alpha}$$
$$\text{donc,} \quad s \mid n \Longrightarrow X^s - 1 \mid X^n - 1.$$

Réciproquement, supposons $X^n - 1 = X^{kp^\alpha} - 1 = (X^k - 1)^{p^\alpha}$, où, dans $\mathbb{N}$, $p \nmid k$ et $\alpha \neq 0$; si $X^s - 1 \mid X^n - 1$ dans $K[X]$, alors nécessairement,

$$X^s - 1 = (X^{k'} - 1)^{p^\beta}, \text{ avec } k' \mid k \text{ et } 0 \leq \beta \leq \alpha;$$
$$\text{d'où,} \quad (X^s - 1 = X^{k'p^\beta} - 1) \Longrightarrow s = k'p^\beta \Longrightarrow s \mid n. \qquad \square$$

Théorème 4.8. *Quels que soient le nombre premier p et l'entier $n \geq 1$, il existe une bijection entre l'ensemble des sous-corps de $\mathbb{F}_{p^n}$ et l'ensemble des diviseurs de n dans $\mathbb{N}^*$. Plus précisément,*

$$\mathbb{F}_{p^s} \text{ sous-corps de } \mathbb{F}_{p^n} \iff s \mid n, \text{ dans } \mathbb{N}^*.$$

Démonstration. Rappelons que pour $n = 1$, le corps $\mathbb{F}_p$ n'a pas de sous-corps propre (Prop. 1.4) ; dans ce cas, on peut dire que le théorème est trivialement vérifié. On suppose dans la suite, $n > 1$.

Notons S un sous-corps de $\mathbb{F}_{p^n}$; S est donc un corps fini de caractéristique p, donc il existe un entier $s > 0$, tel que $|S| = p^s$ (Th. 4.1). On peut écrire :

$$S = \mathbb{F}_{p^s} \quad \text{et} \quad \mathbb{F}_p \subseteq \mathbb{F}_{p^s} \subseteq \mathbb{F}_{p^n}.$$

D'après les Th. 4.5 et 3.3, $\mathbb{F}_{p^n}$ (resp. $\mathbb{F}_{p^s}$) est l'unique corps de décomposition sur $\mathbb{F}_p$, du polynôme $X^{p^n} - X$ (resp. $X^{p^s} - X$), contenant $\mathbb{F}_p$.
La preuve du Th. 4.5 montre que $\mathbb{F}_{p^s}$ est un sous-corps de $\mathbb{F}_{p^n}$ si et seulement si toute racine de $X^{p^s} - X$ dans $\mathbb{F}_{p^s}$ est aussi racine de $X^{p^n} - X$ dans $\mathbb{F}_{p^n}$; alors, compte tenu des résultats (4.4) et (4.5), on a

$$\begin{aligned} \mathbb{F}_{p^s} \text{ sous-corps de } \mathbb{F}_{p^n} &\iff (X^{p^s-1} - 1) \mid (X^{p^n-1} - 1), \text{ dans } \mathbb{F}_p[X], \\ &\iff (p^s - 1) \mid (p^n - 1), \text{ dans } \mathbb{N}^*, \\ &\iff s \mid n, \text{ dans } \mathbb{N}^*. \end{aligned}$$

□

Remarque 4.9. *a*) Si $\mathbb{F}_p \subseteq \mathbb{F}_{p^s} \subseteq \mathbb{F}_{p^n}$, alors le groupe multiplicatif $\mathbb{F}_{p^s}^*$ est l'unique sous-groupe d'ordre $p^s - 1$ du groupe cyclique $\mathbb{F}_{p^n}^*$.
Le Th. 4.8 peut être démontré à partir de cet argument.

b) La preuve du Th. 4.7 montre que quel que soit le diviseur s de n dans $\mathbb{N}^*$, $\mathbb{F}_{p^n}$ est corps de décomposition du polynôme $X^{p^n} - X$, sur le corps $\mathbb{F}_{p^s}$.

5. Propriétés des corps finis

Lemme 4.10. Lemme de Frobenius
Soit K un corps de caractéristique $p \neq 0$, alors l'application

$$\begin{aligned} \phi : K &\longrightarrow K \\ a &\longmapsto a^p \end{aligned}$$

est un endomorphisme de K, appelé **endomorphisme de Frobenius.**
Si le corps K est fini, *alors ϕ est un automorphisme de K.*
Pour $K = \mathbb{F}_p$, $\phi = id_K$.

Démonstration. $car K = p$, donc quel que soit $(a,b) \in K \times K$, on sait que

$$\phi(a+b) = (a+b)^p = a^p + b^p \quad \text{et} \quad \phi(ab) = (ab)^p = a^p b^p, \text{ de plus, } \phi(1) = 1.$$

Ainsi, ϕ est un endomorphisme non nul, donc *injectif* de K.
Si K est *fini*, alors, ϕ injectif $\Longrightarrow$ ϕ bijectif, donc ϕ est un automorphisme de K, d'où

$$K = \{a^p \, ; \, a \in K\}. \tag{4.7}$$

si $K = \mathbb{F}_p$, on a, quel que soit $a \in \mathbb{F}_p$, $a^p = a$, d'où $\phi = id_{\mathbb{F}_p}$. □

Théorème 4.11. *Tout corps fini est parfait.*

Démonstration. K étant un corps fini de caractéristique p, l'égalité (4.7) est vérifiée, donc, d'après le Th. 3.27, K est un corps parfait (Déf. 3.25). □

Théorème 4.12. *Si K est un corps fini, alors toute extension de degré fini sur K est une extension simple, normale et séparable de K.*

Démonstration. On suppose $car K = p$ et $|K| = p^n$, $n > 0$, donc $[K : \mathbb{F}_p] = n$.
Soit L une extension de K telle que $K \subseteq L$ et $[L : K] = r > 1$; L est une extension algébrique de K (Th. 2.26) et K étant un corps parfait (Th. 4.11), L est *séparable* sur K.
D'autre part,

$$([L : K] = r \quad \text{et} \quad [K : \mathbb{F}_p] = n) \Longrightarrow [L : \mathbb{F}_p] = rn.$$

On en déduit que L est corps de décomposition du polynôme $X^{p^{rn}} - X$ sur K (Rem. 4.9 b)), donc L est une extension *normale* de K (Th. 3.15).
On a supposé $r > 1$, donc il existe $g(X) \in K[X]$ tel que

$$X^{p^{rn}-1} - 1 = (X^{p^n-1} - 1)g(X), \quad deg\, g > 0. \tag{4.8}$$

D'après la preuve du Th. 4.5, les éléments du groupe cyclique L^* (resp. K^*) sont les racines du polynôme $X^{p^{rn}-1} - 1$ (resp. $X^{p^n-1} - 1$).
Si λ est un générateur du groupe L^*, alors $\lambda \notin K^*$, donc λ est une racine du polynôme $g(X)$ défini par la relation (4.8) et $K \subset K(\lambda) \subseteq L$.

$$\text{Mais,} \quad L = \{0\} \cup L^* = \{0\} \cup \{\lambda^k \,;\, 1 \leq k \leq p^{rn} - 1\} \Longrightarrow L \subseteq K(\lambda),$$

d'où $L = K(\lambda)$. □

Corollaire 4.13. *p étant un nombre premier, tout corps fini $\mathbb{F}_{p^n}$ est une extension simple, normale et séparable de $\mathbb{F}_p$.*

Démonstration. Il suffit d'appliquer le Th. 4.12 avec $K = \mathbb{F}_p$ et $L = \mathbb{F}_{p^n}$. □

Remarque 4.14. D'après le Th. 4.12, le *Théorème de l'élément primitif* (Th. 3.31) est vérifié par toute extension de degré fini d'un corps fini.
D'après la preuve du Th. 4.12, tout *générateur* ω du groupe cyclique $\mathbb{F}^*_{p^n}$ est un *élément primitif* (Déf. 3.32) pour l'extension $\mathbb{F}_{p^n} : \mathbb{F}_p$; c'est-à-dire que

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\omega).$$

Plus généralement, quels que soient le *diviseur* s de n dans $\mathbb{N}^*$ et le *générateur* ω du groupe cyclique $\mathbb{F}^*_{p^n}$, on a

$$\mathbb{F}_{p^n} = \mathbb{F}_{p^s}(\omega).$$

Précisons qu'en posant $q := \dfrac{p^n - 1}{p^s - 1}$, on a ([12], Ch. III)

$$\mathbb{F}^*_{p^n} = \{\omega^k \,;\, 1 \leq k \leq p^n - 1\} \quad \text{et} \quad \mathbb{F}^*_{p^s} = \{\omega^{ql} \,;\, 1 \leq l \leq p^s - 1\}.$$

Mais, il est important de noter, qu'un élément α, *primitif* pour une extension $\mathbb{F}_{p^n} : \mathbb{F}_p$, donc tel que

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha),$$

n'est pas nécessairement un générateur du groupe $\mathbb{F}^*_{p^n}$. (Cf. Ex. **3.** et **4.** de ce chapitre).

Cette remarque sera utile au Ch. 6, pour l'étude des extensions et polynômes cyclotomiques sur un corps fini.

Cependant, quels que soient le nombre premier p, l'entier $n \geq 1$ et l'élément α, primitif pour l'extension $\mathbb{F}_{p^n} : \mathbb{F}_p$, on a

$$[\mathbb{F}_{p^n} : \mathbb{F}_p] = n \Longrightarrow deg Irr_{\mathbb{F}_p}(\alpha, X) = n.$$

On en conclut que *pour tout nombre premier p et tout entier* $n \geq 1$, *il existe au moins un polynôme irréductible de degré n, dans* $\mathbb{F}_p[X]$.

6. Exercices

1. Soit K un corps fini tel que $|K| = q$ (q est une puissance de la caractéristique de K). Comme dans l'Ex. **7.**, Ch.1, pour tout entier $n > 0$, on considère l'endomorphisme de groupes

$$u_n : K^* \longrightarrow K^*$$
$$x \longmapsto x^n$$

Démontrer que u_n est un automorphisme du groupe K^* si et seulement si

$$n \wedge (q-1) = 1.$$

2. Soit K un corps fini de caractéristique p.

1°) On suppose qu'il existe une *involution* σ de K (Cf. Ex. **11.**, Ch. 2) telle que $\sigma \neq id_K$. On pose

$$L_\sigma := \{x \in K\,;\ \sigma(x) = x\}.$$

Compte tenu des résultats de l'Ex. **11.**, Ch. 2, montrer qu'il existe $n \in \mathbb{N}^*$, tel que

$$|L_\sigma| = p^n \quad \text{et} \quad |K| = p^{2n}.$$

2°) Réciproquement, soit $K = \mathbb{F}_{p^{2n}}$ un corps fini de cardinal p^{2n}, où p est premier et $n \in \mathbb{N}^*$.

Démontrer que l'application

$$\tau : K \longrightarrow K$$
$$x \longmapsto x^{p^n}$$

est l'unique involution de K, autre que id_K, et que $L_\tau = \mathbb{F}_{p^n}$.

3. Soit $\mathbb{F}_2$ le corps à deux éléments.

1°) Prouver que les polynômes

$$p(X) = X^4 + X + 1 \quad \text{et} \quad q(X) = X^4 + X^3 + X^2 + X + 1$$

sont irréductibles sur $\mathbb{F}_2$.

2°) On pose $K := \dfrac{\mathbb{F}_2[X]}{(p(X))}$ et $L := \dfrac{\mathbb{F}_2[X]}{(q(X))}$.

Vérifier que K et L sont des corps finis dont on précisera le cardinal ; sont-ils isomorphes ?

3°) Soit, respectivement, π et σ les surjections canoniques de $\mathbb{F}_2[X]$ sur K et L. On pose

$$\alpha = \pi(X) \quad \text{et} \quad \beta = \sigma(X).$$

Montrer que α engendre le groupe cyclique K^*, mais que β n'engendre pas le groupe cyclique L^*.
Trouver, en fonction de β, un générateur γ du groupe L^* et en déduire un isomorphisme φ de K sur L tel que $\varphi_{/\mathbb{F}_2} = id_{\mathbb{F}_2}$ et $\varphi(\alpha) = \gamma$.

4. Soit $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.
1°) Montrer que les polynômes $X^3 - X + 1$, $X^3 - X - 1$ et $X^2 + 1$ sont irréductibles sur $\mathbb{F}_3$.
2°) On considère les quotients de l'anneau $\mathbb{F}_3[X]$ par les idéaux respectivement engendrés par ces polynômes ; on pose

$$K := \frac{\mathbb{F}_3[X]}{(X^3 - X + 1)}, \quad L := \frac{\mathbb{F}_3[X]}{(X^3 - X - 1)}, \quad H := \frac{\mathbb{F}_3[X]}{(X^2 + 1)}.$$

On note, respectivement, π, σ, τ les surjections canoniques de $\mathbb{F}_3[X]$ sur K, L, H. Justifier les propriétés suivantes :

a) K, L, H sont des corps finis ; préciser leurs cardinaux.

b) Les corps K et L sont isomorphes.

c) K, L, H sont des extensions simples de $\mathbb{F}_3$ telles que si $\alpha := \pi(X)$, $\beta := \sigma(X)$ *et* $\gamma := \tau(X)$, alors $K = \mathbb{F}_3(\alpha)$, $L = \mathbb{F}_3(\beta)$ *et* $H = \mathbb{F}_3(\gamma)$.

3°) On considère les groupes cycliques K^*, L^*, H^*.

a) Préciser l'ordre de chacun de ces groupes.

b) Démontrer que α (resp. β) engendre le groupe K^* (resp. L^*).

c) Prouver que γ n'engendre pas le groupe H^* et trouver un générateur de H^*, en fonction de γ.

5. *Carrés dans un corps fini.*
Soit K un corps fini de caractéristique p et de cardinal q (q est une puissance de p). On pose

$$K := \mathbb{F}_q, \quad \mathbb{F}_q^2 := \{x^2 \,;\, x \in \mathbb{F}_q\}, \quad \mathbb{F}_q^{*2} := \mathbb{F}_q^2 \setminus \{0\}.$$

1°) Montrer que si $p = 2$, alors $\mathbb{F}_q = \mathbb{F}_q^2$ (Lemme 4.10).
2°) On suppose $p \neq 2$. Vérifier que l'application

$$\begin{aligned} \psi : \mathbb{F}_q^* &\longrightarrow \mathbb{F}_q^* \\ x &\longmapsto x^2 \end{aligned}$$

est un endomorphisme du groupe $\mathbb{F}_q^*$.

En considérant $Im\,\psi$ et $Ker\,\psi$, prouver que $|\mathbb{F}_q^{*2}| = \dfrac{q-1}{2}$; en déduire $|\mathbb{F}_q^2|$.

3°) On suppose toujours $p \neq 2$. Démontrer les propriétés suivantes :

a) $x \in \mathbb{F}_q^* \Longrightarrow x^{\frac{q-1}{2}} = \pm 1$.

b) $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.

c) $-1 \in \mathbb{F}_q^{*2} \iff q - 1 \equiv 0 \pmod 4$.

d) Si -1 et x ne sont pas des carrés dans $\mathbb{F}_q^*$, alors $-x$ est un carré dans $\mathbb{F}_q$.

4°) Soit p un nombre premier impair ; dans le corps $\mathbb{F}_p$, on pose

$$A := \{-x^2 \,;\, x \in \mathbb{F}_p\} \quad \text{et} \quad B := \{1 + y^2 \,;\, y \in \mathbb{F}_p\}.$$

Montrer que $|A| = |B| = \dfrac{p+1}{2}$.

En déduire qu'il existe x et y dans $\mathbb{F}_p$ tels que $1+x^2+y^2=0$.

En déduire qu'il existe des entiers a, b tels que $p \mid 1+a^2+b^2$.

6. 1°) Etant donné un entier $n>1$, soit p un nombre premier divisant $1+(n!)^2$ dans $\mathbb{N}^*$.

a) Vérifier que l'on a p impair et $p>n$.

b) En application du 3°)c) de l'exercice 5) précédent, montrer que

$$1+(n!)^2 \equiv 0 \pmod{p} \iff p-1 \equiv 0 \pmod{4}$$

En déduire qu'il existe une infinité de nombres premiers de la forme $1+4m$, $m \in \mathbb{N}^*$.

Donner quelques exemples de tels nombres premiers.

2°) Soit p un nombre premier de la forme $p=4m+1$.

Dans $\mathbb{F}_p[X]$, on considère le polynôme

$$f(X) := X^{4m}-1.$$

Justifier l'affirmation suivante : $f(X)$ est scindé sur $\mathbb{F}_p$ et les racines de $f(X)$, dans $\mathbb{F}_p$, sont les éléments de $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$.

3°) a) Prouver qu'il existe au moins un entier $a \in \mathbb{Z}$ tel que p divise $a^{2m}+1$. Pour un tel entier a, on pose $b=a^m$; montrer que p divise b^2+1 dans $\mathbb{Z}$.

b) On considère p dans l'anneau des entiers de Gauss $\mathbb{Z}[i]$ ([13]). Vérifier que p n'est pas premier, donc n'est pas irréductible dans $\mathbb{Z}[i]$. En déduire qu'il existe, $c+id \in \mathbb{Z}[i]$, différent d'une unité et non associé à p, qui divise p dans $\mathbb{Z}[i]$ ([13]).

– Démontrer que $p=c^2+d^2$.

– En conclure que tout nombre premier $p=4m+1$ dans $\mathbb{N}$, est la somme des carrés de deux entiers c et d, uniques au signe près, et tels que $c \wedge d = 1$ dans $\mathbb{Z}$.

c) Déterminer les nombres premiers $p=4m+1$ tels que $1<p<30$ et les écrire sous forme d'une somme de deux carrés, dans $\mathbb{N}$.

7. 1°) Prouver que le polynôme $f(X)=X^4+1$ est irréductible dans $\mathbb{Z}[X]$ (Appliquer le critère d'Eisenstein à $f(X+1)$).

En déduire que X^4+1 est irréductible dans $\mathbb{Q}[X]$.

2°) Soit p un *nombre premier*. On considère $f(X)=X^4+1$ dans $\mathbb{F}_p[X]$, où $\mathbb{F}_p$ est le corps à p éléments.

a) Montrer que $f(X)$ est réductible dans $\mathbb{F}_2[X]$.

b) On suppose, dans cette question, *p premier impair.*

Montrer qu'un élément α, appartenant à une extension K de $\mathbb{F}_p$, est racine du polynôme $f(X)$ si et seulement si α est un élément d'ordre 8, dans le groupe multiplicatif K^*.

Vérifier que 8 divise p^2-1.

En déduire que pour tout nombre premier impair, le polynôme X^4+1 a une racine dans le corps $\mathbb{F}_{p^2}$ (de cardinal p^2).

3°) En utilisant le résultat de l'Ex. **2.**, Ch. 3, prouver que, quel que soit le nombre premier p, le polynôme X^4+1 est réductible sur $\mathbb{F}_p$.

8. Etant donné un entier $a>1$, sans facteur carré dans $\mathbb{Z}$, on note $\sqrt{a}$ la racine carrée positive de a, dans $\mathbb{R}$, et on considère le polynôme

$$f_a(X) := X^4+2(1-a)X^2+(1+a)^2.$$

1°) a) Soit i le nombre complexe tel que $i^2 = -1$; montrer que le corps $K := \mathbb{Q}(i, \sqrt{a})$ est corps de décomposition, sur $\mathbb{Q}$, du polynôme $f_a(X)$.

b) On pose $z := i + \sqrt{a}$; démontrer que $K = \mathbb{Q}(z)$ et que de plus,
$f_a(X) = Irr_{\mathbb{Q}}(z, X)$.
En déduire que $f_a(X)$ est irréductible dans $\mathbb{Z}[X]$.

2°) Soit p un *nombre premier* ; on note π la surjection canonique de $\mathbb{Z}$ sur $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
Soit $\overline{\pi} : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$ le prolongement canonique de π. On pose

$$\forall n \in \mathbb{Z},\ \pi(n) = \overline{n}\ ;\quad \forall g(X) \in \mathbb{Z}[X],\ \overline{g}(X) = \overline{\pi}(g(X)).$$

a) Pour $p = 2$, vérifier que le polynôme $\overline{f_a}(X)$ est réductible dans $\mathbb{F}_2[X]$.

b) Démontrer que, quel que soit $p \neq 2$, le polynôme $\overline{f_a}(X)$ est réductible sur $\mathbb{F}_p$, en considérant les cas suivants :
1) p divise a.
2) p ne divise pas a et
ou bien, $\overline{a}$ est un carré dans $\mathbb{F}_p^*$;
ou bien, $\overline{a}$ n'est pas un carré dans $\mathbb{F}_p^*$ et
$-\overline{1}$ est un carré dans $\mathbb{F}_p^*$ ou $-\overline{1}$ n'est pas un carré dans $\mathbb{F}_p^*$.
(Voir l'Ex. **5.** de ce chapitre)

9. Etant donné un domaine d'intégrité A ([13], Déf. 1.21) on dira qu'un polynôme est irréductible *sur* A, s'il est irréductible *dans* $A[X]$.
1°) Soit A un anneau factoriel ([13], Déf. 5.87) et $K := FrA$, le corps des fractions de A ([13], Déf. 5.2).
On considère un idéal *premier* I de A tel que $B := A/I$ est : soit un *anneau factoriel*, soit un *corps*.
Pour tout $a \in A$, on note $\overline{a}$ la classe de a modulo I. Soit

$$f(X) := \sum_{0 \leq i \leq n} a_i X^i \in A[X] \text{ et } \overline{f}(X) := \sum_{0 \leq i \leq n} \overline{a_i} X^i \in B[X].$$

On suppose $n > 0$ et $\overline{a_n} \neq 0$; démontrer que

$$\overline{f}(X) \text{ irréductible sur } B \Longrightarrow f(X) \text{ irréductible sur } K. \tag{4.9}$$

En déduire que si $\overline{f}(X)$ est irréductible sur B et $f(X)$ primitif ([13], Déf. 5.102) dans $A[X]$, alors $f(X)$ est *irréductible sur* A.
Applications :
a) Vérifier que $X^3 + X + 1$ est irréductible sur $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$; en déduire que le polynôme $X^3 + 86X^2 + 525X + 1341$ est irréductible sur $\mathbb{Z}$.
b) Prouver que $X^2 + Y^2 + 1$ est irréductible dans $\mathbb{R}[X, Y]$.
2°) Soit p un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; on considère le polynôme

$$f(X) := X^p - X - 1, \quad \text{dans } \mathbb{F}_p[X].$$

a) Vérifier que $f(X)$ n'a pas de racine dans $\mathbb{F}_p$.
b) Soit α une racine de $f(X)$ dans un corps de décomposition, noté E, de $f(X)$ sur $\mathbb{F}_p$. Montrer que $f(X)$ n'a que des racines simples dans E et que ces racines sont les $\alpha + a$, où a décrit $\mathbb{F}_p$.
c) Prouver que $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$; en déduire que $X^p - X - 1$ est irréductible sur $\mathbb{Z}$.

3°) En utilisant le résultat de l'Ex. **2.**, Ch. 3, montrer que X^4+X+1 est irréductible sur le corps $\mathbb{F}_2$; en déduire que les polynômes X^4+X+1 et $3X^4-6X^2+19X+9$ sont irréductibles sur $\mathbb{Z}$.
4°) Compte tenu des résultats des questions 1°) et 3°) de l'Ex. **7.** ci-dessus, vérifier que la propriété exprimée par la relation (4.9) n'admet pas de réciproque.

10. Soit p un nombre premier et $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
1°) Soit $q(X)$ un polynôme *irréductible et unitaire* dans $\mathbb{F}_p[X]$. On pose $d := deg\, q > 1$ et on note $(q(X))$ l'idéal de $\mathbb{F}_p[X]$ engendré par $q(X)$.
a) Vérifier que $\dfrac{\mathbb{F}_p[X]}{(q(X))}$ est un corps fini, dont on précisera le cardinal. Montrer que $q(X)$ divise $X^{p^d}-X$ dans $\mathbb{F}_p[X]$.
b) Soit $n>1$ dans $\mathbb{N}$; démontrer que

$$q(X) \mid X^{p^n}-X \quad \text{dans } \mathbb{F}_p[X] \iff d \mid n \quad \text{dans } \mathbb{N}^*.$$

2°) Soit $f(X) \in \mathbb{F}_p[X]$ tel que $n := deg\, f > 1$.
Soit $n = r_1 r_2 \ldots r_k$ la factorisation de n en un produit de nombres premiers r_i, $1 \le i \le k$, les r_i n'étant pas nécessairement distincts. Pour tout $i (1 \le i \le k)$, on pose $d_i = \dfrac{n}{r_i}$.
Démontrer que le polynôme $f(X)$ est irréductible dans $\mathbb{F}_p[X]$ si et seulement si les conditions suivantes sont satisfaites dans $\mathbb{F}_p[X]$:

$$f(X) \mid X^{p^n}-X \quad \text{et} \quad f(X) \wedge (X^{p^{d_i}}-X) = 1,\ \forall i (1 \le i \le k).$$

3°) Soit $\mathcal{D}_p^n$ l'ensemble des polynômes de $\mathbb{F}_p[X]$, *irréductibles, unitaires et de degré n.*
a) Prouver que l'ensemble $\mathcal{D}_p^n$ est fini. On pose $I_p^n := card(\mathcal{D}_p^n)$.
b) Démontrer la relation :

$$X^{p^n}-X = \prod_{d \mid n} \prod_{q \in \mathcal{D}_p^d} q(X). \tag{4.10}$$

En déduire que

$$p^n = \sum_{d \mid n} d I_p^d \tag{4.11}$$

et que pour tout entier n > 1, on a $p^n \ge n I_p^n$.
c) A partir des résultats précédents, démontrer que pour tout entier $n > 1$, on a

$$n I_p^n \ge p^n - \frac{p^n-1}{p-1}. \tag{4.12}$$

11. Soit $\mathbb{F}_q$ un corps fini de cardinal q, où q est une puissance d'un nombre premier p.
Question préliminaire : Pour tout polynôme $f(X) \in \mathbb{F}_p[X]$, on pose

$$S(f) := \sum_{x \in \mathbb{F}_q} f(x).$$

Pour tout $m \in \mathbb{N}$, on considère $S(X^m) := \sum_{x \in \mathbb{F}_q} x^m$; prouver que

$$S(X^m) = -1, \text{ si } m = 0 \quad \text{ou} \quad \text{si } m \ge 1 \text{ et } (q-1) \mid m;$$
$$S(X^m) = 0, \quad \text{sinon.}$$

Soit $n \in \mathbb{N}^*$; dans l'anneau $\mathbb{F}_q[X_1,\ldots,X_n]$, on désigne par $\mathcal{F}$ une famille *finie* de polynômes non constants :

$$\mathcal{F} = \{f_\lambda\ ;\lambda \in \Lambda\},\quad 1 \leq |\Lambda| < \infty.$$

On rappelle que $x = (x_1,\ldots,x_n) \in \mathbb{F}_q^n$ est un *zéro* d'un polynôme $f \in \mathbb{F}_q[X_1,\ldots,X_n]$, si $f(x) = 0$.
Soit V l'ensemble des zéros communs aux polynômes f_λ, $\lambda \in \Lambda$. Pour tout $\lambda \in \Lambda$, on note $deg\, f_\lambda$ le *degré total* de f_λ.
Le but des questions 1°) et 2°) est de prouver la relation (4.13) (Th. de Chevalley-Warning, [43])

$$\sum_{\lambda\in\Lambda} deg\, f_\lambda < n \Longrightarrow |V| \equiv 0 \pmod{p}. \tag{4.13}$$

1°) Dans $\mathbb{F}_q[X_1\ldots,X_n]$, on considère le polynôme P défini par

$$P := \prod_{\lambda\in\Lambda}(1 - f_\lambda^{q-1}).$$

Pour tout $x \in \mathbb{F}_q^n$, on a donc $P(x) = \prod_{\lambda\in\Lambda}\big(1 - f_\lambda^{q-1}(x)\big)$.
Démontrer les propriétés suivantes :

$$a)\ x \in V \Longrightarrow P(x) = 1\,;\qquad b)\ x \notin V \Longrightarrow P(x) = 0.$$

2°) Pour tout $f \in \mathbb{F}_q[X_1\ldots,X_n]$, on pose $S(f) := \sum_{x\in\mathbb{F}_q^n} f(x)$.

a) Démontrer que

$$|V| \equiv S(P) \pmod{p}. \tag{4.14}$$

b) Prouver que

$$\sum_{\lambda\in\Lambda} deg\, f_\lambda < n \Longrightarrow deg\, P < n(q-1).$$

En déduire que P est combinaison linéaire sur $\mathbb{F}_p$, de monômes de la forme :

$$X_1^{m_1}\ldots X_n^{m_n},\quad \text{où}\quad \sum_{1\leq i\leq n} m_i < n(q-1).$$

Prouver que, pour un tel monôme, il existe $j\,(1 \leq j \leq n)$ tel que $S(X_j^{m_j}) = 0$.
En déduire que $S(X_1^{m_1}\ldots X_n^{m_n}) = 0$.
Justifier alors le résultat (4.13), moyennant la relation (4.14).
3°) En application de la relation (4.13), montrer que si, pour tout $\lambda \in \Lambda$, les polynômes f_λ, sont *sans terme constant,* alors la condition $\sum_{\lambda\in\Lambda} deg\, f_\lambda < n$ implique que ces polynômes ont au moins un zéro commun, non nul.
En conclure que toute forme quadratique sur un corps fini, $f(X_1,X_2,\ldots,X_n)$, $n \geq 3$, a au moins un zéro non trivial.

Chapitre 5
Clôture algébrique d'un corps

Dans tout ce chapitre, la notion essentielle sera celle de *corps algébriquement clos*, dont la définition ([13], Déf. 4.42) a été rappelée dans les Préliminaires du Ch.3.

Proposition 5.1. *Pour un corps K, les propriétés suivantes sont équivalentes*
i) K est algébriquement clos.
ii) Tout polynôme non constant de $K[X]$ est scindé sur K.
iii) Tout polynôme irréductible de $K[X]$ est de degré 1.

Démonstration. *i)* $\Longrightarrow$ *ii)* ([13], Prop. 4.44).
ii) $\Longrightarrow$ *iii)* : Supposons que $f(X)$ soit un polynôme irréductible, de degré $n > 1$, dans $K[X]$; l'hypothèse *ii)* implique que $f(X)$ est scindé sur K, ce qui est impossible, donc $deg\, f = 1$.
iii) $\Longrightarrow$ *i)* : Dans l'anneau factoriel $K[X]$, tout polynôme non constant, $f(X)$, a au moins un diviseur irréductible ; d'après l'hypothèse *iii)* celui-ci est de degré 1, donc $f(X)$ a au moins une racine dans K ; autrement dit, K est algébriquement clos. □

Remarque 5.2. a) *Un corps fini n'est jamais algébriquement clos.*
En effet, soit K un corps fini ; posons $q := |K|$ et $K = \{a_i ; 1 \leq i \leq q\}$.
En notant 1, l'élément unité de K, considérons, dans $K[X]$, le polynôme

$$f(X) := (X - a_1)(X - a_2) \ldots (X - a_q) + 1;$$

alors, quel que soit $i\,(1 \leq i \leq q)$, on a $f(a_i) \neq 0$, donc K n'est pas algébriquement clos.
b) *Un corps algébriquement clos n'admet aucune extension algébrique propre.*

1. Théorème fondamental de l'Algèbre

C'est ainsi, qu'en général, est désigné (en Algèbre) le Théorème suivant.

Théorème 5.3. *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Il existe plusieurs démonstrations de ce résultat, extrêmement important dans l'ensemble des mathématiques. La première fut donnée par Gauss, en 1799. Compte tenu de la rigueur des mathématiques actuelles, cette démonstration présentait quelques imperfections, mais le principe général en était correct. Elle fut d'ailleurs reprise par Gauss, lui-même, en 1815, puis par d'autres mathématiciens. Dans sa version « revue et corrigée », elle figure dans plusieurs ouvrages (par exemple, [27]).

La preuve du Th. 5.3., donnée ici, utilise les propriétés P_1, P_2, P_3 ci-dessous, ainsi que le Théorème fondamental des polynômes symétriques ([13], Th. 8.14).

P_1 : *Tout polynôme de* $\mathbb{R}[X]$, de degré impair, *a au moins une racine dans* $\mathbb{R}$.

Cette propriété résulte d'un théorème d'Analyse, dit *Théorème de la valeur intermédiaire* (supposé connu) ([4]).
En effet, soit $f(X)$ dans $\mathbb{R}[X]$, de degré *n impair* : $f(X) = \sum_{0\leq i\leq n} a_i X^i$.
La fonction polynôme $\tilde{f} : \mathbb{R} \longrightarrow \mathbb{R}$ ([13], Déf. 4.21) est continue ; en supposant, par exemple, le coefficient directeur de f, a_n, strictement positif, alors (Th. de la valeur intermédiaire)

$$(\lim_{x\to-\infty} f(x) = -\infty \text{ et } \lim_{x\to+\infty} f(x) = +\infty) \Longrightarrow \exists x_o \in \mathbb{R} \text{ tel que } f(x_o) = 0.$$

P_2 : *Tout nombre réel* $a \geq 0$ *a une racine carrée dans* $\mathbb{R}$.

Une preuve en est donnée dans l'App. A de ce livre (Cor. A.10).
Les racines carrées, positive et négative d'un nombre réel $a > 0$, sont respectivement notées $\sqrt{a}$ et $-\sqrt{a}$.

P_3 : *Tout nombre complexe a une racine carrée dans* $\mathbb{C}$.

Ce résultat est une conséquence de la propriété P_2 (voir un cours de 1^{er} cycle [3], ou l'Ex. **1.** de ce chapitre).

Remarque 5.4. A partir de la propriété P_3, on montre facilement que tout polynôme du second degré, à coefficients dans $\mathbb{C}$, a deux racines dans $\mathbb{C}$ distinctes ou confondues (Ex.**1.** de ce chapitre).

Notations : Pour $z \in \mathbb{C}$, on désigne par $\overline{z}$ l'imaginaire conjugué de z et on note σ l'automorphisme de $\mathbb{C}$ tel que

$$\forall z \in \mathbb{C},\ \sigma(z) = \overline{z}.$$

Soit $\hat{\sigma}$ l'automorphisme de $\mathbb{C}[X]$ prolongeant σ. Pour $f(X) \in \mathbb{C}[X]$,

$$f(X) = \sum_{0\leq k\leq n} a_k X^k \Longrightarrow \hat{\sigma}(f(X)) = \sum_{0\leq k\leq n} \overline{a_k} X^k.$$

On pose alors, $\overline{f}(X) := \hat{\sigma}(f(X))$.

Remarque 5.5. Compte tenu des notations ci-dessus, $\hat{\sigma}$ étant un automorphisme, on a

$$deg\,\overline{f} = deg\, f ; \tag{5.1}$$

$$f(X) \text{ irréductible} \Longleftrightarrow \overline{f}(X) \text{ irréductible.} \tag{5.2}$$

$$\text{Pour } \alpha \in \mathbb{C},\quad f(\alpha) = 0 \Longleftrightarrow \overline{f}(\overline{\alpha}) = 0. \tag{5.3}$$

Lemme 5.6. *Tout polynôme* irréductible *de* $\mathbb{C}[X]$, *de degré* impair *est nécessairement de degré 1.*

Démonstration. Supposons $f(X) \in \mathbb{C}[X]$, *irréductible* et de degré $n > 1$, *impair.*
Il s'agit de montrer que ces hypothèses conduisent à une contradiction. Sans restreindre la généralité, on peut supposer $f(X)$ *unitaire* et on pose

$$g(X) := f(X)\overline{f}(X),$$

où, compte tenu des notations définies plus haut, $\overline{f}(X) := \hat{\sigma}(f(X))$.

$$\left(\overline{g}(X) = \overline{f}(X)\, f(X) = g(X)\right) \Longrightarrow g(X) \in \mathbb{R}[X].$$

a) Supposons $g(X)$ non irréductible dans $\mathbb{R}[X]$.
Il existe alors g_1, g_2 dans $\mathbb{R}[X]$ tels que

$$g = g_1 g_2, \quad 1 \leq deg\, g_1 < deg\, g, \quad 1 \leq deg\, g_2 < deg\, g. \tag{5.4}$$

Les polynômes f et $\overline{f}$ sont irréductibles dans l'anneau factoriel $\mathbb{C}[X]$. D'autre part, les relations (5.4) montrent que g_1 et g_2 ne sont pas des unités dans $\mathbb{C}[X]$; alors, compte tenu de l'unicité de la factorisation d'un polynôme de $\mathbb{C}[X]$ en un produit d'éléments irréductibles, ([13], Déf. 5.67), on a nécessairement, dans $\mathbb{C}[X]$,

$$g_1 g_2 = f\overline{f} \Longrightarrow (g_1 \sim f \text{ et } g_2 \sim \overline{f}) \quad \text{ou} \quad (g_1 \sim \overline{f} \text{ et } g_2 \sim f). \tag{5.5}$$

Les relations (5.5) impliquent, en particulier

$$deg\, g_1 = deg\, f = n > 1.$$

Or par hypothèse, n est impair et $g_1(X) \in \mathbb{R}[X]$; d'après la propriété P_1, le polynôme g_1 a donc au moins une racine dans $\mathbb{R}$ et, compte tenu des relations (5.5), il en est de même pour le polynôme f (ou $\overline{f}$) ce qui contredit l'hypothèse : f irréductible dans $\mathbb{C}[X]$.

b) On suppose $g(X)$ irréductible dans $\mathbb{R}[X]$.
On pose $d := deg\, g = 2n$ (Cf. relation (5.1)). Soit E un corps de décomposition de g sur $\mathbb{C}$. On a supposé f unitaire, donc $g = f\overline{f}$ est aussi unitaire. Dans $E[X]$, on peut écrire

$$g(X) = \prod_{1 \leq i \leq d} (X - \alpha_i), \tag{5.6}$$

où les α_i, $1 \leq i \leq d$, sont distincts ou confondus dans E. On considère alors le polynôme

$$h(X) := \prod_{1 \leq i < j \leq d} (X - (\alpha_i + \alpha_j)). \tag{5.7}$$

Le degré de h est égal au nombre de couples d'entiers (i, j) tels que $1 \leq i < j \leq d$; d'autre part, on a $n > 1$ et impair, d'où

$$deg\, h = C_d^2 = \frac{d(d-1)}{2} = n(2n-1) \Longrightarrow deg\, h > 1 \text{ et impair.} \tag{5.8}$$

La relation (5.7) montre que le polynôme h est *unitaire* et que tous ses coefficients, autres que le coefficient directeur, sont des polynômes *symétriques* en les α_i, $1 \leq i \leq d$, dans $\mathbb{R}[\alpha_1, \ldots, \alpha_d]$.
Désignons par Σ_i, $1 \leq i \leq d$, les fonctions symétriques élémentaires des α_i ([13], Ch. 8). D'après le Théorème fondamental des polynômes symétriques ([13], Th. 8.14), pour chaque coefficient c de h, autre que le coefficient directeur, il existe un unique polynôme $\varphi \in \mathbb{R}[\Sigma_1, \ldots, \Sigma_d]$ tel que

$$c = c(\alpha_1, \ldots, \alpha_d) = \varphi(\Sigma_1, \ldots, \Sigma_d).$$

Les α_i, $1 \leq i \leq d$, étant les racines du polynôme $g(X) \in \mathbb{R}[X]$, quel que soit $i (1 \leq i \leq d), \Sigma_i \in \mathbb{R}$ ([13], p. 259). On en déduit que $h(X) \in \mathbb{R}[X]$. Or h est de degré impair (Cf. (5.8)) donc h a une racine dans $\mathbb{R}$ (Cf. P_1).

Soit β une racine réelle de $h(X)$; il existe alors un couple (i,j) tel que $1 \leq i < j \leq d$ et $\beta = \alpha_i + \alpha_j$. Posons

$$p_1(X) := g(X + \frac{\beta}{2}) \quad \text{et} \quad p_2(X) := g(-X + \frac{\beta}{2}).$$

$g(X) \in \mathbb{R}[X], \beta \in \mathbb{R}$, donc p_1 et p_2 sont dans $\mathbb{R}[X]$.
Le polynôme g étant, par hypothèse, irréductible dans $\mathbb{R}[X]$, il en est de même pour les polynômes p_1 et p_2 ([13], Ch. 5, Ex. 19) ; on en déduit que, dans l'anneau factoriel $\mathbb{R}[X]$ ([13], Ch. 5),

$$deg\, p_1 = deg\, g = deg\, p_2 \Longrightarrow p_1 \sim p_2 \quad \text{ou} \quad p_1 \wedge p_2 = 1.$$

Mais $p_1(\frac{\alpha_i - \alpha_j}{2}) = g(\alpha_i) = 0$ et $p_2(\frac{\alpha_i - \alpha_j}{2}) = g(\alpha_j) = 0$.
Par suite, p_1 et p_2 ne sont pas premiers entre eux, donc ils sont associés et g étant unitaire, p_1 et p_2 sont aussi unitaires. On en conclut que $p_1 = p_2$ d'où

$$p_1(-X) = p_2(X) = p_1(X).$$

Le polynôme p_1 est symétrique en X, donc il existe un polynôme p dans $\mathbb{R}[X]$, tel que

$$p_1(X) = p(X^2).$$

$$(deg\, p_1 = deg\, g = 2n,\ n > 1) \Longrightarrow deg\, p = n.$$

Le polynôme $p(X) \in \mathbb{R}[X]$, de degré impair $n > 1$, a au moins une racine réelle a (Cf. P_1). Notons α une racine carrée de a dans $\mathbb{C}$ (Cf. P_3) ; alors

$$p(\alpha^2) = 0 \Longrightarrow p_1(\alpha) = g(\alpha + \frac{\beta}{2}) = f(\alpha + \frac{\beta}{2})\overline{f}(\alpha + \frac{\beta}{2}) = 0,$$

$$\text{d'où} \quad f(\alpha + \frac{\beta}{2}) = 0 \quad \text{ou} \quad \overline{f}(\alpha + \frac{\beta}{2}) = 0 \ (\Longleftrightarrow \overline{f(\alpha + \frac{\beta}{2})} = 0).$$

Ainsi f a une racine dans $\mathbb{C}$, ce qui contredit encore l'irréductibilité de f dans $\mathbb{C}[X]$.
On en conclut que, dans $\mathbb{C}[X]$, tout polynôme, irréductible et de degré impair, est nécessairement de degré 1. □

Preuve du Théorème fondamental de l'Algèbre (Th. 5.3) :

Démonstration. Il s'agit de montrer que tout polynôme *irréductible* $f(X)$, de $\mathbb{C}[X]$, est de degré 1 (Cf. Prop. 5.1).
Supposons $n := deg\, f > 1$ et $f(X)$ unitaire. Dans $\mathbb{N}^*$, on peut écrire, de façon unique,

$$n = 2^m q, \quad \text{avec} \quad m \geq 0 \ \text{et} \ q \ \text{impair}.$$

D'après le lemme 5.6, le résultat à prouver est vrai pour $m = 0$.
On suppose $m > 0$ et on raisonne par récurrence sur m ; l'hypothèse de récurrence étant qu'un polynôme irréductible de $\mathbb{C}[X]$, de degré $2^{m'}q'$, où $0 \leq m' < m$ et q' impair, est nécessairement de degré 1.
Soit F un corps de décomposition de f sur $\mathbb{C}$. Dans $F[X]$, on peut écrire

$$f(X) = \prod_{1 \leq i \leq n} (X - \lambda_i),$$

où les λ_i sont distincts ou confondus dans F. On pose

$$k(X) = \prod_{1 \leq i < j \leq n} (X - (\lambda_i + \lambda_j)).$$

$deg\, k = \dfrac{n(n-1)}{2} = 2^{m-1}q(2^m q - 1)$ et $q' := q(2^m q - 1)$ est impair.
D'autre part, comme dans la preuve du lemme 5.6., on montre, à l'aide du Théorème fondamental des polynômes symétriques, que $k(X) \in \mathbb{C}[X]$.
Dans l'anneau factoriel $\mathbb{C}[X]$, écrivons

$$k(X) = r_1(X)\, r_2(X) \ldots r_l(X), \text{ avec } l \geq 1, \tag{5.9}$$

les $r_i(X)$, $1 \leq i \leq l$, étant irréductibles et unitaires (non nécessairement distincts). Pour tout $i\,(1 \leq i \leq l)$, posons $deg\, r_i = 2^{m_i} q_i$ et (quitte à changer l'ordre des r_i) supposons, dans $\mathbb{N}$,

$$m_i \geq 0, q_i \text{ impair} \quad \text{et } 0 \leq m_1 \leq m_2 \leq \ldots m_l. \tag{5.10}$$

Les relations (5.9) et (5.10) impliquent alors,

$$deg\, k = 2^{m-1}q' = \sum_{1 \leq i \leq l} 2^{m_i} q_i = 2^{m_1}(q_1 + \sum_{2 \leq i \leq l} 2^{m_i - m_1} q_i). \tag{5.11}$$

En écrivant, dans $\mathbb{N}$,

$$q_1 + \sum_{2 \leq i \leq l} 2^{m_i - m_1} q_i = 2^s q'', \text{ avec } s \geq 0 \text{ et } q'' \text{ impair},$$

on obtient, en tenant compte des relations précédentes,

$$2^{m-1}q' = 2^{m_1 + s} q'' \Longrightarrow m - 1 = m_1 + s \Longrightarrow m_1 \leq m - 1.$$

Le polynôme irréductible et unitaire $r_1(X)$ est donc de degré $2^{m_1} q_1$, avec $0 \leq m_1 < m$ et q_1 impair ; l'hypothèse de récurrence implique alors $deg\, r_1 = 1$, par suite le polynôme $k(X)$ a au moins une racine dans $\mathbb{C}$.
Notons μ une racine de $k(X)$ dans $\mathbb{C}$; il existe donc un couple (i, j) tel que $1 \leq i < j \leq n$ et $\lambda_i + \lambda_j = \mu$. On considère les polynômes

$$f_1(X) := f(X + \frac{\mu}{2}) \quad \text{et} \quad f_2(X) := f(-X + \frac{\mu}{2}).$$

Le polynôme f étant irréductible et unitaire dans $\mathbb{C}[X]$, il en est de même des polynômes f_1 et f_2. De plus, on vérifie que $\dfrac{\lambda_i - \lambda_j}{2}$ est une racine commune à f_1 et f_2, dans F.
On en déduit, comme dans la preuve du lemme 5.6., que $f_1 = f_2$ et qu'il existe un polynôme $t(X) \in \mathbb{C}[X]$ tel que

$$f_1(X) = f_2(X) = t(X^2);$$

alors, $2deg\, t = deg\, f_1 = deg\, f = n \Longrightarrow deg\, t = 2^{m-1}q$.
Compte tenu de l'hypothèse de récurrence, tout diviseur irréductible de $t(X)$ dans $\mathbb{C}[X]$ est de degré 1, donc le polynôme t a au moins une racine c dans $\mathbb{C}$. Soit γ une racine carrée de c dans $\mathbb{C}$ (Cf. P_3).

$$t(c) = 0 \Longrightarrow f_1(\gamma) = 0 \Longrightarrow f(\gamma + \frac{\mu}{2}) = 0.$$

La dernière égalité contredit l'irréductibilité de $f(X)$, supposé de degré $n > 1$ dans $\mathbb{C}[X]$, donc $deg\, f = 1$. □

Remarque 5.7. Une autre démontration du Th. 5.3, utilisant la théorie de Galois, sera donnée au Ch.7.

2. Plongement d'un corps dans un corps algébriquement clos

Théorème 5.8. *Pour tout corps K, il existe au moins un corps E algébriquement clos et extension de K.*

Démonstration. La preuve proposée s'inspire de celle d'Emile Artin ([5]).

1 / Anneau de polynômes à une infinité d'indéterminées

Etant donné un corps K et une famille $\{X_i\}_{i\in I}$, où I est un ensemble de cardinal infini, on notera

$$A := K[\{X_i\}_{i\in I}],$$

l'anneau des polynômes sur K, à une infinité d'indéterminées, $\{X_i\}_{i\in I}$, dont les éléments sont définis comme suit.
On dit que

$$f \in A \iff \exists n \in \mathbb{N}^* \text{ et } \exists \{i_1, \dots i_n\} \subset I \text{ tels que } f \in K[X_{i_1}, \dots, X_{i_n}].$$

De façon naturelle, on munit A d'une addition et d'une multiplication : quels que soient f et g dans A, pour

$$f \in K[X_{i_1}, \dots, X_{i_n}] \quad \text{et} \quad g \in K[X_{j_1}, \dots, X_{j_m}],$$

on considère $f+g$ et fg dans l'anneau $K[X_{i_1}, \dots, X_{i_n}, X_{j_1}, \dots, X_{j_m}]$.
On vérifie que A est alors muni d'une structure d'anneau unitaire, commutatif, l'élément unité de A étant celui de K ; de plus, K se plonge canoniquement dans A.

2 / Démonstration du Théorème 5.8

Soit A l'anneau des polynômes sur K, à une infinité d'indéterminées indexées par l'ensemble $I = K[X] \setminus K$, donc

$$A = K[\{X_f\}_{f\in K[X]\setminus K}].$$

Notons $\mathfrak{I}$ l'idéal de A engendré par l'ensemble

$$\{f(X_f) \in K[X_f] \subset A \,;\, f \in K[X] \setminus K\}.$$

Montrons que $\mathfrak{I}$ est un idéal *propre* ([13], Déf. 1.45) de A.
Un élément quelconque de $\mathfrak{I}$ s'écrit sous la forme

$$\sum_{1\le i\le n} g_i f_i(X_{f_i}),$$

où $n \in \mathbb{N}^*$ et pour tout $i\,(1 \le i \le n)$, $g_i \in A$, $f_i \in K[X] \setminus K$.
Supposons que l'on ait

$$\sum_{1\le i\le n} g_i f_i(X_{f_i}) = 1. \tag{5.12}$$

Pour tout $i\,(1 \le i \le n)$, désignons par α_i une racine du polynôme $f_i(X_{f_i})$, dans un corps de décomposition sur K et considérons le corps

$$L := K(\alpha_1, \dots, \alpha_n).$$

La relation (5.12) est valable dans $L[\{X_f\}_{f\in K[X]\setminus K}]$, ce qui entraîne la contradiction suivante

$$1 = \sum_{1\le i\le n} g_i f_i(\alpha_i) = 0.$$

On en déduit que $1 \notin \mathfrak{I}$, donc $\mathfrak{I} \neq A$.

$\mathfrak{I}$ étant un idéal propre de l'anneau unitaire et commutatif A, il existe un idéal *maximal* $\mathfrak{M}$ de A contenant $\mathfrak{I}$ ([13], Cor. 2.72).
Posons $E_1 := A/\mathfrak{M}$; E_1 est un corps ([13], Th. 2.62) ; soit π la surjection canonique de A sur E_1 et u l'injection canonique de K dans A :

$$K \xrightarrow{u} A \xrightarrow{\pi} E_1.$$

$\pi \circ u$ est un morphisme non nul, donc un monomorphisme de K dans E_1, par suite E_1 *est une extension de* K. En identifiant K à son image par $\pi \circ u$, on peut considérer que l'on a $K \subseteq E_1$.
Montrons que tout polynôme $f(X) \in K[X] \setminus K$ a au moins une racine dans E_1.
D'après la définition des idéaux $\mathfrak{I}$ et $\mathfrak{M}$, on a

$$\forall f \in K[X] \setminus K, \quad f(X_f) \in \mathfrak{I} \subseteq \mathfrak{M} \Longrightarrow \pi(f(X_f)) = 0, \text{ dans } E_1.$$

Posons $\alpha := \pi(X_f)$ et $f(X_f) = \sum_{0 \leq j \leq n} a_j X_f^j$ dans $K[X_f] \setminus K$; alors

$$\pi(f(X_f)) = 0 \iff \sum_{0 \leq j \leq n} a_j \alpha^j = f(\alpha) = 0.$$

Ainsi α est une racine de f dans E_1.

En reprenant, à partir du corps E_1, le raisonnement fait à partir de K, on construit un corps E_2, extension de E_1, tel que

$$K \subseteq E_1 \subseteq E_2$$

et tout polynôme de $E_1[X] \setminus E_1$ a une racine dans E_2.
En réitérant le processus, on obtient, de proche en proche, une chaîne croissante d'extensions de corps :

$$K \subseteq E_1 \subseteq \cdots \subseteq E_k \subseteq E_{k+1} \subseteq \cdots$$

telle que, quel que soit $k \in \mathbb{N}^*$, tout polynôme de $E_k[X] \setminus E_k$ a au moins une racine dans E_{k+1}.
On pose $E_0 := K$ et $E := \bigcup_{k \in \mathbb{N}} E_k$.
La famille $\{E_k\}_{k \in \mathbb{N}}$ est totalement ordonnée par l'inclusion, donc E est un corps, extension de K. Vérifions que E est algébriquement clos.
Dans $E[X] \setminus E$, soit $f(X) = \sum_{0 \leq i \leq n} a_i X^i$, $deg\, f = n \geq 1$; il existe alors $k \in \mathbb{N}$ tel que $\{a_0, a_1, \ldots, a_n\} \subset E_k$; par suite, $f(X) \in E_k[X] \setminus E_k$.
Le polynôme $f(X)$ a donc au moins une racine dans $E_{k+1} \subseteq E$, d'où E algébriquement clos.
On en conclut que tout corps K peut être *plongé* dans un corps algébriquement clos. □

3. Clôture algébrique d'un corps

Définition 5.9. On appelle **clôture algébrique** d'un corps K, toute extension L de K telle que

i) L est algébrique sur K.

ii) L est un corps algébriquement clos.

Théorème 5.10. *Tout corps K admet une clôture algébrique.*
Plus précisément, si E est un corps algébriquement clos, extension de K, alors

$$\overline{K} := \{\alpha \in E \,;\, \alpha \text{ algébrique sur } K\} \tag{5.13}$$

est un corps et c'est une clôture algébrique de K.

Démonstration. D'après le Th. 5.8., pour tout corps K, il existe au moins un corps E algébriquement clos et extension de K. On considère alors l'ensemble $\overline{K}$ défini par la relation (5.13).
Vérifions que $\overline{K}$ est un sous-corps de E.
On a $\overline{K} \neq \emptyset$, car $K \subseteq \overline{K}$. Il faut alors prouver que quels que soient α, β dans $\overline{K}$, on a $\alpha - \beta$ et $\alpha\beta$ dans $\overline{K}$ et si $\alpha \neq 0$, alors $\alpha^{-1} \in \overline{K}$.
D'après la définition de $\overline{K}$, α et β sont algébriques sur K, donc $K(\alpha, \beta)$ est une extension algébrique de K telle que

$$K \subseteq K(\alpha, \beta) \subseteq \overline{K}.$$

Or $\alpha - \beta$ et $\alpha\beta$ sont dans $K(\alpha, \beta)$, donc dans $\overline{K}$. De plus, $\alpha \neq 0$ implique

$$\alpha^{-1} \in K(\alpha) \subseteq K(\alpha, \beta) \subseteq \overline{K}.$$

On en déduit que $\overline{K}$ *est une extension algébrique de* K.

Il reste à prouver que $\overline{K}$ est un corps algébriquement clos.
Soit $f(X)$ un polynôme non constant dans $\overline{K}[X]$.

$$\overline{K} \subseteq E \Longrightarrow f(X) \in E[X] \setminus E.$$

E étant algébriquement clos, $f(X)$ a au moins une racine α dans E.
Or, $f(X) \in \overline{K}[X]$, donc α est algébrique sur $\overline{K}$; d'après la Rem. 2.32,

$$(\overline{K} : K \text{ algébrique et } \alpha \text{ algébrique sur } \overline{K}) \Longrightarrow \alpha \text{ algébrique sur } K.$$

On en déduit que $\alpha \in \overline{K}$, par suite $\overline{K}$ est *algébriquement clos*.
En conclusion : $\overline{K}$ est une *clôture algébrique de* K. □

Exemple 5.11. :
1) $\mathbb{C}$ est extension algébrique de $\mathbb{R}$ ($\mathbb{C} = \mathbb{R}(i)$) et $\mathbb{C}$ est un corps algébriquement clos (Th. 5.3), donc $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
2) On remarque que $\mathbb{C}$ *n'est pas une clôture algébrique de* $\mathbb{Q}$, car $\mathbb{C}$ n'est pas algébrique sur $\mathbb{Q}$, puisqu'il contient, en particulier les nombres π et e qui sont transcendants sur $\mathbb{Q}$ (Cf. App. B, ou cor. 5.20.). Cependant $\mathbb{C}$ est algébriquement clos et contient $\mathbb{Q}$, donc

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \,;\, \alpha \text{ algébrique sur } \mathbb{Q}\} \subsetneq \mathbb{C}$$

est une clôture algébrique de $\mathbb{Q}$ (Th. 5.10.).
On peut prouver, de différentes façons, que $\overline{\mathbb{Q}}$ est *de degré infini* sur $\mathbb{Q}$.
Dans l'Ex. **13.**, Ch. 2., on montre que si

$$p_1 < p_2 < \cdots < p_n < p_{n+1} < \ldots$$

est la suite croissante des nombres premiers dans $\mathbb{N}$, alors

$$F : \mathbb{Q}, \text{ où } F = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}, \ldots),$$

est une extension *algébrique* de *degré infini* sur $\mathbb{Q}$. D'après la définition de $\overline{\mathbb{Q}}$, on a

$$\mathbb{Q} \subset F \subset \overline{\mathbb{Q}},$$

alors

$$[F : \mathbb{Q}] \text{ infini} \Longrightarrow [\overline{\mathbb{Q}} : \mathbb{Q}] \text{ infini}.$$

L'Ex. **2.** de ce chapitre donne une autre justification de cette propriété.

Remarque 5.12. A priori, il peut exister différents corps algébriquement clos et extensions de K, donc éventuellement différentes clôtures algébriques de K, mais nous allons prouver qu'elles sont toutes K-isomorphes.

Lemme 5.13. *Soit $L : K$ et $E : K$ des extensions de corps, respectivement définies par les couples (L,u) et (E,v)* (Rem. 1.9). *Si l'extension $L : K$ est algébrique et si le corps E est algébriquement clos, alors*

1) *il existe un monomorphisme $\sigma : L \longrightarrow E$ tel que $\sigma \circ u = v$;*

2) *si de plus, L est algébriquement clos et E est algébrique sur $v(K)$, alors σ est un isomorphisme.*

Démonstration. On peut supposer $K \subseteq L$ et $K \subseteq E$, c'est-à-dire que u et v sont des injections canoniques.

1) On désigne par $\mathcal{F}$ l'ensemble des extensions *algébriques* F de K telles que $K \subseteq F \subseteq L$ et pour lesquelles il existe un monomorphisme $\tau : F \longrightarrow E$, tel que $\tau_{/K} = v$.

Soit $\mathcal{S}$ l'ensemble des couples (F,τ), où $F \in \mathcal{F}$. On a $\mathcal{S} \neq \emptyset$, car $(K,v) \in \mathcal{S}$.
On considère, dans $\mathcal{S}$, la relation binaire, notée $\leq$, définie par

$$(F,\tau) \leq (F',\tau') \iff F \subseteq F' \text{ et } \tau'_{/F} = \tau.$$

La relation $\leq$ est une *relation d'ordre partiel* dans $\mathcal{S}$ (à vérifier).

Montrons que l'ensemble partiellement ordonné $\mathcal{S}$ est *inductif* ([13], Déf. 2.69).

Soit $\{(F_i,\tau_i)\}_{i\in I}$ une famille totalement ordonnée d'éléments de $\mathcal{S}$, alors
$F := \bigcup_{i\in I} F_i$ est un corps tel que $K \subseteq F \subseteq L$; de plus, pour tout $i \in I$, F_i est algébrique sur K, par suite F est algébrique sur K.

On définit un monomorphisme $\tau : F \longrightarrow E$ en posant, quel que soit $i \in I$, $\tau_{/F_i} = \tau_i$, ce qui implique $\tau_{/K} = v$.

On en déduit que le couple (F,τ), ainsi défini, appartient à $\mathcal{S}$ et est un majorant pour la famille $\{(F_i,\tau_i)\}_{i\in I}$. Par suite, l'ensemble partiellement ordonné $\mathcal{S}$ est *inductif* ; alors, selon l'axiome de Zorn ([13], p. 50), il existe au moins un élément *maximal* dans $\mathcal{S}$; notons (M,σ) un tel élément.

On a $K \subseteq M \subseteq L$, M algébrique sur K et $\sigma_{/K} = v$; démontrons que $M = L$. Supposons $M \subsetneq L$; il existe alors $\alpha \in L$ tel que $\alpha \notin M$. Par hypothèse, α est algébrique sur K ; posons $p(X) := Irr_K(\alpha,X)$.

Soit $\hat{v} : K[X] \longrightarrow E[X]$ le prolongement canonique de v ; on pose

$$\hat{p}(X) := \hat{v}(p(X)).$$

Par hypothèse, E est algébriquement clos, donc le polynôme $\hat{p}(X)$ a au moins une racine β dans E.

Désignons par σ' le monomorphisme de $M(\alpha)$ dans L défini par :

$$\sigma'_{/M} = \sigma \quad \text{et} \quad \sigma'(\alpha) = \beta.$$

On a alors

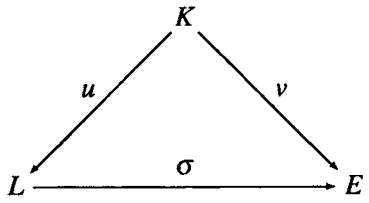
$$\sigma'_{/K} = v \quad \text{et} \quad K \subseteq M \subsetneq M(\alpha) \subseteq L.$$

De plus $M(\alpha)$ est algébrique sur K, d'où

$$(M(\alpha),\sigma') \in \mathcal{S} \quad \text{et} \quad (M,\sigma) \lneqq (M(\alpha),\sigma') ;$$

ce qui contredit la maximalité de (M,σ) dans $\mathcal{S}$; ainsi, $M = L$, d'où le diagramme com-

mutatif :



donc $\sigma \circ u = v$, ce qui est équivalent à $\sigma_{/K} = id_K$, lorsque u et v sont les injections canoniques.

2) Montrons que si E est algébrique sur $v(K)$ et L algébriquement clos, alors le monomorphisme $\sigma : L \longrightarrow E$ est surjectif.

D'après ce qui précède, on a

$$v(K) = \sigma(K) \quad \text{et} \quad \sigma(K) \subseteq \sigma(L) \subseteq E.$$

D'autre part,

$$L \text{ algébriquement clos} \Longrightarrow \sigma(L) \text{ algébriquement clos.}$$

Soit $\gamma \in E$; posons $p(X) := Irr_{\sigma(K)}(\gamma, X)$. On peut considérer $p(X)$ comme un polynôme de $\sigma(L)[X]$, or $\sigma(L)$ est algébriquement clos, donc $\gamma \in \sigma(L)$, d'où $\sigma(L) = E$.

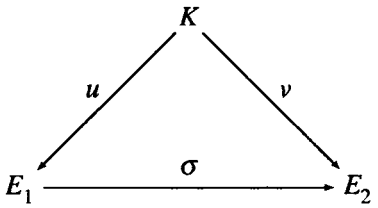
On en conclut que σ est un isomorphisme. □

Théorème 5.14. *Deux clôtures algébriques d'un corps K sont K-isomorphes.*

Démonstration. Soit E_1 et E_2 deux clôtures algébriques d'un corps K.

Les hypothèses permettent d'appliquer la partie 2) du lemme 5.13. avec $L = E_1$ et $E = E_2$.

On obtient, alors le diagramme commutatif suivant, où l'on peut supposer que u et v sont les injections canoniques de K dans E_1 et K dans E_2,



d'après le lemme 5.13, σ est un isomorphisme, de plus $\sigma \circ u = v$ équivaut à $\sigma_{/K} = id_K$; donc σ est un K-isomorphisme. □

Remarque 5.15. Le Th. 5.14 montre que tout corps K a une clôture algébrique unique, à un K-isomorphisme près ; on pourra donc éventuellement parler de *la* clôture algébrique d'un corps et celle-ci sera généralement noter $\overline{K}$.

4. Clôture algébrique d'un corps fini

Comme dans le chapitre 4, p étant un nombre premier et n un entier strictement positif, on notera $\mathbb{F}_{p^n}$ un corps fini de caractéristique p et de cardinal p^n et on supposera $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$.

Rappel : Un corps fini ne peut être algébriquement clos (Rem. 5.2).

D'autre part, pour m et n dans $\mathbb{N}^*$, on a (Th. 4.8)

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n.$$

Par suite, quels que soient m et n dans $\mathbb{N}^*$,

$$1 \leq m \leq n \Longrightarrow m! \mid n! \Longrightarrow \mathbb{F}_{p^{m!}} \subseteq \mathbb{F}_{p^{n!}}.$$

Théorème 5.16. *Soit p un nombre premier, alors pour tout entier $n \geq 1$, $E = \bigcup_{k \in \mathbb{N}^*} \mathbb{F}_{p^{k!}}$ est une clôture algébrique du corps fini $\mathbb{F}_{p^n}$.*

Démonstration. La famille $\{\mathbb{F}_{p^{k!}}\}_{k \in \mathbb{N}^*}$ de corps finis de caractéristique p, étant totalement ordonnée par l'inclusion, $E = \bigcup_{k \in \mathbb{N}^*} \mathbb{F}_{p^{k!}}$ est un corps. De plus,

$$\forall k \in \mathbb{N}^*, \ (\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^{k!}} \Longrightarrow \mathbb{F}_{p^k} \subseteq E). \tag{5.14}$$

a) Montrons que, quel que soit $n \in \mathbb{N}^*$, E est une extension algébrique de $\mathbb{F}_{p^n}$.
Soit n donné dans $\mathbb{N}^*$ et x quelconque dans E ;

$$x \in E \Longrightarrow \exists m \in \mathbb{N}^* \text{ tel que } x \in \mathbb{F}_{p^{m!}}.$$

On choisit le plus petit entier m tel que $x \in \mathbb{F}_{p^{m!}}$.

– Si $m \leq n$, alors $\mathbb{F}_{p^{m!}} \subseteq \mathbb{F}_{p^{n!}} \Longrightarrow x \in \mathbb{F}_{p^{n!}}$ et (Th. 2.26.)
$[\mathbb{F}_{p^{n!}} : \mathbb{F}_{p^n}] < \infty \Longrightarrow \mathbb{F}_{p^{n!}}$ algébrique sur $\mathbb{F}_{p^n}$,
d'où x algébrique sur $\mathbb{F}_{p^n}$.
– Si $n < m$, on a alors, $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^{n!}} \subset \mathbb{F}_{p^{m!}}$ et $[\mathbb{F}_{p^{m!}} : \mathbb{F}_{p^n}] < \infty$,
d'où, comme précédemment, x algébrique sur $\mathbb{F}_{p^n}$.

b) Démontrons que E est algébriquement clos.
Soit $f(X) \in E[X]$ tel que $f(X) = \sum_{0 \leq i \leq r} a_i X^i$, $\deg f = r \geq 1$.
Il existe $k \in \mathbb{N}^*$ tel que $\{a_0, a_1, \ldots, a_r\} \subseteq \mathbb{F}_{p^{k!}}$; on a alors $f(X) \in \mathbb{F}_{p^{k!}}[X]$.
Soit L un corps de décomposition de f sur $\mathbb{F}_{p^{k!}}$, alors L est de degré fini sur $\mathbb{F}_{p^{k!}}$ (Th. 4.5) ; on en déduit que L est de degré fini sur $\mathbb{F}_p$, car

$$[L : \mathbb{F}_p] = [L : \mathbb{F}_{p^{k!}}] \, [\mathbb{F}_{p^{k!}} : \mathbb{F}_p].$$

Si $[L : \mathbb{F}_p] = s$, alors L est un corps fini de cardinal p^s que l'on peut identifier à $\mathbb{F}_{p^s}$ (Cf. Ch. 4) et d'après la relation (5.14), on a $L = \mathbb{F}_{p^s} \subseteq E$.
Par suite, le polynôme $f(X)$ est scindé sur E ; on en déduit que E est algébriquement clos (Prop. 5.1.).
En conclusion, quel que soit l'entier $n \geq 1$, $E = \bigcup_{k \in \mathbb{N}^*} \mathbb{F}_{p^{k!}}$ est une clôture algébrique du corps fini $\mathbb{F}_{p^n}$. □

5. Transcendance de e et de π sur $\mathbb{Q}$

Une preuve complète de la transcendance, sur $\mathbb{Q}$, des nombres réels e et π, utilisant des méthodes classiques d'Analyse, est donnée dans l'appendice B. La démontration que nous proposons ici s'appuie sur le **Théorème de Lindemann-Weierstrass** ([29], p. 268), que nous ne pouvons démontrer dans le cadre de ce livre, mais que nous appliquerons.

Définition 5.17. Soit $L : K$ une extension de corps ; des éléments $\alpha_1, \ldots, \alpha_n$ de L, $n \in \mathbb{N}^*$, sont dits **algébriquement indépendants sur** K si

$$\forall\, f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n] \setminus K,\ \ f(\alpha_1, \ldots, \alpha_n) \neq 0.$$

Remarque 5.18. a) La définition 5.17 généralise, pour $n > 1$, la définition d'un élément transcendant sur un corps (Déf. 2.2), qui correspond au cas $n = 1$.
b) Des éléments algébriquement indépendants, sur un corps K, sont, a fortiori, algébriquement indépendants, sur tout sous-corps de K.

Théorème 5.19. Théorème de Lindemann-Weierstrass
Quel que soit $n \in \mathbb{N}^*$, si $z_1, z_2, \ldots z_n$ sont des éléments de $\overline{\mathbb{Q}}$ linéairement indépendants sur $\mathbb{Q}$, alors les nombres complexes $e^{z_1}, e^{z_2}, \ldots, e^{z_n}$ sont algébriquement indépendants sur $\overline{\mathbb{Q}}$.

Corollaire 5.20. *e et π sont transcendants sur $\mathbb{Q}$.*

Démonstration. D'après le Th. 5.19, appliqué dans le cas $n = 1$, quel que soit $z \neq 0$ dans $\overline{\mathbb{Q}}$, e^z est transcendant sur $\overline{\mathbb{Q}}$; alors, en prenant $z = 1$, on obtient : e transcendant sur $\overline{\mathbb{Q}}$, donc a fortiori, sur $\mathbb{Q}$.
Par ailleurs, dans $\mathbb{C}$, $e^{i\pi} = \cos\pi + i\sin\pi = -1 \in \mathbb{Q} \subset \overline{\mathbb{Q}}$.
Par suite, d'après ce qui précède, $i\pi \notin \overline{\mathbb{Q}}$; alors, $i \in \overline{\mathbb{Q}}$ implique $\pi \notin \overline{\mathbb{Q}}$, donc π est transcendant sur $\mathbb{Q}$. □

6. Théorème de Frobenius

Le corps gauche des **quaternions réels** $\mathbb{H}$ ([13], Déf. 1.6), qui intervient dans le Théorème de Frobenius (publié en 1878), est étudié dans "Eléments de théorie des anneaux" ([13], Ch. 3).
Rappelons que $\mathbb{R}$ et $\mathbb{C}$ sont des sous-corps commutatifs de $\mathbb{H}$ et qu'en particulier, le centre ([13], Déf. 1.32.) de $\mathbb{H}$ est le corps $\mathbb{R}$. ([13], Prop. 3.86.).

Théorème 5.21. *Tout corps K, non nécessairement commutatif, dont le centre contient le corps $\mathbb{R}$ des nombres réels, et qui est de dimension finie sur $\mathbb{R}$, est isomorphe soit à $\mathbb{R}$, soit au corps des nombres complexes $\mathbb{C}$, soit au corps des quaternions réels $\mathbb{H}$.*

Démonstration. En notant $Z(K)$ le centre de K, on a, par hypothèse,

$$\mathbb{R} \subseteq Z(K) \subseteq K \quad \text{et} \quad [K : \mathbb{R}] = dim_{\mathbb{R}} K < \infty. \tag{5.15}$$

– Si K est un corps *commutatif*, alors $Z(K) = K$ et

$$1 \leq [K : \mathbb{R}] < \infty \Longrightarrow K = \mathbb{R} \quad \text{ou} \quad K \simeq \mathbb{C},$$

car $\mathbb{C}$ est clôture algébrique de $\mathbb{R}$ et $[\mathbb{C} : \mathbb{R}] = 2$.

– Supposons K *non commutatif* ; dans la relation (5.15), on a

$$\mathbb{R} \subseteq Z(K) \subsetneq K.$$

Soit $x \in K \setminus \mathbb{R}$ et $\mathbb{R}(x)$ le plus petit sous-corps commutatif de K contenant $\mathbb{R}$ et x, alors

$$1 < [\mathbb{R}(x) : \mathbb{R}] < \infty \Longrightarrow \mathbb{R}(x) \simeq \mathbb{C}.$$

On en déduit qu'il existe $\varepsilon_1 \in K \setminus \mathbb{R}$ tel que

$$\varepsilon_1^2 = -1 \quad \text{et} \quad \mathbb{R}(\varepsilon_1) = \mathbb{R}(x).$$

Le corps $\mathbb{R}$ n'ayant pas d'extension algébrique *propre*, autre que $\mathbb{C}$ (à un isomorphisme

près), $\mathbb{R}(\varepsilon_1)$ est un sous-corps commutatif *maximal* de K et tout élément de K qui commute avec ε_1 est dans $\mathbb{R}(\varepsilon_1)$.
Soit $y \in K \setminus \mathbb{R}(\varepsilon_1)$; y ne commute pas avec ε_1, posons $z := y\varepsilon_1 - \varepsilon_1 y$.

$$\text{On a} \quad z \neq 0, \quad \varepsilon_1 z = y + \varepsilon_1 y \varepsilon_1 \quad \text{et} \quad z\varepsilon_1 = -y - \varepsilon_1 y \varepsilon_1,$$
$$\text{d'où} \quad (z\varepsilon_1 = -\varepsilon_1 z \neq 0) \Longrightarrow z \notin \mathbb{R}(\varepsilon_1) \Longrightarrow \mathbb{R}(z) \neq \mathbb{R}(\varepsilon_1).$$

Or, $\mathbb{R}(z)$ est, une extension algébrique propre de $\mathbb{R}$ contenue dans K, d'où

$$\mathbb{R}(z) \simeq \mathbb{R}(\varepsilon_1) \simeq \mathbb{C}.$$
$$\text{On en déduit que} \quad \mathbb{R}(z) \neq \mathbb{R}(\varepsilon_1) \Longrightarrow \mathbb{R} = \mathbb{R}(z) \cap \mathbb{R}(\varepsilon_1).$$
$$\text{Par suite,} \quad z\varepsilon_1 = -\varepsilon_1 z \Longrightarrow z^2 \varepsilon_1 = -z\varepsilon_1 z = \varepsilon_1 z^2,$$
$$\Longrightarrow z^2 \in \mathbb{R}(z) \cap \mathbb{R}(\varepsilon_1) = \mathbb{R}.$$

Mais $z \notin \mathbb{R}$, donc z^2 n'est pas un nombre réel positif, d'où $z^2 < 0$ dans $\mathbb{R}$.
Soit $\sqrt{-z^2}$ la racine carrée positive de $-z^2$ dans $\mathbb{R}$; posons $\varepsilon_2 := \dfrac{z}{\sqrt{-z^2}}$, alors

$$\varepsilon_2^2 = -1 \quad \text{et} \quad \varepsilon_1 \varepsilon_2 = -\varepsilon_2 \varepsilon_1.$$

Posons $\varepsilon_3 := \varepsilon_1 \varepsilon_2$; dans K, $\varepsilon_1, \varepsilon_2, \varepsilon_3$ vérifient les relations

$$\varepsilon_1^2 = \varepsilon_2^2 = \varepsilon_3^2 = -1, \tag{5.16}$$
$$\varepsilon_1 \varepsilon_2 = -\varepsilon_2 \varepsilon_1 = \varepsilon_3 \; ; \; \varepsilon_2 \varepsilon_3 = -\varepsilon_3 \varepsilon_2 = \varepsilon_1 \; ; \; \varepsilon_3 \varepsilon_1 = -\varepsilon_1 \varepsilon_3 = \varepsilon_2. \tag{5.17}$$

De plus, les éléments $1, \varepsilon_1, \varepsilon_2, \varepsilon_3$ sont linéairement indépendants sur $\mathbb{R}$, comme on peut le vérifier, en montrant que les relations (5.16) et (5.17) impliquent (avec $\varepsilon_0 := 1$)

$$\Big(\sum_{0 \leq i \leq 3} a_i \varepsilon_i = 0, \text{ où } a_i \in \mathbb{R}, \forall i (0 \leq i \leq 3) \Big) \Longrightarrow a_i = 0, \forall i (0 \leq i \leq 3).$$

On en déduit que le sous-corps K_1 de K engendré par $\{1, \varepsilon_1, \varepsilon_2, \varepsilon_3\}$ est *isomorphe au corps des quaternions* $\mathbb{H}$ ([13], Ch. 3) ; $\mathbb{R}$ est alors le centre de K_1 et on a

$$\mathbb{R} \subset \mathbb{R}(\varepsilon_1) \subset K_1 \subseteq K, \quad \text{avec } \mathbb{R}(\varepsilon_1) \simeq \mathbb{C}.$$

Montrons que $K_1 = K$.
Supposons qu'il existe $u \in K \setminus K_1$; alors $u \notin \mathbb{R}(\varepsilon_1)$. En considérant l'extension de $\mathbb{R}$ contenue dans K et obtenue par l'adjonction de ε_1 et u, soit $\mathbb{R}(\varepsilon_1, u)$, on obtient

$$\mathbb{R}(\varepsilon_1) \subset \mathbb{R}(\varepsilon_1, u) \subset K,$$

ce qui est en contradiction avec la maximalité du corps commutatif $\mathbb{R}(\varepsilon_1)$ dans K, d'où $K_1 = K$. □

7. Exercices

1. *Justification de la propriété P_3 et de la Rem.* 5.4.
1°) Montrer que pour tout élément $a + ib \in \mathbb{C} = \mathbb{R}(i)$, où $i^2 = -1$, il existe $z \in \mathbb{C}$ tel que $z^2 = a + ib$.
Indication : en posant $z = x + iy$, vérifier que la question revient à trouver x et y dans $\mathbb{R}$ tels que

$$(x^2 + y^2)^2 = a^2 + b^2 \quad \text{et} \quad 2xy = b.$$

En déduire qu'en désignant par $\sqrt{a^2+b^2}$ la racine carrée positive de a^2+b^2 dans $\mathbb{R}$, on obtient

$$z = \pm\left(\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + \varepsilon i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}\right),$$

où $\varepsilon = 1$ si $b > 0$ et $\varepsilon = -1$ si $b < 0$.

2°) Montrer que le résultat précédent entraîne que tout polynôme du second degré $f(X) := \alpha X^2 + \beta X + \gamma$ de $\mathbb{C}[X]$ a deux racines dans $\mathbb{C}$, distinctes ou confondues.

Indication : écrire $f(X) = \alpha\left[(X+\frac{\beta}{2\alpha})^2 - \frac{\beta^2}{4\alpha^2} + \frac{\gamma}{\alpha}\right]$.

2. Etant donné un nombre premier p ([13], App. A, Déf. A.5), pour tout entier $n > 1$, on considère le polynôme

$$f_n(X) = X^n + pX^{n-1} + pX^{n-2} + \cdots + pX + p.$$

1°) Prouver, à l'aide du critère d'Eisenstein ([13], Prop. 5.112), que tout polynôme $f_n(X)$ est irréductible dans $\mathbb{Z}[X]$; en déduire que $f_n(X)$ est irréductible dans $\mathbb{Q}[X]$ ([13], Prop. 5.108).

2°) Démontrer que pour tout entier $n > 1$, on a $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$; en conclure que

$[\overline{\mathbb{Q}} : \mathbb{Q}]$ est infini.

3. Les corps $\overline{\mathbb{Q}}$ et $\overline{\mathbb{Q}} \cap \mathbb{R}$ sont-ils des corps ordonnés ? (Cf. App. A.)

4. 1°) Soit $K = \mathbb{Q}(\sqrt{2})$ et $L = \mathbb{Q}(i)$, où $i^2 = -1$ dans $\mathbb{C}$.
Déterminer, dans $\mathbb{C}$, la clôture algébrique de chacun de ces corps.

2°) Soit $M = \mathbb{Q}(\pi)$ et $\overline{M}$ la clôture algébrique de M contenue dans $\mathbb{C}$; vérifier que

$$\overline{\mathbb{Q}} \subsetneq \overline{M} \subsetneq \mathbb{C}.$$

5. Soit L une extension algébrique d'un corps K de cardinal *infini*. En considérant L comme une réunion disjointe d'ensembles finis, chacun d'eux étant l'ensemble des racines, dans L, d'un polynôme unitaire, irréductible de $K[X]$, prouver que

$$card(L) = card(K).$$

En déduire que la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ est dénombrable.

6. *Nullstellensatz théorème de Hilbert*

K étant un corps algébriquement clos, soit $n > 1$ dans $\mathbb{N}$ et $K[X_1, \ldots, X_n]$ l'algèbre des polynômes à n indéterminées sur K.

Conventions préliminaires :

– Un élément P de K^n sera appelé *un point* ;

$$P \in K^n \iff P = (a_1, \ldots, a_n),\ a_i \in K,\ \forall i (1 \leq i \leq n).$$

K^n est alors considéré comme *n-espace affine* sur K ([23]).

– Pour $f \in K[X_1, \ldots, X_n]$ et $P = (a_1, \ldots, a_n)$ dans K^n, on pose

$$f(P) := f(a_1, \ldots, a_n).$$

On dit que P est un *zéro* de f si $f(P) = 0$.

– Pour $f \in K[X_1, \ldots, X_n]$, on pose

$$V(f) := \{P \in K^n\ ;\ f(P) = 0\}.$$

On dit que $V(f)$ est *l'hypersurface de K^n engendrée par f* ([23]).

D'une façon générale, pour une partie *non vide* S de $K[X_1, \ldots, X_n]$, on pose

$$V(S) := \{P \in K^n\ ;\ f(P) = 0,\ \forall f \in S\}$$

$V(S)$ est, par définition, la *variété algébrique affine de K^n engendrée par S* ([23]).
Si S est une partie finie, non vide, de $K[X_1,\ldots,X_n]$, telle que

$$S=\{f_1,\ldots,f_r\},\ ;\ r\in\mathbb{N}^*,\ f_i\in K[X_1,\ldots,X_n],\ \forall i(1\leq i\leq r),$$
$$\text{on écrira}\qquad V(S)=V(f_1,\ldots,f_r).$$

I

1°) a) Vérifier que $V(0)=K^n$ et $V(K[X_1,\ldots,X_n])=\emptyset$.
b) S et S' étant des parties non vides de $K[X_1,\ldots,X_n]$, montrer que

$$S\subseteq S'\Longrightarrow V(S)\supseteq V(S').$$

c) S étant une partie non vide de $K[X_1,\ldots,X_n]$, vérifier que

$$V(S)=\cap_{f\in S}V(f).$$

I désignant l'idéal de $K[X_1,\ldots,X_n]$ engendré par S, prouver que

$$V(I)=V(S).$$

2°) On dit qu'une partie E de K^n est une *variété algébrique affine* de K^n, s'il existe une partie non vide S de $K[X_1,\ldots,X_n]$ telle que

$$E=V(S).$$

Démontrer que, pour toute variété algébrique affine E de K^n, il existe une famille finie $\{f_1,\ldots,f_r\}, r\in\mathbb{N}^*$, de polynômes de
$K[X_1,\ldots,X_n]$ telle que

$$E=V(f_1,\ldots,f_r)\quad\text{(voir [13], Th. 4.72)}$$

– Vérifier que K^n et la partie vide de K^n sont des variétés algébriques affines de K^n.
– En conclure que toute variété algébrique affine de K^n est l'intersection d'un nombre fini d'hypersurfaces de K^n.

II

Etant donné une partie non vide F de K^n, on pose

$$I(F):=\{f\in K[X_1,\ldots,X_n]\ ;\ f(P)=0,\forall P\in F\}$$

et par convention $I(\emptyset)=K[X_1,\ldots,X_n]$.
1°) a) Prouver que pour toute partie F de K^n, $I(F)$ est un idéal de $K[X_1,..,X_n]$. On dira que $I(F)$ est *l'idéal de F*.
b) Montrer que $I(K^n)=(0)$ (voir [13], Prop. 4.71).
c) Vérifier que pour deux parties de K^n, F et F',

$$F\subseteq F'\Longrightarrow I(F)\supseteq I(F').$$

d) S étant une partie non vide de $K[X_1,\ldots,X_n]$ et F une partie de K^n, démontrer que

$$S\subseteq I(V(S))\quad\text{et}\quad F\subseteq V(I(F)).$$

En déduire les égalités

$$V(I(V(S)))=V(S)\quad\text{et}\quad I(V(I(F)))=I(F).$$

2°) Soit point $P=(a_1,\ldots,a_n)\in K^n$; on considère l'application

$$\sigma_P: K[X_1,\ldots,X_n]\longrightarrow K$$
$$f\longmapsto f(P).$$

On note que σ_P est un morphisme d'anneaux unitaires.
Prouver que $I:=Ker\,\sigma_P$ est un idéal maximal de $K[X_1,\ldots,X_n]$.
3°) Rappels ([13], Ex. **14.** et **15.**, Ch. 2) :
B désignant un anneau unitaire commutatif, pour tout idéal J de B, on pose

$$\sqrt{J}:=\{x\in B\ ;\ \exists m\in\mathbb{N}^*, x^m\in J\}.$$

$\sqrt{J}$ est appelé le *radical* de J.

$\sqrt{J}$ est un idéal de B contenant J et on dit que J est un *idéal radical* si $J = \sqrt{J}$. On vérifiera que tout idéal premier est un idéal radical.
a) Montrer que pour tout point P de K^n, $I(P)$ est un idéal radical.
b) Prouver que, plus généralement, quelle que soit la partie F de K^n, $I(F)$ est un idéal radical.

III

I étant un idéal de $K[X_1,\ldots,X_n]$, le but de ce qui suit est de démontrer l'égalité :

$$I(V(I)) = \sqrt{I}. \tag{5.18}$$

1°) Montrer que pour tout idéal I de $K[X_1,\ldots,X_n]$, on a
$$V(I) = V(\sqrt{I}) \quad \text{et} \quad \sqrt{I} \subseteq I(V(I)).$$
2°) L'objet de cette question est de prouver l'inclusion
$$I(V(I)) \subseteq \sqrt{I}.$$
a) Examiner les cas $I = 0$ et $I = K[X_1,\ldots,X_n]$.
b) On suppose $I \neq 0$ et $I \neq K[X_1,\ldots,X_n]$; justifier l'existence, dans $K[X_1,\ldots,X_n]$, d'un nombre fini de polynômes, $f_1,\ldots,f_r$,
$r \geq 1$, engendrant I.
Etant donné un polynôme $g \in I(V(I)) \setminus \{0\}$, il s'agit de trouver $m \in \mathbb{N}^*$ tel que $g^m \in I$.
On considére l'anneau de polynômes à $n+1$ indéterminées :
$$B := K[X_1,\ldots,X_n,Y].$$
Soit J l'idéal de B engendré par $\{f_1,\ldots,f_r,gY-1\}$.
– Démontrer que l'on a $V(J) \neq \emptyset$ dans K^n.
– Justifier l'exitence de $r+1$ polynômes $\{h_1,\ldots,h_r,q\}$ dans B, tels que
$$1 = \sum_{1\leq j\leq r} h_i f_i + q(gY-1).$$
On considère le morphisme d'anneaux unitaires
$$\phi : K[X_1,\ldots,X_n,Y] \longrightarrow K(X_1,\ldots,X_n),$$
où $K(X_1,\ldots,X_n)$ est le corps des fractions rationnelles à n indéterminées sur K, tel que

$$\phi_{/K} = id_K,\ \phi(X_i) = X_i, \forall i\,(1 \leq i \leq n) \text{ et } \phi(Y) = \frac{1}{g}.$$

Démontrer que $1 = \sum_{1\leq j\leq r} \phi(h_i) f_j$, où, pour tout $j\,(1 \leq j \leq r)$, $\phi(h_j)$ est de la forme $\frac{r_j}{g^{m_j}}$, avec $r_j \in K[X_1,\ldots,X_n]$ et $m_j \in \mathbb{N}^*$.
Trouver $m \in \mathbb{N}^*$ tel que $g^m \in I$. En déduire l'égalité (5.18).
3°) Prouver, en utilisant la relation (5.18), que pour tout idéal *propre* I de $K[X_1,\ldots,X_n]$, on a $V(I) \neq \emptyset$.
[Montrer que $V(I) = \emptyset$ conduit à une contradiction].

Chapitre 6
Polynômes et extensions cyclotomiques

Pour tout corps K, on note $\overline{K}$ une clôture algébrique de K.
Rappel de notation ([13]) : le *p.g.c.d.* de deux éléments non nuls a, b d'un D.I. est désigné par $a \wedge b$.

1. Notion de racine $n^{ème}$ primitive de l'unité

Définition 6.1. Etant donné un corps K et un entier $n \geq 1$, on appelle **racine $n^{ème}$ de l'unité** de K , tout $\alpha \in \overline{K}$ racine du polynôme $X^n - 1$ de $K[X]$.

Proposition 6.2. *Les notations étant celles de la* Déf. 6.1, *si* $car K = p > 0$ *et* $n = p^m$, $m \in \mathbb{N}^*$, *alors, dans* $\overline{K}$, 1 *est l'unique racine du polynôme* $X^n - 1$ *de* $K[X]$.

Démonstration. Les hypothèses $car K = p$ et $n = p^m$ impliquent, dans $K[X]$, ([13], Prop. 1.78)

$$X^n - 1 = X^{p^m} - 1 = (X-1)^{p^m},$$

donc 1 est l'unique racine du polynôme $X^{p^m} - 1$, à l'ordre de multiplicité p^m. □

Remarque 6.3. Si, dans la Déf. 6.1, on a $car K = p > 0$ et $p \mid n$, alors il existe $k \in \mathbb{N}^*$ tel que $n = kp^m, m \in \mathbb{N}^*$ et $p \nmid k$, d'où, dans $K[X]$,

$$X^n - 1 = X^{kp^m} - 1 = (X^k - 1)^{p^m}.$$

Compte tenu de la Prop. 6.2, l'équation $X^n - 1 = 0$ se ramène à
$X^k - 1 = 0$, avec $p \nmid k$.

En conséquence, dans toute la suite de ce chapitre, nous supposerons que, dans le contexte de la Déf. 6.1, le corps K et l'entier n satisfont à la condition :

$$car K = 0 \quad \text{ou} \quad car K = p > 0 \text{ et } p \nmid n. \tag{6.1}$$

Proposition 6.4. *Si un corps* K *et un entier* $n \geq 1$ *vérifient la condition* (6.1), *alors le polynôme* $X^n - 1$ *a* n *racines distinctes dans* $\overline{K}$.
L'ensemble U_n, *des* n *racines* $n^{èmes}$ *de l'unité de* K, *est un sous-groupe* cyclique *du groupe multiplicatif* $\overline{K}^* = \overline{K} \setminus \{0\}$.

Démonstration. La proposition est immédiate pour $n = 1$; supposons $n > 1$ et posons $q_n(X) := X^n - 1$; on a $q_n'(X) = nX^{n-1}$.
La condition (6.1) implique alors $q_n \wedge q_n' = 1$, donc le polynôme $q_n(X)$ n'a que des racines simples dans $\overline{K}$ (Rem. 3.22)

Soit U_n l'ensemble des n racines distinctes de $q_n(X)$ dans $\overline{K}$, on a $U_n \subset \overline{K}^*, 1 \in U_n$ et si α, β sont deux éléments de U_n, alors

$$\left((\alpha\beta^{-1})^n = \alpha^n\beta^{-n} = 1\right) \Longrightarrow \alpha\beta^{-1} \in U_n.$$

On en déduit que U_n est un sous-groupe fini d'ordre n du groupe multiplicatif $\overline{K}^*$; par suite le groupe U_n est *cyclique* (Cor. 4.4). □

Définition 6.5. Etant donné un corps K et un entier $n \geq 1$ vérifiant la condition (6.1), on appelle **racine $n^{ème}$ primitive de l'unité** de K, tout générateur du groupe cyclique U_n ([12], Ch. III).

Remarque 6.6. Dans les conditions de la Déf. 6.5, un élément ω de U_n est une racine $n^{ème}$ *primitive* de l'unité si et seulement si ω est un élément *d'ordre n* dans le groupe U_n ([12], p.36) ; c'est-à-dire, pour $n > 1$:

$$\omega^n = 1 \quad \text{et} \quad \forall k(1 \leq k < n), \omega^k \neq 1.$$

On rappelle que le nombre des générateurs d'un groupe cyclique d'ordre n est $\varphi(n)$, où φ est la fonction d'Euler ([12], p.99). Le calcul de $\varphi(n)$ ([12], p.105) donne $\varphi(1) = 1$ et pour

$$n = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k},$$

où les $p_i, 1 \leq i \leq k$, sont des nombres premiers deux à deux distincts et les m_i sont non nuls dans $\mathbb{N}$,

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k}). \tag{6.2}$$

Notations : Dans le contexte de la Déf. 6.5, l'ensemble des racines $n^{èmes}$ *primitives* de l'unité d'un corps K sera noté Ω_n. Compte tenu de la propriété rappelée dans la Rem. 6.6, on a

$$| \Omega_n | = \varphi(n)$$

et quel que soit $\omega \in \Omega_n$,

$$U_n = \{\omega^k \, ; \, 1 \leq k \leq n, \text{ dans } \mathbb{N}\}, \tag{6.3}$$

$$\Omega_n = \{\omega^k \in U_n \, ; \quad k \wedge n = 1\}. \tag{6.4}$$

Exemple 6.7. Si $K = \mathbb{Q}$, alors $\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ (Cf. Ch.5) et quel que soit l'entier $n > 1$,

$$U_n = \{\alpha_k := exp\frac{2k\pi i}{n}; \quad 1 \leq k \leq n\}, \tag{6.5}$$

$$\Omega_n = \{\alpha_k \in U_n \, ; \, k \wedge n = 1\}. \tag{6.6}$$

2. Extensions cyclotomiques - Polynômes cyclotomiques

Comme dans le paragraphe précédent, K désigne un corps et $n \geq 1$ un entier qui vérifient la condition (6.1).

Proposition 6.8. *Compte tenu des notations définies précédemment, pour tout $\omega \in \Omega_n$, le polynôme $Irr_K(\omega, X)$ est séparable et $K(\omega)$ est une extension de degré fini et normale sur K.*

Démonstration. La propriété est triviale pour $n = 1$, on suppose $n > 1$.
Quel que soit $\omega \in \Omega_n$, le polynôme $Irr_K(\omega, X)$ divise $X^n - 1$ dans $K[X]$, il est donc séparable sur K, d'après la Prop. 6.4.
On remarque que si ω et ω' sont deux racines $n^{èmes}$ *primitives* de l'unité dans $\overline{K}$, alors d'après la relation (6.3), on a

$$U_n = \{\omega^k \,;\, 1 \leq k \leq n\} = \{\omega'^k \,;\, 1 \leq k \leq n\},$$

ainsi $\omega \in K(\omega')$ et $\omega' \in K(\omega)$, d'où $K(\omega) = K(\omega')$.
L'extension $K(\omega) : K$ est donc indépendante du choix de ω dans Ω_n.
Pour tout ω dans Ω_n, $K(\omega)$ est un corps de rupture du polynôme $X^n - 1$; mais $U_n \subset K(\omega)$ entraîne que $K(\omega)$ est corps de décomposition de $X^n - 1$ sur K. On en déduit que $K(\omega)$ est une extension normale et de degré fini sur K (Th. 3.15). □

Remarque 6.9. La Prop. 6.8 montre que tout $\omega \in \Omega_n$ est séparable sur K ; on en déduira, au Ch. 7 (Cor. 7.18), que $K(\omega) : K$ est séparable.

Définition 6.10. Compte tenu des notations et des résultats ci-dessus,
1) Quel que soit $\omega \in \Omega_n$, l'extension $K(\omega) : K$ est appelée la $n^{ème}$ **extension cyclotomique** de K.
2) Le polynôme $\Phi_n(X) := \prod_{\omega \in \Omega_n} (X - \omega)$
est appelé le $n^{ème}$ **polynôme cyclotomique** sur K.

Remarque 6.11. Le polynôme $\Phi_n(X)$ est unitaire dans $\overline{K}[X]$ ou, plus précisément, dans $K(\omega)[X]$, où $\omega \in \Omega_n$. D'autre part,

$$|\Omega_n| = \varphi(n) \Longrightarrow deg\,\Phi_n = \varphi(n),$$

où φ est la fonction d'Euler.

Exemple 6.12. Supposons $K = \mathbb{Q}$ et déterminons les polynômes $\Phi_n(X)$ pour $1 \leq n \leq 4$, sachant que, pour $n > 1$, on a

$$\Omega_n = \{exp\frac{2k\pi i}{n} \,;\, 1 \leq k < n,\ k \wedge n = 1\}.$$
$$\Omega_1 = \{1\} \Longrightarrow \Phi_1(X) = X - 1.$$
$$\Omega_2 = \{-1\} \Longrightarrow \Phi_2(X) = X + 1.$$
$$\Omega_3 = \{j, j^2\} \Longrightarrow \Phi_3(X) = X^2 + X + 1.$$
$$\Omega_4 = \{i, -i\} \Longrightarrow \Phi_4(X) = X^2 + 1.$$

Pour $1 \leq n \leq 4$, on remarque que le $n^{ème}$ polynôme cyclotomique sur $\mathbb{Q}$ est unitaire dans $\mathbb{Z}[X]$. Cette propriété sera confirmée et généralisée par le Th. 6.14, dont la preuve utilisera le lemme suivant.

Lemme 6.13. *Soit A un anneau unitaire commutatif et $p(X)$ un polynôme non constant de $A[X]$, dont le coefficient directeur est inversible dans A ; alors, pour tout polynôme $f(X) \in A[X]$, il existe $q(X)$ et $r(X)$ dans $A[X]$ tels que*

$$f(X) = p(X)q(X) + r(X), \text{ avec } r(X) = 0 \text{ ou } deg\, r < deg\, p.$$

Démonstration. Soit $\big(p(X)\big)$ l'idéal de $A[X]$ engendré par $p(X)$ et

$$B := A[X]/(p(X)).$$

On note π la surjection canonique de $A[X]$ sur B ; on pose

$$\pi(X) := x \quad \text{et} \quad \text{pour tout } a \in A, \pi(a) := \overline{a}.$$

Le coefficient directeur de $p(X)$ étant inversible, on peut supposer que $p(X)$ est unitaire. En effet, si

$$p(X) = \sum_{0 \le i \le n} a_i X^i, \text{ avec } a_n \text{ inversible, on peut écrire}$$
$$p(X) = a_n p_1(X), \text{ où } p_1(X) \text{ est unitaire dans } A[X]; \text{ alors,}$$
$$\big(p(X)\big) = \big(p_1(X)\big) \Longrightarrow B = A[X]/(p_1(X)).$$

Nous supposons donc $p(X)$ unitaire. Pour tout $f(X) \in A[X]$, on pose

$$\pi(f(X)) = \overline{f(X)};$$
$$\text{ainsi,} \qquad f(X) = \sum_{0 \le i \le m} b_i X^i \Longrightarrow \overline{f(X)} = \sum_{0 \le i \le m} \overline{b}_i x^i.$$

En posant $\overline{A} := \pi(A)$, on peut identifier B à l'anneau de polynômes $\overline{A}[x]$ et dans B,

$$\overline{p(X)} = x^n + \sum_{0 \le i \le n-1} \overline{a}_i x^i = 0 \Longrightarrow x^n = -\sum_{0 \le i \le n-1} \overline{a}_i x^i;$$

par suite, pour tout élément $\overline{f(X)} \in B$, il existe $\overline{r(X)} \in B$ tel que

$$\overline{f(X)} = \overline{r(X)}, \text{ avec } deg\, \overline{r(X)} \le n-1.$$

On en conclut qu'il existe $r(X) \in A[X]$ tel que

$$f(X) \equiv r(X) \pmod{p(X)}, \text{ avec } r(X) = 0 \text{ ou } deg\, r \le n-1, \text{ donc,}$$
$$f(X) = p(X)q(X) + r(X), \text{ avec } r(X) = 0 \text{ ou } deg\, r \le n-1 < deg\, p. \qquad \square$$

Théorème 6.14. *Etant donné un corps K et un entier $n \ge 1$, satisfaisant à la condition* (6.1), *pour tout d divisant n dans $\mathbb{N}^*$, on a*

1) $\quad X^n - 1 = \prod_{d|n} \Phi_d(X).$

2) $\quad car\, K = 0 \Longrightarrow \Phi_n(X)$ *unitaire dans* $\mathbb{Z}[X]$.

$(car\, K = p > 0$ *et* $p \nmid n) \Longrightarrow \Phi_n(X)$ *unitaire dans* $\mathbb{F}_p[X]$, *où* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Démonstration. Sans restreindre la généralité des hypothèses, on peut supposer que, si $car\, K = 0$ (resp. car K = p > 0), le sous-corps premier de K est $\mathbb{Q}$ (resp. $\mathbb{F}_p$) ; alors, dans le premier cas, on a $X^n - 1 \in \mathbb{Z}[X]$ et dans le second cas, $X^n - 1 \in \mathbb{F}_p[X]$.

1) Le groupe U_n des racines $n^{èmes}$ de l'unité dans $\overline{K}$ étant cyclique d'ordre n (Prop. 6.4), pour tout diviseur d de n, dans $\mathbb{N}$, il existe exactement $\varphi(d)$ éléments d'ordre d dans U_n ([12], Ch. III), ce sont les racines $d^{èmes}$ primitives de l'unité dans $\overline{K}$, c'est-à-dire les éléments de Ω_d. On en déduit que

$$U_n = \bigcup_{d|n} \Omega_d. \tag{6.7}$$

Dans $\overline{K}[X]$, on a donc $\quad X^n - 1 = \prod_{\alpha \in U_n} (X - \alpha) = \prod_{d|n} \big(\prod_{\alpha \in \Omega_d} (X - \alpha) \big),$

d'où, d'après la définition de $\Phi_d(X)$ (Déf. 6.10),

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{6.8}$$

2) Pour $n = 1$, quelle que soit la caractéristique du corps K, on a $\Phi_1(X) = X - 1$, donc la propriété 2) du Th. 6.14 est vérifiée.
Pour $n > 1$, on raisonne par récurrence sur n. L'hypothèse de récurrence implique que pour tout diviseur d de n tel que $1 \leq d < n$, dans $\mathbb{N}^*$, $\Phi_d(X)$ est unitaire dans $\mathbb{Z}[X]$ si $carK = 0$ (resp. unitaire dans $\mathbb{F}_p[X]$ si $carK = p > 0$ et $p \nmid n$). Posons

$$\phi(X) = \prod_{d|n,\, d<n} \Phi_d(X).$$

Le polynôme $\phi(X)$ est unitaire dans $\mathbb{Z}[X]$ si $carK = 0$ (resp. unitaire dans $\mathbb{F}_p[X]$ si $carK = p > 0$ et $p \nmid n$). Compte tenu de la relation (6.8), dans $\overline{K}[X]$), on a

$$X^n - 1 = \phi(X)\Phi_n(X) \tag{6.9}$$

– Dans le cas où $carK = 0$, en appliquant le lemme 6.13, on obtient, dans $\mathbb{Z}[X]$,

$$X^n - 1 = \phi(X)q(X) + r(X), \text{ avec } r(X) = 0 \text{ ou } deg\, r < deg\, \phi. \tag{6.10}$$

– Dans le cas où $carK = p > 0, p \nmid n$, on obtient (6.10) en effectuant la division euclidienne de $X^n - 1$ par $\phi(X)$ dans $\mathbb{F}_p[X]$.
Les relations (6.9) et (6.10) impliquent, dans $\overline{K}[X]$),

$$\phi(X)\big(\Phi_n(X) - q(X)\big) = r(X). \tag{6.11}$$

Si $r(X) \neq 0$, alors le premier membre de l'égalité (6.11) est un polynôme de degré supérieur ou égal au degré de ϕ, tandis que le second membre est de degré strictement inférieur à celui de ϕ, d'où une contradiction.
On en déduit que $r(X) = 0$, par suite, $\Phi_n(X) = q(X)$. Ainsi la relation (6.9) est une égalité dans $\mathbb{Z}[X]$ (resp. dans $\mathbb{F}_p[X]$) et les polynômes $\phi(X)$, $X^n - 1$ étant unitaires, $\Phi_n(X)$ est unitaire. □

En vue du Th. 6.17, nous introduisons ici la fonction arithmétique de Möbius ; il s'agit, comme pour la fonction d'Euler, d'une fonction arithmétique classique ([28]).

Définition 6.15. On appelle **fonction de Möbius**, l'application

$$\begin{aligned} \mu : \mathbb{N}^* &\longrightarrow \mathbb{N}^* \\ d &\longmapsto \mu(d) \end{aligned}$$

telle que $\mu(1) = 1$

$\mu(d) = (-1)^k$, si d est produit de k nombres premiers distincts

$\mu(d) = 0$, si d est divisible par le carré d'un nombre premier.

Proposition 6.16. *Pour tout entier $n > 0$, on a*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & si\ n = 1 \\ 0, & si\ n > 1. \end{cases}$$

Démonstration. D'après la Déf. 6.15, la propriété énoncée est vraie pour $n = 1$. Pour $n > 1$, soit $p_1, p_2, \ldots, p_k$ les nombres premiers distincts divisant n, alors

$$\begin{aligned}\sum_{d|n}\mu(d) &= \mu(1) + \sum_{1\le i\le k}\mu(p_i) + \Big(\sum_{1\le i<j\le k}\mu(p_ip_j)\Big) + \cdots + \mu(p_1p_2\ldots p_k)\\ &= 1 + (-1)C_k^1 + (-1)^2C_k^2 + \cdots + (-1)^k\\ &= \big(1+(-1)\big)^k = 0.\end{aligned}$$

□

Théorème 6.17. *Etant donné un corps K et un entier $n > 0$ vérifiant la condition* (6.1)*, si $\Phi_n(X)$ est le $n^{ème}$ polynôme cyclotomique sur K, alors*

$$\Phi_n(X) = \prod_{d|n}(X^{\frac{n}{d}} - 1)^{\mu(d)}, \tag{6.12}$$

où μ est la fonction de Möbius.

Démonstration. Pour tout $n \in \mathbb{N}^*$, posons $h(n) := \Phi_n(X)$ et $H(n) := X^n - 1$.
D'autre part, pour d divisant n dans $\mathbb{N}^*$, posons $d' := \dfrac{n}{d}$.
A partir de la relation (6.8) et de la Prop. 6.16, on obtient

$$\prod_{d|n}(X^{d'} - 1)^{\mu(d)} = \prod_{d|n}\big(H(d')\big)^{\mu(d)} = \prod_{d|n}\Big(\prod_{c|d'}h(c)\Big)^{\mu(d)}.$$

Posons $\quad A = \{(d,c) \in \mathbb{N}^* \times \mathbb{N}^* \,;\, d \mid n \text{ et } c \mid d'\}.$

On a aussi $\quad A = \{(d,c) \in \mathbb{N}^* \times \mathbb{N}^* \,;\, c \mid n \text{ et } d \mid c'\}$, où $c' = \dfrac{n}{c}$,

d'où
$$\begin{aligned}\prod_{d|n}(X^{d'} - 1)^{\mu(d)} &= \prod_{(d,c)\in A}\big(h(c)\big)^{\mu(d)} = \prod_{c|n}\Big(\prod_{d|c'}h(c)\Big)^{\mu(d)}\\ &= \prod_{c|n}(h(c))^{\gamma}, \text{ où } \gamma = \sum_{d|c'}\mu(d) \quad \text{(Prop. 6.16)}\\ &= h(n) = \Phi_n(X).\end{aligned}$$

□

Exemple 6.18. Appliquons le Th. 6.17. pour trouver le polynôme cyclotomique $\Phi_8(X)$ sur $\mathbb{Q}$, sans utiliser les racines $8^{èmes}$ de l'unité dans $\mathbb{C}$. La relation (6.12) nous donne

$$\begin{aligned}\Phi_8(X) &= (X^8-1)^{\mu(1)}(X^4-1)^{\mu(2)}(X^2-1)^{\mu(4)}(X-1)^{\mu(8)}\\ &= (X^8-1)(X^4-1)^{-1}\\ &= X^4 + 1.\end{aligned}$$

3. Polynômes et extensions cyclotomiques sur $\mathbb{Q}$

Théorème 6.19. *Soit $n \in \mathbb{N}^*$ et $\Phi_n(X)$ le $n^{ème}$ polynôme cyclotomique sur $\mathbb{Q}$, alors, pour toute racine $n^{ème}$* primitive *de l'unité $\omega \in \overline{\mathbb{Q}}$, on a*

$$Irr_{\mathbb{Q}}(\omega, X) = \Phi_n(X), \quad \textit{donc} \quad [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n).$$

Démonstration. La propriété est vérifiée pour $n = 1$; on supposera $n > 1$.
Ω_n étant l'ensemble des racines $n^{èmes}$ *primitives* de l'unité dans $\overline{\mathbb{Q}}$, par définition on a

$$\Phi_n(X) = \prod_{\omega\in\Omega_n}(X - \omega).$$

D'après le Th. 6.14, $\Phi_n(X)$ est dans $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, par suite, pour tout $\omega \in \Omega_n$,

$$\Phi_n(\omega) = 0 \Longrightarrow Irr_{\mathbb{Q}}(\omega, X) \mid \Phi_n(X), \text{ dans } \mathbb{Q}[X]. \tag{6.13}$$

Posons $p_\omega(X) = Irr_{\mathbb{Q}}(\omega, X)$; il existe alors $q(X) \in \mathbb{Q}[X]$, tel que

$$\Phi_n(X) = p_\omega(X) q(X). \tag{6.14}$$

$\Phi_n(X)$ est unitaire dans $\mathbb{Z}[X]$ (Th. 6.14), $p_\omega(X)$ est unitaire dans $\mathbb{Q}[X]$, donc $q(X)$ est unitaire dans $\mathbb{Q}[X]$.
On rappelle alors ([13], Lemme 5.106) qu'il existe γ et δ dans $\mathbb{Q}^*$, tels que

$$p_\omega(X) = \gamma g(X), \quad q(X) = \delta h(X), \tag{6.15}$$

où $g(X)$ et $h(X)$ sont primitifs dans $\mathbb{Z}[X]$.
Notons a (resp. b) le coefficient directeur de $g(X)$ (resp. $h(X)$) ; les égalités (6.15) impliquent $1 = \gamma a$ et $1 = \delta b$. En tenant compte de la relation (6.14), on obtient

$$ab\Phi_n(X) = g(X)h(X), \quad \text{dans } \mathbb{Z}[X].$$

Dans $\mathbb{Z}[X]$, les polynômes g et h sont primitifs et $\Phi_n(X)$ est unitaire, on peut donc supposer $ab = 1$ et $a = 1, b = 1$, d'où $p_\omega(X) = g(X)$.
Par suite, le polynôme unitaire $p_\omega(X)$ est primitif dans $\mathbb{Z}[X]$ et irréductible dans $\mathbb{Q}[X]$; on en conclut ([13], Prop. 5.108) que

$p_\omega(X)$ est unitaire et irréductible dans $\mathbb{Z}[X]$.

Il reste à vérifier que pour $\omega' \neq \omega$ dans Ω_n, on a $p_{\omega'}(X) = p_\omega(X)$.
Il suffit de montrer que tout $\omega' \in \Omega_n$ est racine de $p_\omega(X)$. On sait que

$$\Omega_n = \{\omega^k \,;\, 1 \leq k < n \text{ et } k \wedge n = 1\}.$$

a) Supposons $\omega' = \omega^r$, $1 \leq r < n$, $r \nmid n$ et *r premier*. Posons

$$p_{\omega^r}(X) = Irr_{\mathbb{Q}}(\omega^r, X);$$

alors, $p_{\omega^r}(\omega^r) = 0 \Longrightarrow p_\omega(X)$ et $p_{\omega^r}(X^r)$ ont une racine commune ω.

Supposons $p_{\omega^r}(X) \wedge p_\omega(X) = 1$. Les polynômes $p_{\omega^r}(X)$ et $p_\omega(X)$ sont alors deux diviseurs unitaires et irréductibles de $X^n - 1$ dans $\mathbb{Z}[X]$, donc il existe $q(X) \in \mathbb{Z}[X]$ tel que

$$X^n - 1 = p_\omega(X) p_{\omega^r}(X) q(X). \tag{6.16}$$

Notons π la surjection canonique de $\mathbb{Z}$ sur le corps $\mathbb{Z}/r\mathbb{Z}$ et $\hat{\pi}$ le prolongement canonique de π, de $\mathbb{Z}[X]$ sur $(\mathbb{Z}/r\mathbb{Z})[X]$. Pour tout $f(X) \in \mathbb{Z}[X]$, on pose $\hat{\pi}(f(X)) = \overline{f}(X)$; en particulier,

$$\hat{\pi}(X^n - 1) = X^n - \overline{1}.$$

Le nombre premier r ne divise pas n, donc $X^n - \overline{1}$ n'a que des racines simples dans un corps de décomposition sur $\mathbb{Z}/r\mathbb{Z}$. D'autre part, la relation (6.16) entraîne

$$X^n - \overline{1} = \overline{p_\omega}(X)\overline{p_{\omega^r}}(X)\overline{q}(X), \quad \text{dans } (\mathbb{Z}/r\mathbb{Z})[X]. \tag{6.17}$$

Or $p_\omega(X)$ et $p_{\omega^r}(X^r)$ ont une racine commune, donc ils ne sont pas premiers entre eux et $p_\omega(X)$ étant irréductible dans $\mathbb{Z}[X]$, nécessairement

$$p_\omega(X) \mid p_{\omega^r}(X^r), \text{ dans } \mathbb{Z}[X].$$

Il existe donc $u(X) \in \mathbb{Z}[X]$, tel que $p_{\omega^r}(X^r) = p_\omega(X)u(X)$ et r étant premier,

$$\overline{p_\omega}(X)\overline{u}(X) = \overline{p_{\omega^r}}(X^r) = \left(\overline{p_{\omega^r}}(X)\right)^r, \text{ dans } (\mathbb{Z}/r\mathbb{Z})[X].$$

On en déduit que, dans l'anneau factoriel $(\mathbb{Z}/r\mathbb{Z})[X]$, les polynômes $\overline{p_\omega}(X)$ et $\overline{p_{\omega^r}}(X)$ ont au moins un diviseur *irréductible* commun, que nous noterons $\overline{v}(X)$. La relation (6.17) implique alors

$$\left(\overline{v}(X)\right)^2 \mid X^n - \overline{1}, \quad \text{dans } (\mathbb{Z}/r\mathbb{Z})[X].$$

Mais $\overline{v}(X)$ étant irréductible, on a $deg\,\overline{v}(X) \geq 1$, donc le polynôme $X^n - \overline{1}$ a au moins une racine double dans un corps de décomposition sur $\mathbb{Z}/r\mathbb{Z}$, ce qui est en contradiction avec l'hypothèse : $r \nmid n$ (Prop. 6.4). On en conclut que, dans $\mathbb{Z}[X]$, les polynômes irréductibles et unitaires $p_{\omega^r}(X)$ et $p_\omega(X)$ ne sont pas premiers entre eux, par suite,

$$p_{\omega^r}(X) = p_\omega(X). \tag{6.18}$$

b) Supposons $\omega' = \omega^s$, avec $1 < s < n, s \wedge n = 1$.
Soit $s = r_1 r_2 \dots r_k$ la factorisation de s, en nombres premiers, non nécessairementdistincts dans $\mathbb{N}$. A partir du résultat (6.18), on obtient :

$$p_\omega(X) = p_{\omega^{r_1}}(X) = p_{\omega^{r_1 r_2}}(X) = \cdots = p_{\omega^{r_1 \cdots r_k}}(X) = p_{\omega^s}(X).$$

Ainsi, quel que soit $\omega \in \Omega_n$, $p_\omega(X) = Irr_{\mathbb{Q}}(\omega, X)$ admet pour racines les $\varphi(n)$ racines $n^{èmes}$ *primitives* de l'unité contenues dans $\overline{\mathbb{Q}}$, donc

$$\Phi_n(X) \mid Irr_{\mathbb{Q}}(\omega, X), \text{ dans } \mathbb{Q}[X].$$

En tenant compte de la relation (6.13) et du fait que les deux polynômes considérés sont unitaires dans $\mathbb{Z}[X]$, on obtient, pour tout $\omega \in \Omega_n$,

$$\Phi_n(X) = Irr_{\mathbb{Q}}(\omega, X), \quad \text{d'où} \quad [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n). \qquad \square$$

4. Théorème de Wedderburn

Théorème 6.20. *Tout anneau à division (ou corps gauche)* fini *est un corps (commutatif).*

Démonstration. Il existe plusieurs démonstrations de ce théorème, celle que nous donnons ici est une application du Th. 6.14 (relation (6.8)).
a) Soit A un anneau à division (ou corps gauche) *fini* ([13], Déf. 1.6) ; le groupe multiplicatif fini $A^* = A \setminus \{0\}$ est alors *non abélien.*
Soit $Z(A)$ le centre de A ([13], Déf. 1.32) :

$$Z(A) = \{x \in A \,;\, ax = xa, \forall a \in A\}.$$

Le but de la démonstration est de prouver que $Z(A) = A$.

On remarque que $Z(A)$ est un sous-corps *commutatif* de A et, A étant fini, $Z(A)$ est un corps fini ; posons

$$q := |Z(A)|.$$

L'anneau à division fini A est un espace vectoriel sur $Z(A)$, nécessairement de dimension finie et

$$n := dim_{Z(A)}A \Longrightarrow |A| = q^n.$$

On est ramené à prouver que $n = 1$.

b) Supposons $n > 1$ et considérons le groupe A^* comme opérant sur lui-même par conjugaison ([12], p.177) :

$$A^* \times A^* \longrightarrow A^*$$
$$(a,x) \longmapsto axa^{-1}.$$

Soit $\{x_i\}_{1\leq i\leq r}$, $1 \leq r \leq q^n - 1$ dans $\mathbb{N}$, une famille de représentants des classes de conjugaison (distinctes) de A^*.
Pour tout $x \in A^*$, notons $C(x)$ le *centralisateur* de x dans A^* ([12], p.64) :

$$C(x) = \{a \in A^* \,;\, ax = xa\}.$$

$C(x)$ est un sous-groupe de A^* ([12], p.76) et, $[A^* : C(x)]$ désignant l'indice de $C(x)$ dans A^*, "*l'équation aux classes*" s'écrit ici ([12], Cor. 5.22) :

$$|A^*| = \sum_{1\leq i\leq r} [A^* : C(x_i)] = q^n - 1. \tag{6.19}$$

Soit $Z(A^*)$ le centre du groupe A^* ; on a

$$Z(A^*) = Z(A) \setminus \{0\} \Longrightarrow |Z(A^*)| = q - 1.$$
$$x \in Z(A^*) \Longrightarrow C(x) = A^* \Longrightarrow [A^* : C(x)] = 1.$$

Quitte à réordonner l'ensemble des $x_i\,(1 \leq i \leq r)$, on peut supposer

$$x_i \in Z(A^*), \forall i\,(1 \leq i \leq q-1) \quad \text{et} \quad x_i \notin Z(A^*),\ \forall i\,(q \leq i \leq r).$$

Par suite, la relation (6.19) permet d'écrire

$$q^n - 1 = q - 1 + \sum_{q\leq i\leq r} [A^* : C(x_i)]. \tag{6.20}$$

Pour tout $i\,(q \leq i \leq r)$, posons

$$D_i = \{a \in A \,;\, ax_i = x_i a\} = C(x_i) \cup \{0\}.$$

On vérifie que D_i est un sous-anneau de A, contenant $Z(A)$; ainsi D_i est un espace vectoriel de dimension finie sur le corps fini $Z(A)$; alors,

$$n_i := dim_{Z(A)} D_i \Longrightarrow |D_i| = q^{n_i} \Longrightarrow |C(x_i)| = q^{n_i} - 1.$$

$C(x_i)$ étant un sous-groupe de A^*, son ordre $q^{n_i} - 1$ divise $q^n - 1 = |A^*|$ ([12], Th. 2.9) et on obtient ([12], Prop. 2.15) :

$$[A^* : C(x_i)] = \frac{q^n - 1}{q^{n_i} - 1}.$$

La relation (6.20) s'écrit alors,

$$q^n - 1 = q - 1 + \sum_{q\leq i\leq r} \frac{q^n - 1}{q^{n_i} - 1} \tag{6.21}$$

Rappelons que, dans $\mathbb{N}$, ([13], App. A, Prop. A.37)

$$q^{n_i} - 1 \mid q^n - 1 \iff n_i \mid n.$$

D'autre part, d'après le lemme 4.7, on a

$$d \mid n, \text{ dans } \mathbb{N}^* \iff X^d - 1 \mid X^n - 1, \text{ dans } \mathbb{Q}[X].$$

Pour tout diviseur d de n, il existe donc $g_d(X) \in \mathbb{Q}[X]$, tel que

$$X^n - 1 = (X^d - 1)g_d(X). \tag{6.22}$$

Or, d'après le Th. 6.14, on a

$$X^d - 1 = \prod_{k|d} \Phi_k(X), \quad \text{de plus,} \quad k \mid d \Longrightarrow k \mid n, \tag{6.23}$$

$$\text{alors} \quad (6.8) \Longrightarrow X^n - 1 = (X^d - 1) \prod_{d'|n, d<d'\leq n} \Phi_{d'}(X). \tag{6.24}$$

Dans le domaine d'intégrité $\mathbb{Q}[X]$, les relations (6.22) et (6.24) impliquent

$$g_d(X) = \prod_{d'|n, d<d'\leq n} \Phi_{d'}(X) = \Big(\prod_{d'|n, d<d'<n} \Phi_{d'}(X)\Big)\Phi_n(X).$$

Par suite (Th. 6.14.), quel que soit le diviseur d de n, $g_d(X)$ est unitaire dans $\mathbb{Z}[X]$ et $\Phi_n(X)$ divise $g_d(X)$ dans $\mathbb{Z}[X]$.
On en déduit que, dans $\mathbb{Z}$, pour l'entier $q = |Z(A)| > 1$ et pour tout diviseur $d \geq 1$ de n,

$$(6.22) \Longrightarrow g_d(q) = \frac{q^n - 1}{q^d - 1} \Longrightarrow \Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}. \tag{6.25}$$

En appliquant la relation (6.25) aux diviseurs n_i de n intervenant dans la relation (6.21), on obtient :

$$(\forall i (q \leq i \leq r),\ \Phi_n(q) \mid \frac{q^n - 1}{q^{n_i} - 1}) \Longrightarrow \Phi_n(q) \mid \sum_{q\leq i\leq r} \frac{q^n - 1}{q^{n_i} - 1}.$$

$$\text{D'autre part,} \quad (6.8) \Longrightarrow \Phi_n(q) \mid q^n - 1,$$

$$\text{alors} \quad (6.21) \Longrightarrow \Phi_n(q) \mid q - 1.$$

Or, $\Phi_n(q) = \prod_{\omega\in\Omega_n} (q - \omega)$, où $\omega = exp\frac{2k\pi i}{n}$, $1 \leq k < n$, $k \wedge n = 1$; si pour tout $\omega \in \Omega_n$, on note $|q - \omega|$ le module du nombre complexe $q - \omega$, alors,

$$\omega \neq 1 \longrightarrow |q - \omega| > q - 1, \quad \text{d'où,} \quad |\Phi_n(q)| > q - 1, \text{ dans } \mathbb{Z};$$

par suite, pour $n > 1$, l'entier $\Phi_n(q)$ ne peut diviser $q - 1$.
On en conclut que $n = 1$, donc $A = Z(A)$, ainsi l'anneau à division fini A est un corps (commutatif). □

5. Polynômes cyclotomiques sur un corps fini

Remarque 6.21. a) Les résultats du chapitre 4 montrent que *tout corps fini de caractéristique p est une extension cyclotomique du corps* $\mathbb{F}_p$.
En effet, $\mathbb{F}_q$ étant un corps fini de caractéristique p et de cardinal $q = p^m, m \in \mathbb{N}^*$, on a (Rem. 4.14),

$$\mathbb{F}_q = \mathbb{F}_p(\omega), \tag{6.26}$$

où ω est un *générateur* du groupe cyclique $\mathbb{F}_q^*$, donc une racine $(q-1)^{ème}$ *primitive* de l'unité de $\mathbb{F}_p$, ainsi $\mathbb{F}_q$ est la $(q-1)^{ème}$ extension cyclotomique de $\mathbb{F}_p$.
Plus généralement, étant donné le corps fini $\mathbb{F}_{p^m}$, pour tout diviseur s de m, $\mathbb{F}_{p^m}$ est une extension cyclotomique du sous-corps $\mathbb{F}_{p^s}$ (Cf. Rem. 4.14).
b) Compte tenu de la relation (6.26),

$$q = p^m \iff [\mathbb{F}_q : \mathbb{F}_p] = m = [\mathbb{F}_p(\omega) : \mathbb{F}_p],$$

donc le degré du polynôme $Irr_{\mathbb{F}_p}(\omega, X)$ est m.
– Dans les *cas particuliers* suivants,

$$p = 2 \text{ et } m = 1 \text{ ou } 2, \quad \text{ou bien,} \quad p = 3 \text{ et } m = 1, \tag{6.27}$$

on vérifie que $m = \varphi(p^m - 1)$; on en déduit que dans $\mathbb{F}_p[X]$,

$$Irr_{\mathbb{F}_p}(\omega, X) = \Phi_{q-1}(X), \text{ où } q = p^m.$$

– Mais *en général* (c'est-à-dire, sauf dans les cas particuliers précédents), on a (voir, par exemple, le cas $p = 3, m = 2$) :

$$1 \leq m < \varphi(p^m - 1), \quad \text{donc} \quad deg\, Irr_{\mathbb{F}_p}(\omega, X) < deg\, \Phi_{q-1}(X), \text{ où } q = p^m.$$

Si Ω_{q-1} est l'ensemble des racines $(q-1)^{èmes}$ *primitives* de l'unité de $\mathbb{F}_p$, alors dans $\mathbb{F}_p[X]$, on a, pour tout $\omega \in \Omega_{q-1}$, :

$$Irr_{\mathbb{F}_p}(\omega, X) \mid \Phi_{q-1}(X) \quad \text{et} \quad Irr_{\mathbb{F}_p}(\omega, X) \neq \Phi_{q-1}(X). \tag{6.28}$$

On en déduit que le polynôme $\Phi_{q-1}(X)$, où $q = p^m$, n'est pas nécessairement irréductible sur $\mathbb{F}_p$; cette propriété sera confirmée par l'étude qui suit.

A. Notion de $n^{ème}$ polynôme primitif sur $\mathbb{F}_p$

Soit p un nombre premier et $n > 1$, un entier tel que $p \nmid n$, auxquels on associe U_n et Ω_n définis par les relations (6.3) et (6.4), dans $\overline{\mathbb{F}_p}$.

1/ Pour tout $\omega \in \Omega_n$, posons $p_\omega(X) := Irr_{\mathbb{F}_p}(\omega, X)$.
La $n^{ème}$ extension cyclotomique $\mathbb{F}_p(\omega) : \mathbb{F}_p$ est indépendante du choix de ω dans Ω_n et de degré fini (Prop. 6.8.) ; alors,

$$(deg\, p_\omega(X) = m, \forall \omega \in \Omega_n) \iff ([\mathbb{F}_p(\omega) : \mathbb{F}_p] = m, \forall \omega \in \Omega_n), \tag{6.29}$$

$$\iff (\mathbb{F}_p(\omega) = \mathbb{F}_{p^m}, \forall \omega \in \Omega_n). \tag{6.30}$$

Définition 6.22. Dans le contexte ci-dessus, on appellera, $n^{ème}$ **polynôme primitif** sur $\mathbb{F}_p$, tout polynôme $p_\omega(X) = Irr_{\mathbb{F}_p}(\omega, X)$, où $\omega \in \Omega_n$.

Remarque 6.23. Par définition, tout $\omega \in \Omega_n$ engendre le groupe cyclique U_n d'ordre n, formé par les racines du polynôme $X^n - 1 \in \mathbb{F}_p[X]$. Par suite, dans les conditions (6.29), (6.30), U_n est un sous-groupe du groupe cyclique $\mathbb{F}_{p^m}^*$ d'ordre $p^m - 1$, d'où

$$n \mid p^m - 1 \quad \text{et} \quad n \neq p^m - 1 \Longrightarrow U_n \subsetneq \mathbb{F}_{p^m}^*.$$

Dans le cas où $n \neq p^m - 1$, aucun élément $\omega \in \Omega_n$ n'engendre le groupe $\mathbb{F}_{p^m}^*$, cependant, pour tout $\omega \in \Omega_n$, on a $\mathbb{F}_{p^m} = \mathbb{F}_p(\omega)$ (Cf. Rem. 4.14), donc ω est un *élément primitif* (Déf. 3.32) pour l'extension $\mathbb{F}_{p^m} : \mathbb{F}_p$.

2/ Le $n^{ème}$ polynôme cyclotomique sur $\mathbb{F}_p$, $\Phi_n(X)$, est unitaire dans $\mathbb{F}_p[X]$ (Th. 6.14.) et il découle de sa définition (Déf. 6.10), que, quel que soit le polynôme $p(X)$, unitaire et irréductible dans $\mathbb{F}_p[X]$, on a

$$p(X) \mid \Phi_n(X) \iff \exists\, \omega \in \Omega_n, \text{ tel que } p(X) = p_\omega(X). \tag{6.31}$$

Proposition 6.24. *Le $n^{ème}$ polynôme* cyclotomique *sur $\mathbb{F}_p$, $\Phi_n(X)$, est le produit des $n^{èmes}$ polynômes* primitifs *sur $\mathbb{F}_p$ distincts et*

$$(deg\, p_\omega(X) = m, \forall\, \omega \in \Omega_n) \Longrightarrow m \mid \varphi(n).$$

Démonstration. D'après sa définition, le polynôme $\Phi_n(X)$ n'a que des racines simples dans $\overline{\mathbb{F}_p}$, donc dans l'anneau factoriel $\mathbb{F}_p[X]$, on peut écrire

$$\Phi_n(X) = p_1(X)p_2(X)\dots p_k(X), \quad \text{où} \quad 1 \le k \le \varphi(n) \tag{6.32}$$

et les polynômes $p_i(X)$, $1 \le i \le k$, sont unitaires, irréductibles, deux à deux distincts et séparables (Déf. 3.16). Compte tenu de (6.31),

$$\forall i (1 \le i \le k),\ \exists\, \omega_i \in \Omega_n \text{ tel que } p_i(X) = p_{\omega_i}(X);$$
$$\text{alors,} \quad (deg\, p_{\omega_i}(X) = m, \forall i (1 \le i \le k)) \Longrightarrow km = deg\, \Phi_n(X) = \varphi(n). \qquad \square$$

3/ Calcul de $m = [\mathbb{F}_p(\omega) : \mathbb{F}_p]$, où $\omega \in \Omega_n$.

Remarque 6.25. D'après les résultats obtenus précédemment,

$$(\omega \in \Omega_n \quad \text{et} \quad m = [\mathbb{F}_p(\omega) : \mathbb{F}_p]) \Longrightarrow n \mid p^m - 1, \quad \text{dans } \mathbb{N}^*. \tag{6.33}$$
$$\text{D'autre part,} \qquad n \mid p^m - 1 \iff p^m \equiv 1 \pmod{n}. \tag{6.34}$$

Considérons alors l'anneau $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

$$(p \nmid n \text{ et } p \text{ premier}) \Longrightarrow p \wedge n = 1,$$

par suite, $\overline{p}$ est un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$, donc un élément du groupe multiplicatif G_n, formé par les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. On rappelle que le groupe G_n est d'ordre $\varphi(n)$.

De plus, $m = deg\, p_\omega(X) = [\mathbb{F}_p(\omega) : \mathbb{F}_p]$ entraîne que m est, dans $\mathbb{N}^*$, *le plus petit entier* tel que $p^m \equiv 1 \pmod{n}$; en notant $o(\overline{p})$ l'ordre de $\overline{p}$ dans le groupe multiplicatif G_n, on en déduit que

$$m = [\mathbb{F}_p(\omega) : \mathbb{F}_p] \iff o(\overline{p}) = m, \text{ dans } G_n. \tag{6.35}$$

Cas particuliers :

1) On rappelle que, dès le début de ce paragraphe, on a supposé $n > 1$ car, $n = 1 \Longrightarrow m = 1$, quel que soit le nombre premier p.

2) $p \equiv 1 \pmod{n} \Longrightarrow m = 1$.

En particulier, $(n = 2$ et p impair$) \Longrightarrow p \equiv 1 \pmod{2} \Longrightarrow m = 1$.

Proposition 6.26. *Soit $n > 2$ dans $\mathbb{N}$ et p un nombre premier tel que $p \nmid n$ et $p \not\equiv 1 \pmod{n}$. Si la factorisation de n dans $\mathbb{N}^*$ est*

$$n = 2^\alpha q_1^{\alpha_1} \dots q_k^{\alpha_k}, \tag{6.36}$$

où l'on suppose $\alpha \ge 0, k \ge 0$ et pour $k > 0$, les q_i, $1 \le i \le k$, sont des nombres premiers impairs deux à deux distincts et les α_i sont non nuls, on obtient les résultats suivants, pour

le degré m de la $n^{ème}$ extension cyclotomique sur $\mathbb{F}_p$:

$$(k=0\,;\alpha=2) \Longrightarrow m=2; \tag{6.37}$$

$$(k=0\,;\,2<\alpha) \Longrightarrow m=2^{\alpha-2}; \tag{6.38}$$

$$(1\leq k\,;\,0\leq\alpha<2) \Longrightarrow m=p.p.c.m.\,(o(\overline{p}_{(i)})\,;\,1\leq i\leq k); \tag{6.39}$$

$$(1\leq k\,;\,\alpha=2) \Longrightarrow m=p.p.c.m.\,(2,o(\overline{p}_{(i)})\,;\,1\leq i\leq k); \tag{6.40}$$

$$(1\leq k\,;\,2<\alpha) \Longrightarrow m=p.p.c.m.\,(2^{\alpha-2},o(\overline{p}_{(i)})\,;\,1\leq i\leq k), \tag{6.41}$$

où $\overline{p}_{(i)}$ désigne la classe d'équivalence de p modulo $q_i^{\alpha_i}$ et $o(\overline{p}_{(i)})$ est l'ordre de $\overline{p}_{(i)}$ dans le groupe multiplicatif $G_{q_i^{\alpha_i}}$.

Démonstration. Compte tenu de la relation (6.35), les résultats énoncés découlent de la structure du groupe G_n (Cf. Ex.**1.**, de ce chapitre).
L'hypothèse $n>2$ entraîne que pour $k=0$, on a $\alpha\geq 2$.
L'hypothèse $p\not\equiv 1 \pmod{n}$ implique $\overline{p}\neq\overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$; on écarte ainsi les cas où $m=1$.

Examen des différents cas (le détail des preuves est laissé au lecteur, en application de l'Ex. **1.** de ce chapitre) :

$$(k=0,\ \alpha=2) \Longrightarrow n=4, \text{ alors } \quad G_4\simeq\mathbb{Z}/2\mathbb{Z} \Longrightarrow m=o(\overline{p})=2.$$

$$(k=0,\ 2<\alpha) \Longrightarrow G_n\simeq(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$$
$$\Longrightarrow m=p.p.c.m.\,(2,2^{\alpha-2})=2^{\alpha-2}.$$

$$(1\leq k,\ \alpha=0) \Longrightarrow G_n\simeq G_{q_1^{\alpha_1}}\times\cdots\times G_{q_k^{\alpha^k}}$$
$$\Longrightarrow m=p.p.c.m.\,\big(o(\overline{p}_{(i)})\,;\,1\leq i\leq k\big).$$

$$(1\leq k,\ \alpha=1) \Longrightarrow G_n\simeq G_2\times G_{q_1^{\alpha_1}}\times\cdots\times G_{q_k^{\alpha^k}}$$
$$\Longrightarrow m=p.p.c.m.\,\big(o(\overline{p}_{(i)})\,;\,1\leq i\leq k\big).$$

$$(1\leq k,\ \alpha=2) \Longrightarrow G_n\simeq G_4\times G_{q_1^{\alpha_1}}\times\cdots\times G_{q_k^{\alpha^k}}$$
$$\Longrightarrow m=p.p.c.m.\,\big(2,o(\overline{p}_{(i)})\,;\,1\leq i\leq k\big).$$

$$(1\leq k,\ 2<\alpha) \Longrightarrow G_n\simeq G_{2^\alpha}\times G_{q_1^{\alpha_1}}\times\cdots\times G_{q_k^{\alpha^k}}$$
$$\Longrightarrow m=p.p.c.m.\,\big(2^{\alpha-2},o(\overline{p}_{(i)})\,;\,1\leq i\leq k\big).$$ □

Exemple 6.27. 1) $n=2^5=32, p=7$. Soit $\overline{7}$ la classe d'équivalence de 7 modulo 2^5 ; dans le groupe G_{2^5}, d'ordre $\varphi(2^5)=2^4=16$, on a, d'après le résultat (6.38),

$$m=o(\overline{7})=2^3=8.$$

On en conclut que la $32^{ème}$ extension cyclotomique sur $\mathbb{F}_7$ est $\mathbb{F}_{7^8}$; tout $32^{ème}$ polynôme *primitif* sur $\mathbb{F}_7$ est de degré 8 ; alors le $32^{ème}$ polynôme *cyclotomique* sur $\mathbb{F}_7$, qui est de degré $\varphi(32)=16$, est le produit de deux polynômes unitaires, irréductibles, de degré 8. (Prop. 6.24.).

2) $n=3^3=27, p=19$. Le groupe G_{3^3} est d'ordre $\varphi(3^3)=2\times 3^2=18$ et cyclique (Ex. **1.**, Ch. 6).
Pour tout $x\in\mathbb{Z}$, soit $\bar{x}$ la classe de x modulo 3^3. Le résultat (6.39) donne

$$m = o(\overline{19}) \text{ dans le groupe } G_{3^3}.$$
$$19^2 = 361 \Longrightarrow \overline{19}^2 = \overline{10} \Longrightarrow \overline{19}^3 = \overline{190} = \overline{1},$$
d'où $m = o(\overline{19}) = 3$.
En conclusion : la $27^{ème}$ extension cyclotomique sur $\mathbb{F}_{19}$ est $\mathbb{F}_{19^3}$; les $27^{èmes}$ polynômes *primitifs* sur $\mathbb{F}_7$ sont de degré 3 ; alors le $27^{ème}$ polynôme *cyclotomique* sur $\mathbb{F}_{19}$, qui est de degré 18, est le produit de six polynômes unitaires, irréductibles, de degré 3.

3) $n = 3 \times 5^2 = 75$, $p = 2$. Le groupe G_n est cyclique et d'ordre
$$\varphi(n) = \varphi(3)\,\varphi(5^2) = 2 \times (4 \times 5) = 40.$$
Notons, respectivement, $\bar{2}$, $\dot{2}$, et $\ddot{2}$ les classes d'équivalence de 2 modulo 75, modulo 3 et modulo 5^2 ; alors d'après la Prop. 6.26., relation (6.39),
$$m = o(\bar{2}) = p.p.c.m.\big(o(\dot{2}), o(\ddot{2})\big),$$
où $o(\bar{2})$, $o(\dot{2})$ et $o(\ddot{2})$ sont les ordres de $\bar{2}$, $\dot{2}$ et $\ddot{2}$, respectivement, dans les grou-pes G_{75}, G_3 et G_{5^2}.
Dans le groupe G_3 d'ordre 2, on a $o(\dot{2}) = 2$ et on vérifie que $\ddot{2}$ engendre le groupe cyclique G_{5^2}, d'ordre 20, d'où
$$m = p.p.c.m.(2, 20) = 20.$$
Ainsi la $75^{ème}$ extension cyclotomique sur $\mathbb{F}_2$ est $\mathbb{F}_{2^{20}}$; le degré d'un $75^{ème}$ polynôme *primitif* sur $\mathbb{F}_2$ est égal à 20, donc le $75^{ème}$ polynôme *cyclotomique* sur $\mathbb{F}_2$, qui est de degré 40, est le produit de deux polynômes unitaires, irréductibles, de degré 20.

4) $n = 2^3 \times 5 = 40$, $p = 7$. L'ordre du groupe G_{40} est
$$\varphi(2^3 \times 5) = 2^2 \times 4 = 16.$$
D'après la Prop. 6.26, relation (6.40),
$$m = p.p.c.m.\big(2, o(\dot{7})\big),$$
où $\dot{7}$ est la classe d'équivalence de 7 modulo 5 et $o(\dot{7})$ est l'ordre de $\dot{7} = \dot{2}$ dans le groupe G_5. Or, $\dot{2}$ est d'ordre 4 dans G_5, d'où $m = 4$.
La $40^{ème}$ extension cyclotomique sur $\mathbb{F}_7$ est donc $\mathbb{F}_{7^4}$; tout $40^{ème}$ polynôme *primitif* sur $\mathbb{F}_7$ est de degré 4 et le $40^{ème}$ polynôme *cyclotomique* sur $\mathbb{F}_7$, qui est de degré 16, est le produit de quatre polynômes unitaires, irréductibles, de degré 4.

B. Factorisation dans $\mathbb{F}_p[X]$ - Algorithme de Berlekamp

Ce paragraphe est motivé par la recherche d'une méthode de détermination (pour tout entier $n > 1$) des facteurs irréductibles du $n^{ème}$ polynôme *cyclotomique* sur $\mathbb{F}_p$, c'est-à-dire, des $n^{èmes}$ polynômes *primitifs* sur $\mathbb{F}_p$ (Prop. 6.24)

1/ Propriétés préliminaires

Lemme 6.28. *Etant donné un anneau factoriel A et un entier $k > 1$, on considère, dans A, des éléments non nuls $a_1, a_2, \ldots, a_k$*, deux à deux premiers entre eux *et un élément $b \neq 0$ tel que*
$$b \quad \textit{divise} \quad \prod_{1 \leq i \leq k} a_i \quad \textit{et} \quad \forall i (1 \leq i \leq k),\ b \nmid a_i.$$
Pour tout $i (1 \leq i \leq k)$, on pose $d_i = b \wedge a_i$, alors
1) *Pour tout couple (i, j), $1 \leq i < j \leq k$, on a $d_i \wedge d_j = 1$.*
2) *Il existe une unité $u \in A$ telle que $b = u \prod_{1 \leq i \leq k} d_i$.*

Démonstration. On remarque que, pour tout $i(\leq i \leq k)$, $b \nmid a_i$ entraîne $d_i \neq b$.
1) Soit (i,j), $1 \leq i < j \leq k$, posons $\delta = d_i \wedge d_j$; alors

$$(\delta \mid d_i \quad \text{et} \quad d_i = b \wedge a_i) \Longrightarrow \delta \mid a_i.$$

De même, on a $\delta \mid a_j$; par suite, $a_i \wedge a_j = 1 \Longrightarrow d_i \wedge d_j = 1$.

2) Quel que soit $i(1 \leq i \leq k)$, on a $d_i \mid b$; alors,

$$\left(d_i \wedge d_j = 1, \forall (i,j), i \neq j\right) \Longrightarrow \prod_{1 \leq i \leq k} d_i \mid b,$$

donc il existe $u \in A^*$ tel que $b = u \prod_{1 \leq i \leq k} d_i$.
Démontrons que u est une unité dans A.
Quel que soit $i(1 \leq i \leq k)$, $d_i = b \wedge a_i$ implique qu'il existe α_i, β_i, dans A^*, tels que ([13], Prop. 5.43)

$$a_i = \alpha_i d_i, \quad b = \beta_i d_i \quad \text{et} \quad \alpha_i \wedge \beta_i = 1. \tag{6.42}$$

Posons $\alpha = \prod_{1 \leq i \leq k} \alpha_i$; des égalités (6.42) et de l'intégrité de l'anneau factoriel A on déduit que

$$\left(b = u \prod_{1 \leq i \leq k} d_i, \prod_{1 \leq i \leq k} a_i = \alpha \prod_{1 \leq i \leq k} d_i \quad \text{et} \quad b \mid \prod_{1 \leq i \leq k} a_i\right) \Longrightarrow u \mid \alpha. \tag{6.43}$$

$$\text{De plus, } \forall i (1 \leq i \leq k)\left(b = u \prod_{1 \leq j \leq k} d_j = \beta_i d_i\right) \Longrightarrow \beta_i = u \prod_{j \neq i} d_j.$$

D'après (6.42), $\forall i (1 \leq i \leq k)$, $\alpha_i \wedge \beta_i = 1$, d'où

$$\forall i (1 \leq i \leq k), \quad \left(\alpha_i \wedge u \prod_{j \neq i} d_j = 1 \Longrightarrow \alpha_i \wedge u = 1\right). \tag{6.44}$$

Dans l'anneau factoriel A, (6.44) implique $\alpha \wedge u = 1$ et avec le résultat (6.43), on obtient

$$(u \mid \alpha \text{ et } u \wedge \alpha = 1) \Longrightarrow u \in U_A,$$

U_A étant le groupe des unités de A. □

Proposition 6.29. *Soit $\mathbb{F}_q$ un corps fini de cardinal q et de caractéristique p.*
1) *Pour tout polynôme $g(X) \in \mathbb{F}_q[X]$, on a*

$$\left(g(X)\right)^q - g(X) = \prod_{\alpha \in \mathbb{F}_q} (g(X) - \alpha)$$

$$\text{et } (\deg g > 0,\ \alpha \neq \alpha' \text{ dans } \mathbb{F}_q) \Longrightarrow (g(X) - \alpha) \wedge (g(X) - \alpha') = 1.$$

2) *Etant donné $g(X) \in \mathbb{F}_q[X] \setminus \mathbb{F}_q$, si $f(X)$ est un polynôme non constant,* unitaire *de $\mathbb{F}_q[X]$, divisant $\left(g(X)\right)^q - g(X)$ et ne divisant aucun des $g(X) - \alpha$, $\alpha \in \mathbb{F}_q$, alors, en posant*

$$\forall \alpha \in \mathbb{F}_q,\ d_\alpha(X) := f(X) \wedge (g(X) - \alpha)$$

et en prenant $d_\alpha(X)$ unitaire, on obtient

$$f(X) = \prod_{\alpha \in \mathbb{F}_q} d_\alpha(X). \tag{6.45}$$

Démonstration. 1) Posons $Y := g(X)$, et considérons $Y^q - Y$ dans $\mathbb{F}_q[Y]$.
Tout $\alpha \in \mathbb{F}_q$ vérifie $\alpha^q - \alpha = 0$, donc est racine du polynôme $Y^q - Y$, par suite

$$Y^q - Y = \prod_{\alpha \in \mathbb{F}_q} (Y - \alpha) \Longrightarrow \left(g(X)\right)^q - g(X) = \prod_{\alpha \in \mathbb{F}_q} (g(X) - \alpha).$$

Supposons que $g(X)-\alpha$ et $g(X)-\alpha'$ aient un diviseur commun $r(X)\in\mathbb{F}_q[X]\setminus\mathbb{F}_q$. Soit $\beta\in\overline{\mathbb{F}_q}$, une racine du polynôme $r(X)$; alors

$$\big(g(\beta)-\alpha=0 \text{ et } g(\beta)-\alpha'=0\big)\Longrightarrow \alpha=\alpha',$$

ce qui est contraire à l'hypothèse $\alpha\neq\alpha'$, donc

$$(g(X)-\alpha)\wedge(g(X)-\alpha')=1.$$

2) Compte tenu des hypothèses, appliquons le Lem. 6.28., dans l'anneau factoriel $\mathbb{F}_q[X]$; on obtient

$$f(X)=u\prod_{\alpha\in\mathbb{F}_q} d_\alpha(X),\ u\in\mathbb{F}_q^*.$$

Mais $f(X)$ étant unitaire, ainsi que les $d_\alpha(X)$, on a $u=1$, donc

$$f(X)=\prod_{\alpha\in\mathbb{F}_q} d_\alpha(X). \qquad \square$$

2/ Polynômes $f(X)$-réducteurs

Les résultats de ce paragraphe découlent de la Prop. 6.29 et du Théorème Chinois (encore appelé Théorème des restes chinois) que nous rappelons ici ([13], Ch. 2).

Théorème Chinois
Etant donné un domaine principal A ([13], Déf. 2.7) *et $k\in\mathbb{N}^*$, si $p_1,p_2,\dots,p_k$ sont des éléments* non nuls et deux à deux premiers entre eux *dans A, alors, quel que soit le k-*uple $(c_1,c_2,\dots,c_k)\in A^k$, *il existe $a\in A$ tel que*

$$\forall i(1\leq i\leq k),\quad a\equiv c_i \pmod{p_i}.$$

De plus, si $b\in A$ vérifie la même propriété que a, alors

$$b\equiv a \pmod{\prod_{1\leq i\leq k} p_i}.$$

Dans ce qui suit, on se limite à étudier la factorisation, dans $\mathbb{F}_q[X]$, d'un polynôme $f(X)$ tel que

$$f(X)=p_1(X)p_2(X)\dots p_k(X),\quad k\in\mathbb{N}^*, \tag{6.46}$$

où les $p_i(X)$, $1\leq i\leq k$, sont *irréductibles, unitaires, et deux à deux distincts* dans $\mathbb{F}_q[X]$, le problème étant de trouver une méthode de détermination des $p_i(X)$, connaissant $f(X)$.

Proposition 6.30. *Etant donné $f(X)\in\mathbb{F}_q[X]$ satisfaisant à la condition* (6.46) *et un k-uple $(\alpha_1,\alpha_2,\dots,\alpha_k)$ d'éléments de $\mathbb{F}_q$, alors il existe $g(X)\in\mathbb{F}_q[X]$ tel que*

$$\forall i(1\leq i\leq k),\quad g(X)\equiv\alpha_i \pmod{p_i(X)}; \tag{6.47}$$

$$\textit{ce qui entraîne}\qquad \big(g(X)\big)^q\equiv g(X) \pmod{f(X)}. \tag{6.48}$$

Démonstration. Etant donné un k-uple $(\alpha_1,\alpha_2,\dots,\alpha_k)$ d'éléments de $\mathbb{F}_q\subset\mathbb{F}_q[X]$, d'après le Théorème Chinois, appliqué dans le domaine principal $\mathbb{F}_q[X]$, il existe $g(X)\in\mathbb{F}_q[X]$ tel que

$$\begin{aligned}
&\forall i(1\leq i\leq k),\ g(X)\equiv\alpha_i \pmod{p_i(X)};\\
&\text{par suite}\quad \big(g(X)\big)^q\equiv\alpha_i^q \pmod{p_i(X)},\\
\text{et}\quad &\alpha_i\in\mathbb{F}_q\Longrightarrow\alpha_i^q=\alpha_i\Longrightarrow\big(g(X)\big)^q\equiv\alpha_i \pmod{p_i(X)}.
\end{aligned}$$

La seconde partie du Théorème Chinois et l'hypothèse (6.46) entraînent

$$(g(X))^q \equiv g(X) \pmod{\prod_{1\le i\le k} p_i(X)};$$

$$\text{donc} \quad (6.46) \text{ et } (6.47) \Longrightarrow (g(X))^q \equiv g(X) \pmod{f(X)}. \qquad \square$$

Remarque 6.31. Dans le contexte de la Prop. 6.30,
a) on note qu'un polynôme *constant*, α, satisfait à (6.47) si et seulement si le k-uple donné $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ est tel que

$$\forall i (1 \le i \le k),\ \alpha_i = \alpha.$$

b) pour un polynôme $g(X)$ de $\mathbb{F}_q[X] \setminus \mathbb{F}_q$, on a $(g(X))^q = g(X^q)$,
car q est une puissance de la caractéristique p du corps $\mathbb{F}_q$; par suite

$$(g(X))^q \equiv g(X) \pmod{f(X)} \iff g(X^q) \equiv g(X) \pmod{f(X)}.$$

Proposition 6.32. *Soit $f(X) \in \mathbb{F}_q[X]$ vérifiant* (6.46).
1) *Etant donné un k-uple $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{F}_q^k$, parmi les polynômes de $\mathbb{F}_q[X]$ qui vérifient* (6.47), *il existe un* unique *polynôme $h(X)$ tel que*

$$\deg h < \deg f.$$

2) *Si $h(X) \in \mathbb{F}_q[X]$ satisfait aux conditions*

$$(h(X))^q \equiv h(X) \pmod{f(X)} \quad \text{et} \quad \deg h < \deg f, \tag{6.49}$$

alors il existe un unique *k-uple, $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{F}_q^k$ tel que*

$$\forall i (1 \le i \le k),\ h(X) \equiv \alpha_i \pmod{p_i(X)}.$$

3) *Il existe exactement q^k polynômes de $\mathbb{F}_q[X]$ vérifiant* (6.49).

Démonstration. 1) Soit $g(X) \in \mathbb{F}_q[X]$ vérifiant (6.47) pour un k-uple de $\mathbb{F}_q^k$, $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Si $\deg g < \deg f$, on prend $h = g$.
Dans le cas où $\deg g \ge \deg f$, en effectuant la division euclidienne de $g(X)$ par $f(X)$ dans $\mathbb{F}_q[X]$, on obtient un unique couple de polynômes $(\mu(X), h(X))$ tel que

$$g(X) = \mu(X) f(X) + h(X) \quad \text{et} \quad \deg h < \deg f;$$
$$\text{d'où,} \quad h(X) = g(X) - \mu(X) p_1(X) \ldots p_k(X).$$

Or, par hypothèse, $g(X)$ vérifie (6.47), donc pour tout $i (1 \le i \le k)$,

$$\exists \lambda_i(X) \in \mathbb{F}_q[X], \text{ tel que } g(X) = \lambda_i(X) p_i(X) + \alpha_i;$$
$$\text{d'où} \quad h(X) = \lambda_i(X) p_i(X) + \alpha_i - \mu(X) p_1(X) \ldots p_k(X),$$
$$\text{donc,} \quad h(X) \equiv \alpha_i \pmod{p_i(X)}.$$

Ainsi $h(X)$ vérifie (6.47) et $\deg h < \deg f$; s'il existe $h_1(X) \ne h(X)$ dans $\mathbb{F}_q[X]$, satisfaisant à ces mêmes propriétés, alors le Théorème Chinois, appliqué à $h(X)$ et $h_1(X)$, et l'hypothèse (6.46) entraînent

$$h_1(X) \equiv h(X) \pmod{f(X)},$$

donc, $f(X)$ divise $h_1(X) - h(X)$ dans $\mathbb{F}_q[X]$, mais

$$(\deg h_1 < \deg f \text{ et } \deg h < \deg f) \Longrightarrow \deg(h_1 - h) < \deg f$$

d'où une contradiction ; on en conclut que $h_1(X) = h(X)$.

2) Soit $h(X) \in \mathbb{F}_q[X]$ vérifiant les conditions (6.49).
D'après la Prop. 6.29, on a

$$\big(h(X)\big)^q - h(X) = \prod_{\alpha \in \mathbb{F}_q} \big(h(X) - \alpha\big) \tag{6.50}$$

$$\text{et } (\deg h > 0,\ \alpha \neq \alpha' \text{ dans } \mathbb{F}_q) \Longrightarrow \big(h(X) - \alpha\big) \wedge \big(h(X) - \alpha'\big) = 1. \tag{6.51}$$

Pour $h(X)$ non constant, vérifiant (6.49), la relation (6.50) implique

$$\prod_{1 \leq i \leq k} p_i(X) \mid \prod_{\alpha \in \mathbb{F}_q} \big(h(X) - \alpha\big).$$

Dans l'anneau factoriel $\mathbb{F}_q[X]$, les polynômes $p_i(X)$ sont, par hypothèse, deux à deux distincts et irréductibles donc premiers ; par suite,

$$\forall i (1 \leq i \leq k),\ \exists \alpha_i \in \mathbb{F}_q \text{ tel que } p_i(X) \mid h(X) - \alpha_i$$
$$\text{et} \quad \forall \alpha \in \mathbb{F}_q (\alpha \neq \alpha_i \Longrightarrow p_i(X) \nmid (h(X) - \alpha)).$$

On en déduit qu'il existe un *unique* k-uple, $(\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_q$ tel que

$$\forall i (1 \leq i \leq k),\ h(X) \equiv \alpha_i \pmod{p_i(X)}.$$

D'autre part, quel que soit $\alpha \in \mathbb{F}_q$, le polynôme constant α vérifie (6.49) et il lui correspond le k-uple, $(\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_q$ tel que $\alpha_i = \alpha$, quel que soit i, $1 \leq i \leq k$ (Rem. 6.31.).

3) D'après la détermination (ci-dessus) de l'unique k-uple $(\alpha_1, \ldots, \alpha_k)$ d'éléments de $\mathbb{F}_q$ associé à un polynôme $h(X)$, vérifiant (6.49), le nombre de ces polynômes est égal au nombre d'applications de l'ensemble $\{p_1(X), \ldots, p_k(X)\}$ dans $\mathbb{F}_q$, c'est-à-dire, q^k ([3], Ch.III). □

Définition 6.33. Etant donné $f(X) \in \mathbb{F}_q[X]$ vérifiant la condition (6.46), on dira que $h(X) \in \mathbb{F}_q[X]$ est un polynôme $f(X)$-**réducteur** s'il satisfait aux conditions :

$$\big(h(X)\big)^q \equiv h(X) \pmod{f(X)} \quad \text{et} \quad 0 < \deg h < \deg f. \tag{6.52}$$

Remarque 6.34. Pour $f(X)$ vérifiant (6.46), la Prop. 6.32 montre qu'il existe q^k polynômes $h(X)$ satisfaisant aux conditions (6.49), dont q sont des polynômes *constants*.

Proposition 6.35. *Soit $f(X)$ satisfaisant à la condition* (6.46), *avec $k > 1$.*
Si $h(X) \in \mathbb{F}_q[X]$ est un polynôme $f(X)$-réducteur, alors, en posant, pour tout $\alpha \in \mathbb{F}_q$,
$d_\alpha(X) = f(X) \wedge \big(h(X) - \alpha\big)$, *on obtient*

$$f(X) = \prod_{\alpha \in \mathbb{F}_q} d_\alpha(X). \tag{6.53}$$

Démonstration. Par hypothèse, on a $0 < \deg h < \deg f$, donc $f(X)$ ne divise aucun des facteurs $h(X) - \alpha$; l'application de la Prop. 6.29 donne alors

$$f(X) = \prod_{\alpha \in \mathbb{F}_q} d_\alpha(X). \qquad \square$$

Remarque 6.36. La factorisation (6.53) de $f(X)$ dépend du choix du polynôme $f(X)$-réducteur $h(X)$.
D'autre part, dans l'égalité

$$\prod_{1\le i\le k} p_i(X) = \prod_{\alpha\in\mathbb{F}_q} d_\alpha(X)$$

les $p_i(X)$, $1 \le i \le k$ sont, par hypothèse, distincts et irréductibles, mais il n'en n'est pas, nécessairement de même, pour les polynômes
$d_\alpha(X) = f(X) \wedge \big(h(X) - \alpha\big), \alpha \in \mathbb{F}_q$, où $h(X)$ est un polynôme $f(X)$-réducteur donné.
En effet, soit $(\alpha_1, \ldots, \alpha_k)$ l'unique k-uple d'éléments de $\mathbb{F}_q$ associé à $h(X)$(Prop. 6.32).
Pour $\alpha \in \mathbb{F}_q \setminus \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, on a

$$\forall i (1 \le i \le k),\ p_i(X) \wedge \big(h(X) - \alpha\big) = 1, \text{ d'où } d_\alpha(X) = 1.$$

Par suite, $deg\, d_\alpha > 0 \iff \alpha \in \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ et dans ce cas (Rel. 6.51),

$$\alpha_i \neq \alpha_j \Longrightarrow d_{\alpha_i}(X) \wedge d_{\alpha_j}(X) = 1.$$

D'autre part, dans l'unique k-uple associé au polynôme $h(X)$, tous les éléménts ne sont pas égaux (Prop. 6.32, Rem. 6.34), mais certains peuvent l'être ; par exemple, si $\alpha_1 = \alpha_2$, alors $d_{\alpha_1}(X) = d_{\alpha_2}(X)$ et

$$p_1(X) \mid (h(X) - \alpha_1) \Longrightarrow p_1(X) \mid d_{\alpha_1}(X),$$
$$p_2(X) \mid (h(X) - \alpha_1) \Longrightarrow p_2(X) \mid d_{\alpha_1}(X).$$

Ainsi $p_1(X)p_2(X) \mid d_{\alpha_1}(X)$, donc, $d_{\alpha_1}(X)$ n'est pas un facteur irréductible de $f(X)$.
Cependant, nous verrons, dans le paragraphe suivant que le calcul des $d_\alpha(X)$ pour, éventuellement, plusieurs polynômes $f(X)$-réducteurs, permettra de déterminer les k facteurs distincts et irréductibles de $f(X)$.

3/ Algorithme de Berlekamp

Pour $f(X) \in \mathbb{F}_q[X]$ vérifiant (6.46), l'Algorithme de Berlekamp est un processus qui permet déterminer les polynômes $f(X)$-réducteurs et par suite les facteurs irréductibles, unitaires, distincts de $f(X)$.

Théorème 6.37. Algorithme de Berlekamp
Soit $f(X) \in \mathbb{F}_q[X]$, vérifiant (6.46) ; on suppose $s := deg\, f > 1$.
Pour tout $i (0 \le i \le s-1)$, on note $r_i(X)$ le reste de la division euclidienne de X^{iq} par $f(X)$, dans $\mathbb{F}_q[X]$. On pose

$$r_i(X) := \sum_{0\le j\le s-1} b_{ij} X^j \quad et \quad B := (b_{ij}),$$

où la matrice B appartient à l'anneau $M_s(\mathbb{F}_q)$ des matrices carrées d'ordre s sur $\mathbb{F}_q$.
1) *Pour $h(X) := \sum_{0\le i\le s-1} a_i X^i \in \mathbb{F}_q[X]$, les conditions (6.49) :*

$$h(X^q) \equiv h(X) \pmod{f(X)} \quad et \quad deg\, h < deg\, f$$

est équivalente à

$$(a_0, a_1, \ldots, a_{s-1})(B - I) = 0 \tag{6.54}$$

où, 0 désigne l'élément nul de $\mathbb{F}_q{}^s$ et I est la matrice unité de $M_s(\mathbb{F}_q)$.
2) *$f(X)$ est le produit de k facteurs unitaires, irréductibles, distincts* (Cf. (6.46)) *si et seulement si*

$$rang(B - I) = s - k. \tag{6.55}$$

Démonstration. 1) Pour tout i, $0 \leq i \leq s-1$, il existe $q_i(X)$ et $r_i(X)$, uniques dans $\mathbb{F}_q[X]$ ([13], Th. 4.33), tels que

$$X^{iq} = f(X)q_i(X) + r_i(X), \quad \text{et} \quad deg\, r_i < deg\, f, \quad \text{d'où}$$
$$X^{iq} \equiv r_i(X) \pmod{f(X)} \quad \text{et} \quad deg\, r_i < deg\, f.$$

Les conditions ($f(X)$ vérifie (6.46)) et ($deg\, f = s > 1$) impliquent $r_i(X) \neq 0$.
Soit $h(X) := \sum_{0 \leq i \leq s-1} a_i X^i$ dans $\mathbb{F}_q[X]$, vérifiant (6.49).
Compte tenu de la Rem. 6.31, b), on a alors, dans l'anneau quotient $\mathbb{F}_q[X]/(f(X))$ (en conservant la notation X pour la classe de X modulo $f(X)$),

$$h(X^q) = h(X) \quad \text{et} \quad deg\, h < deg\, f, \quad \text{d'où}$$

$$\begin{aligned}
h(X) \text{ vérifie(6.49)} &\iff \sum_{0 \leq i \leq s-1} a_i r_i(X) = \sum_{0 \leq i \leq s-1} a_i X^i, \\
&\iff \sum_{0 \leq i \leq s-1} a_i \Big(\sum_{0 \leq j \leq s-1} b_{ij} X^j \Big) = \sum_{0 \leq i \leq s-1} a_i X^i; \\
&\iff \sum_{0 \leq j \leq s-1} \Big(\sum_{0 \leq i \leq s-1} a_i b_{ij} \Big) X^j = \sum_{0 \leq j \leq s-1} a_j X^j, \\
&\iff \sum_{0 \leq i \leq s-1} a_i b_{ij} = a_j, \ \forall j (0 \leq j \leq s-1), \\
&\iff (a_0, a_1, \ldots, a_{s-1})(B - I) = 0.
\end{aligned}$$

2) Ce qui précède montre que la matrice B est déterminée par la donnée du polynôme $f(X)$ et d'après la relation (6.54), les coefficients $a_i, 0 \leq i \leq s-1$, forment une solution du système (S) de s équations linéaires sur $\mathbb{F}_q$, à s inconnues, dont la $j^{ème}$ équation $(0 \leq j \leq s-1)$ s'écrit

$$\sum_{0 \leq i \leq s-1} a_i b_{ij} - a_j = 0.$$

On peut aussi considérer que la matrice $(B - I)$ définit le morphisme

$$\begin{aligned}
\Psi : \mathbb{F}_q{}^s &\longrightarrow \mathbb{F}_q{}^s \\
(a_0, a_1, \ldots, a_{s-1}) &\longmapsto (a_0, a_1, \ldots, a_{s-1})(B - I).
\end{aligned}$$

On a $dim_{\mathbb{F}_q} Im\Psi + dim_{\mathbb{F}_q} Ker\Psi = s$, d'où (Prop. 6.34.),

$$\begin{aligned}
\text{le système } (S) \text{ a } q^k \text{ solutions} &\iff dim_{\mathbb{F}_q} Ker\Psi = k, \\
&\iff dim_{\mathbb{F}_q} Im\Psi = s - k, \\
&\iff rang(B - I) = s - k. \qquad \square
\end{aligned}$$

Remarque 6.38. $Ker\Psi$ est le *sous-espace nul* correspondant au morphisme Ψ ou à la matrice $B - I$.
Les définitions de s et k, impliquent $1 < s - k \leq s - 1$ et

$$rang(B - I) = s - 1 \iff f(X) \text{ irréductible}$$
$$rang(B - I) = s - k < s - 1 \iff f(X) \text{ réductible et produit de } k \text{ facteurs irréductibles, unitaires, distincts.}$$

Le premier cas montre que l'algorithme de Berlekamp peut servir de *critère d'irréductibilité* pour les polynômes de $\mathbb{F}_q[X]$.

Dans le second cas, si l'on identifie toute solution $(a_0, a_1, \ldots, a_{s-1})$ du système (S), au polynôme $h(X) = \sum_{0 \leq i \leq s-1} a_i X^i$, alors le $\mathbb{F}_q$-espace vectoriel $Ker\,\Psi$ contient au moins une base formée de k polynômes $h_j(X), 1 \leq j \leq k$, où l'on peut supposer $h_1(X) = 1$ et les $h_j(X), 2 \leq j \leq k$, sont des polynômes $f(X)$-réducteurs.

4/ Applications de l'algotithme de Berlekamp

Exemple 6.39. Soit, dans $\mathbb{N}$, $n > 1$ et p premier tel que $p \nmid n$.
La Prop. 6.24. montre que tout polynôme cyclotomique $\Phi_n(X)$ sur $\mathbb{F}_p$ satisfait à la condition (6.46), ses facteurs irréductibles et unitaires étant les $n^{èmes}$ polynômes primitifs sur $\mathbb{F}_p$; ceux-ci peuvent donc être déterminés par la méthode de l'Algorithme de Berlekamp (Th. 6.37), appliquée dans le cas où $q = p$.
Exemple : on considère le $7^{ème}$ polynôme cyclotomique sur $\mathbb{F}_2$; avec les notations du Th. 6.37, on a, dans ce cas,

$$q = 2,\ f(X) = \Phi_7(X),\ s = deg\, f = \varphi(7) = 7 - 1 = 6.$$

$$X^7 - 1 = (X-1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$$

$$\text{implique} \qquad \Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1.$$

Les polynômes $r_i(X)$, pour $0 \leq i \leq 5$, sont les seconds membres des relations d'équivalences ci-dessous (sachant que $q = 2$, donc $-1 = 1$)

$$\begin{aligned}
&i = 0 \Longrightarrow 1 \equiv 1 \pmod{\Phi_7(X)}\\
&i = 1 \Longrightarrow X^2 \equiv X^2 \pmod{\Phi_7(X)}\\
&i = 2 \Longrightarrow X^4 \equiv X^4 \pmod{\Phi_7(X)}\\
&i = 3 \Longrightarrow X^6 \equiv X^5 + X^4 + X^3 + X^2 + X + 1 \pmod{\Phi_7(X)}\\
&i = 4 \Longrightarrow X^8 \equiv X \pmod{\Phi_7(X)}\\
&i = 5 \Longrightarrow X^{10} \equiv X^3 \pmod{\Phi_7(X)}.
\end{aligned}$$

On en déduit la matrice $B - I$, dans $M_6(\mathbb{F}_2)$:

$$B - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

La relation $(a_0, a_1, \ldots, a_5)(B - I) = 0$ équivaut au système (S) suivant

$$(S) : \begin{cases} a_3 = 0 \\ a_1 + a_3 + a_4 = 0 \\ a_1 + a_2 + a_3 = 0 \\ a_5 = 0 \\ a_2 + a_3 + a_4 = 0 \\ a_3 + a_5 = 0 \end{cases}$$

On vérifie que

$$(rang\,(B-I)=4=6-2)\Longrightarrow k=2.$$

Le $7^{ème}$ polynôme cyclotomique sur $\mathbb{F}_2$, $\Phi_7(X)$, est donc le produit de deux $7^{èmes}$ polynômes primitifs, $p_1(X), p_2(X)$, de même degré m tel que $2m=6$, d'où $m=3$; d'autre part, $2^3=8$, donc

$$\mathbb{F}_8 \text{ est la } 7^{ème} \text{ extension cyclotomique sur } \mathbb{F}_2.$$

Le système (S) a quatre solutions ; on a $q=2$, donc deux d'entre elles correspondent à des polynômes constants (Rem. 6. 34), d'où deux polynômes $\Phi_7(X)$-réducteurs.
L'inconnue a_0 n'intervient pas dans le système (S), donc est quelconque dans $\mathbb{F}_2$; de plus $a_3=a_5=0$, d'où les solutions de (S) :

$$(0,0,0,0,0,0),\ (1,0,0,0,0,0),\ (0,1,1,0,1,0),\ (1,1,1,0,1,0).$$

Les deux premières correspondent au polynôme nul et au polynôme $h_1(X)=1$, les deux polynômes $\Phi_7(X)$-réducteurs sont alors,

$$h_2(X)=X+X^2+X^4,\quad h_3(X)=1+X+X^2+X^4.$$

D'après ce qui précède, le sous-espace nul est de dimension $k=2$; $\{h_1,h_2\}$ et $\{h_1,h_3\}$ sont des bases de ce sous-espace nul.
Déterminons la factorisation de $\Phi_7(X)$ par la relation (6.53) avec h_2, sachant que les deux $7^{èmes}$ polynômes primitifs sur $\mathbb{F}_2$ sont de degré 3.

$$\begin{aligned}&\Phi_7(X)\wedge(X^4+X^2+X)=X^3+X+1=p_1(X)\\&\Phi_7(X)\wedge(X^4+X^2+X+1)=X^3+X^2+1=p_2(X),\\\text{d'où}\quad&\Phi_7(X)=(X^3+X^2+1)(X^3+X+1).\end{aligned}$$

Les racines des polynômes $p_1(X)$ et $p_2(X)$ sont les racines $7^{èmes}$-primitives de l'unité du corps $\mathbb{F}_2$; ce sont donc les six générateurs du groupe cyclique $U_7=\mathbb{F}_8\setminus\{0\}$.

On remarquera que la valeur $m=3$ du degré d'un $7^{ème}$ polynôme primitif, est bien celle que l'on obtient en appliquant la Prop. 6.26 :

$$(6.39)\Longrightarrow m=o(\overline{2}) \text{ dans } G_7 \Longrightarrow m=3.$$

Exemple 6.40. Factorisation dans $\mathbb{F}_2[X]$, de

$$f(X)=X^8+X^6+X^5+X^4+X^3+X^2+1.$$

On a $f'(X)=X^4+X^3=X^3(X+1)$, d'où $f(X)\wedge f'(X)=1$; le polynôme $f(X)$ n'a donc que des racines simples dans un corps de décomposition sur $\mathbb{F}_2$ ([13], Cor. 8.49), on en déduit que $f(X)$ vérifie la condition (6.46), pour un certain entier $k\geq 1$.
Selon le Th. 6.37, déterminons les polynômes $r_i(X)$, $0\leq i\leq 7$.

$$\begin{aligned}&i=0\Longrightarrow 1\equiv 1 \pmod{f(X)}\\&i=1\Longrightarrow X^2\equiv X^2 \pmod{f(X)}\\&i=2\Longrightarrow X^4\equiv X^4 \pmod{f(X)}\\&i=3\Longrightarrow X^6\equiv X^6 \pmod{f(X)}\\&i=4\Longrightarrow X^8\equiv X^6+X^5+X^4+X^3+X^2+1 \pmod{f(X)}\\&i=5\Longrightarrow X^{10}\equiv X^7+X^3+1 \pmod{f(X)}\\&i=6\Longrightarrow X^{12}\equiv X^7+X^6+X^4+X^3+X^2+X \pmod{f(X)}\\&i=7\Longrightarrow X^{14}\equiv X^7+X^6+X^5+X^4+X^3+X^2+X+1.\end{aligned}$$

On en déduit la matrice $B-I$, dans $M_8(\mathbb{F}_2)$:

$$B-I=\begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&1&1&0&0&0&0&0\\ 0&0&1&0&1&0&0&0\\ 0&0&0&1&0&0&1&0\\ 1&0&1&1&0&1&1&0\\ 1&0&0&1&0&1&0&1\\ 0&1&1&1&1&0&0&1\\ 1&1&1&1&1&1&1&0 \end{pmatrix}.$$

La condition $(a_0,a_1,\ldots,a_7)(B-I)=0$ équivaut au système (S) :

$$(S):\begin{cases} a_4+a_5+a_7=0\\ a_1+a_6+a_7=0\\ a_1+a_2+a_4+a_6+a_7=0\\ a_3+a_4+a_5+a_6+a_7=0\\ a_2+a_6+a_7=0\\ a_4+a_5+a_7=0\\ a_3+a_4+a_7=0\\ a_5+a_6=0 \end{cases}$$

On vérifie que la matrice $B-I$ est de rang $5=8-3$, donc $f(X)$ est le produit de 3 facteurs irréductibles, unitaires, distincts. Le nombres des polynômes $f(X)$-réducteurs est $2^3-2=6$. A chaque solution $(a_0,a_1,\ldots a_7)$ du système (S) correspond un polynôme $h(X)=\sum_{0\le i\le 7} a_iX^i$, d'où, les polynômes $f(X)$-réducteurs $h_j(X)$, $2\le j\le 7$ (a_o est arbitraire dans $\mathbb{F}_2$).

$$\begin{aligned}
&(0,0,0,0,0,0,0,0)\Longrightarrow h_0(X)=0\\
&(1,0,0,0,0,0,0,0)\Longrightarrow h_1(X)=1\\
&(0,1,1,0,1,0,0,1)\Longrightarrow h_2(X)=X+X^2+X^4+X^7\\
&(1,1,1,0,1,0,0,1)\Longrightarrow h_3(X)=1+X+X^2+X^4+X^7\\
&(0,0,0,1,0,1,1,1)\Longrightarrow h_4(X)=X^3+X^5+X^6+X^7\\
&(1,0,0,1,0,1,1,1)\Longrightarrow h_5(X)=1+X^3+X^5+X^6+X^7\\
&(0,1,1,1,1,1,1,0)\Longrightarrow h_6(X)=X+X^2+X^3+X^4+X^5+X^6\\
&(1,1,1,1,1,1,1,0)\Longrightarrow h_7(X)=1+X+X^2+X^3+X^4+X^5+X^6.
\end{aligned}$$

En calculant les *p.g.c.d.* par l'algorithme d'Euclide ([13], Ch. 5) et en tenant compte des Rem. 6.36, on obtient :

$$\begin{aligned}
f(X)\wedge h_2(X)&=X^3+X^2+1, \text{ irréductible dans } \mathbb{F}_2[X];\\
f(X)\wedge h_4(X)&=X^3+X+1, \text{ irréductible dans } \mathbb{F}_2[X];\\
f(X)\wedge h_6(X)&=X^2+X+1, \text{ irréductible dans } \mathbb{F}_2[X].
\end{aligned}$$

On en déduit la factorisation de $f(X)$ recherchée :

$$f(X)=(X^2+X+1)(X^3+X+1)(X^3+X^2+1).$$

Remarque 6.41. a) Comme on l'a signalé dans la Rem. 6.36, dans la formule (6.53), certains facteurs $d_\alpha(X)$ peuvent être réductibles (c'était le cas dans l' exemple précédent) ; mais on remarque que, d'une façon générale, un polynôme $d_\alpha(X)$ vérifie la condition (6.46), son degré est inférieur à celui de $f(X)$ et ses facteurs irréductibles divisent $f(X)$. On peut donc, éventuellement, réappliquer la méthode de l'algorithme de Berlekamp à un tel polynôme $d_\alpha(X)$, et, s'il le faut, répéter le processus, jusqu'à l'obtention de la factorisation recherchée pour $f(X)$.
b) Dans les exemples précédents, le degré du polynôme $f(X)$ n'est pas très élevé et le corps de base est $\mathbb{F}_2$; le nombre des polynômes $f(X)$-réducteurs n'est donc pas trop grand ; et même, dans le second exemple, la connaissance de deux facteurs irréductibles pouvait permettre de calculer sans peine, le troisième.
Mais on conçoit facilement que, lorsque le degré de $f(X)$, ainsi que le nombre des éléments du corps $\mathbb{F}_q$ sont élevés, la méthode de l'algorithme de Berlekamp devient impraticable « à la main », et il est nécessaire de faire appel à l'informatique, ce qui est possible, puisqu'il s'agit d'une méthode algorithmique.

6. Exercices

1. *Structure du groupe des éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$.
Pour tout entier $n \geq 2$, on désigne par G_n le groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$; on note $\bar{x}$, la classe modulo n d'un élémént x de $\mathbb{Z}$.
G_n est l'ensemble des générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$ ([12], Prop. 3.24), donc

$$G_n = \{\bar{x} \in \mathbb{Z}/n\mathbb{Z} \,;\, x \wedge n = 1\}$$

et on rappelle que $| G_n | = \varphi(n)$.
1°) Montrer que si, dans $\mathbb{N}$, on a

$$n = 2^\alpha q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k} \geq 2,$$

avec $\alpha \geq 0$, $k \geq 0$, les q_i étant, pour $k \geq 1$, des nombres premiers impairs, deux à deux distincts, alors

$$G_n \simeq G_{2^\alpha} \times G_{q_1^{\alpha_1}} \times \cdots \times G_{q_k^{\alpha_k}}.$$

2°) Soit q un nombre premier *impair*.
a) Démontrer, par récurrence sur α, que pour tout entier $\alpha > 0$, il existe $\lambda \in \mathbb{N}^*$ tel que

$$(1+q)^{q^\alpha} = 1 + \lambda q^{\alpha+1} \quad \text{et} \quad q \nmid \lambda. \tag{6.56}$$

b) Préciser l'ordre du groupe G_{q^α} et vérifier que l'élément $\overline{1+q}$ est d'ordre $q^{\alpha-1}$ dans G_{q^α}.
3°) a) Vérifier que le groupe G_q est cyclique d'ordre $q-1$.
b) Pour tout $x \in \mathbb{Z}$, $\bar{x}$ désignant, dans cette question, la classe de x modulo q^α, on note $\dot{x}$ la classe de x modulo q et on considère le morphisme de groupes

$$\begin{aligned} \psi : G_{q^\alpha} &\longrightarrow G_q \\ \bar{x} &\longmapsto \dot{x}. \end{aligned}$$

Prouver que $| Ker\,\psi | = q^{\alpha-1}$ et en tenant compte du 2 °) b), montrer que $Ker\,\psi$ est un sous-groupe cyclique de G_{q^α}.
c) Soit $\bar{x} \in G_{q^\alpha}$ tel que $\dot{x}$ soit un générateur du groupe G_q.
On note $< \bar{x} >$ le sous-groupe de G_{q^α} engendré par $\bar{x}$. Montrer qu'il existe un élément $\bar{y} \in < \bar{x} >$ d'ordre $q-1$.

En déduire l'ordre de $\overline{y}(\overline{1+q})$ dans G_{q^α} ; en conclure que le groupe G_{q^α} est cyclique et

$$G_{q^\alpha} \simeq \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/q^{\alpha-1}\mathbb{Z}.$$

4°) On considère le groupe G_{2^α}, pour $\alpha \in \mathbb{N}^*$.
a) Vérifier les propriétés suivantes :

$$\alpha = 1 \Longrightarrow G_2 = \{\overline{1}\}, \text{ dans } \mathbb{Z}/2\mathbb{Z}.$$
$$\alpha = 2 \Longrightarrow G_{2^2} \text{ cyclique d'ordre 2.}$$

Dans les questions b) et c) qui suivent, on suppose $\alpha > 2$.
b) Démontrer, par récurrence sur α, que pour tout entier $\alpha > 2$, il existe $\lambda \in \mathbb{N}^*$ tel que

$$5^{2^\alpha} = 1 + \lambda 2^{\alpha+2}. \tag{6.57}$$

c) Pour tout $x \in \mathbb{Z}$, $\overline{x}$ désignant, ici, la classe de x modulo 2^α, on note $\dot{x}$ la classe de x modulo $2^2 = 4$ et on considère le morphisme de groupes :

$$\psi : G_{2^\alpha} \longrightarrow G_{2^2}$$
$$\overline{x} \longmapsto \dot{x}.$$

– Prouver que $\overline{5} \in Ker\,\psi$; en déduire que, dans le groupe G_{2^α}, $Ker\,\psi$ est un sous-groupe cyclique d'ordre $2^{\alpha-2}$.
– On considère le sous-groupe d'ordre 2 de G_{2^α}, $H := \{-\overline{1}, \overline{1}\}$. En posant $K := Ker\,\psi$, montrer que

$$G_{2^\alpha} = HK.$$

En déduire que

$$G_{2^\alpha} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}.$$

En conclure que pour $\alpha > 2$, le groupe G_{2^α} n'est pas cyclique.
5°) Expliciter une preuve détaillée de la Prop. 6.26.

2. Soit soit K un corps de caractéristique 0 et $n > 1$ dans $\mathbb{N}$. On suppose que le polynôme $X^n - 1$ est scindé sur K.
Soit $f(X) := X^n - a$, où $a \in K^*, a \neq 1$. On note E un corps de décomposition de $f(X)$ sur K.
a) Vérifier que $f(X)$ n'a que des racines simples dans E.
b) Soit ω une racine $n^{ème}$ *primitive* de l'unité de K et $\alpha \in E$ une racine de $f(X)$, montre que l'ensemble des racines de $f(X)$ dans E est

$$\{\omega^k \alpha\,;\, 0 \leq k \leq n-1\}.$$

En déduire que $E = K(\alpha)$.

3. Soit K une extension algébrique de $\mathbb{Q}$, $a \in K^*$, $n \in \mathbb{N}^*$ et $\alpha \in \overline{\mathbb{Q}}$ une racine du polynôme $X^n - a$.
1°) On suppose, dans cette question, que le polynôme $X^n - a$ est *non irréductible* sur K.
Soit $f(X)$ un diviseur de $X^n - a$, dans $K[X]$, de degré d tel que $1 \leq d \leq n-1$ et soit $\varepsilon_n \in \overline{\mathbb{Q}}$, une racine $n^{ème}$ *primitive* de l'unité.
a) Montrer que le terme constant de $f(X)$ est de la forme $\varepsilon_n^c \alpha^d$, où $c \in \mathbb{N}$ (voir Ex. **2.** précédent).

b) Soit $s := d \wedge n$ (p.g.c.d. de d et n). Démontrer qu'il existe une racine $n^{ème}$ de l'unité $\eta \in \overline{\mathbb{Q}}$, telle que

$$\eta\alpha^s \in K.$$

2°) Soit p un nombre premier et $X^p - a$ dans $K[X], a \neq 0$.
Montrer que si a n'a pas de racine $p^{ème}$ dans K, alors $X^p - a$ est *irréductible* sur K.

4. Déterminer le $5^{ème}$ polynôme cyclotomique sur $\mathbb{F}_2$.

5. Utiliser l'algorithme de Berlekamp pour factoriser les polynômes suivants :

$$X^{10} + X^5 + 1 \quad \text{sur } \mathbb{F}_2;$$
$$X^8 + X^6 + X^4 + X^3 + 1 \quad \text{sur } \mathbb{F}_2;$$
$$X^7 + X^6 + X^5 - X^3 + X^2 - X - 1 \quad \text{sur } \mathbb{F}_3.$$

Chapitre 7
Fondements de la Théorie de Galois

Préliminaires
La Théorie de Galois est l'étude des extensions de corps $L : K$ au moyen du groupe des K-automorphismes de L (Déf. 7.1).
Cette méthode, introduite par le mathématicien français Evariste **Galois** (1811-1832), s'avéra d'une grande efficacité (Voir la Préface de ce livre) ; elle lui permit, en particulier, de résoudre un problème qui préoccupait les mathématiciens de son époque, à savoir : *la caractérisation* des équations polynômiales dites *résolubles par radicaux* (Voir Ch. 9).
Par ailleurs, grâce à la Théorie de Galois, il a été possible d'apporter des réponses à plusieurs questions que se posaient les mathématiciens, parfois depuis l'Antiquité, telle la construction des polygones réguliers par la règle et le compas (voir le par. **3.** de ce chapitre).

1. Groupe de Galois - Correspondance de Galois

Pour une extension de corps $L : K$, on supposera, de façon générale, $K \subseteq L$.

A. Groupe de Galois

Définition 7.1. Etant donné une extension L d'un corps K, on dit qu'un automorphisme σ du corps L est un **K-automorphisme** de L, si $\sigma_{/K} = id_K$.

Remarque 7.2. Les K-automorphismes de L ne sont autres que les automorphismes de la K-algèbre L ; leur ensemble forme un *sous-groupe* du groupe *Aut* L de tous les automorphismes du corps L.

Définition 7.3. On appelle **groupe de Galois** d'une extension de corps $L : K$, le groupe des K-automorphismes de L.

Notation : Le groupe de Galois d'une extension $L : K$ sera noté
$$G(L : K).$$

Exemple 7.4. 1) Si $L = K$, alors $G(L : K) = \{id_L\} = \{id_K\}$.

2) $K = \mathbb{R}$, $L = \mathbb{C}$; puisque
$$\mathbb{C} = \mathbb{R}(i) = \{x + iy\ ;\ (x, y) \in \mathbb{R} \times \mathbb{R}\},$$
tout $\sigma \in G(\mathbb{C} : \mathbb{R})$ est déterminé par la donnée de $\sigma(i)$; or,
$$i^2 = -1 \Longrightarrow (\sigma(i))^2 = \sigma(i^2) = \sigma(-1) = -1,$$
$$\text{d'où} \quad \sigma(i) = i \quad \text{ou} \quad \sigma(i) = -i.$$
Par suite $G(\mathbb{C} : \mathbb{R}) = \{id_{\mathbb{C}}, \gamma\}$, où γ est l'automorphime de conjugaison défini par
$$\forall x + iy \in \mathbb{C},\ \gamma(x + iy) = x - iy.$$

Le groupe $G(\mathbb{C}:\mathbb{R})$ est d'ordre 2, donc cyclique.

3) $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{3})$; on a

$$Irr_{\mathbb{Q}}(\sqrt{3},X)=X^2-3 \Longrightarrow [\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2;$$

$$\mathbb{Q}(\sqrt{3})=\{x+y\sqrt{3}\,;\,(x,y)\in\mathbb{Q}\times\mathbb{Q}\};$$

donc tout $\sigma\in G(\mathbb{Q}(\sqrt{3}):\mathbb{Q})$ est déterminé par la donnée de $\sigma(\sqrt{3})$; or,

$$(\sigma(\sqrt{3}))^2=\sigma(3)=3 \Longrightarrow \sigma(\sqrt{3})=\pm\sqrt{3},$$

par suite $G(\mathbb{Q}(\sqrt{3}):\mathbb{Q})=\{id_{\mathbb{Q}(\sqrt{3})},\sigma\}$, où

$$\forall(x+y\sqrt{3})\in\mathbb{Q}(\sqrt{3}),\ \sigma(x+y\sqrt{3})=x-y\sqrt{3}.$$

Le groupe $G(\mathbb{Q}(\sqrt{3}):\mathbb{Q})$ est encore d'ordre 2.

4) $K=\mathbb{Q}$, $L=\mathbb{Q}(\lambda)$, où $\lambda:=\sqrt[3]{2}\in\mathbb{R}$.
Soit $\sigma\in G(\mathbb{Q}(\lambda):\mathbb{Q})$, alors

$$(\sigma(\lambda))^3=\sigma(\lambda^3)=\sigma(2)=2.$$

L'automorphisme σ de $\mathbb{Q}(\lambda)$ se prolonge en un automorphisme :

$$\begin{aligned}\hat{\sigma}:\mathbb{Q}(\lambda)[X] &\longrightarrow \mathbb{Q}(\lambda)[X]\\ \sum_{0\le i\le n} a_iX^i &\longmapsto \sum_{0\le i\le n}\sigma(a_i)X^i;\end{aligned}$$

d'où $\hat{\sigma}(X^3-2)=X^3-2$. Par suite, dans $\mathbb{Q}(\lambda)$, σ transforme une racine cubique de 2 en une racine cubique de 2, or on a $\mathbb{Q}(\lambda)\subset\mathbb{R}$ et λ est la seule racine cubique réelle de 2, donc $\sigma(\lambda)=\lambda$, ce qui implique

$$G(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})=\{id_{\mathbb{Q}(\sqrt[3]{2})}\}.$$

B. Correspondance de Galois

A toute extension de corps $L:K$, on associe les deux ensembles suivants :
$\mathcal{F}:=$ l'ensemble des corps intermédiaires de $L:K$ (Déf. 1.20) ;
$\mathcal{H}:=$ l'ensemble des sous-groupes de $G(L:K)$.

Définition 7.5. Pour tout $H\in\mathcal{H}$, on appelle **invariant de H dans L**, l'ensemble :

$$Inv_L(H):=\{x\in L \quad ; \quad \forall\sigma\in H,\ \sigma(x)=x\}. \tag{7.1}$$

Proposition 7.6. *Compte tenu des notations précédentes, pour toute extension de corps $L:K$, on a*

$$1)\ F\in\mathcal{F}\Longrightarrow G(L:F)\in\mathcal{H}.$$
$$2)\ H\in\mathcal{H}\Longrightarrow Inv_L(H)\in\mathcal{F}.$$

Démonstration. Par hypothèse, $K\subseteq F\subseteq L$.
1) Soit $\sigma\in G(L:F)$; σ est un automorphisme du corps L tel que $\sigma_{/F}=id_F$, donc, a fortiori, $\sigma_{/K}=id_K$, d'où $\sigma\in G(L:K)$. On en déduit que $G(L:F)$ est un sous-groupe de $G(L:K)$, donc $G(L:F)\in\mathcal{H}$.

2) Les éléments $\sigma\in H$ étant des K-automorphismes de L, on vérifie facilement que l'ensemble $Inv_L(H)$ est un sous-corps de L contenant K, autrement dit, $Inv_L(H)\in\mathcal{F}$. □

Les résultats de la Prop. 7.6 amènent à associer à toute extension de corps $L : K$ les applications :

$$\begin{array}{lll} \gamma : \mathcal{F} \longrightarrow \mathcal{H} & \qquad & \gamma' : \mathcal{H} \longrightarrow \mathcal{F} \\ F \longmapsto G(L:F) & & H \longmapsto Inv_L(H). \end{array}$$

Proposition 7.7. *Les ensembles $\mathcal{F}$ et $\mathcal{H}$ étant partiellement ordonnés par l'inclusion, les applications γ et γ', associées à une extension de corps $L : K$, vérifient les propriétés suivantes :*

$$\forall (F_1, F_2) \in \mathcal{F} \times \mathcal{F}, \quad F_1 \subseteq F_2 \Longrightarrow \gamma(F_2) \subseteq \gamma(F_1); \tag{7.2}$$

$$\forall (H_1, H_2) \in \mathcal{H} \times \mathcal{H}, \quad H_1 \subseteq H_2 \Longrightarrow \gamma'(H_2) \subseteq \gamma'(H_1); \tag{7.3}$$

$$F \in \mathcal{F} \Longrightarrow F \subseteq \gamma' \circ \gamma(F) \quad ; \quad H \in \mathcal{H} \Longrightarrow H \subseteq \gamma \circ \gamma'(H); \tag{7.4}$$

$$F \in \mathcal{F} \Longrightarrow \gamma(F) = \gamma \circ \gamma' \circ \gamma(F); \tag{7.5}$$

$$H \in \mathcal{H} \Longrightarrow \gamma'(H) = \gamma' \circ \gamma \circ \gamma'(H). \tag{7.6}$$

Démonstration. Par hypothèse, on a $K \subseteq F_1 \subseteq F_2 \subseteq L$, donc F_2 est un corps intermédiaire pour l'extension $L : F_1$. On en déduit que (Prop. 7.6)

$$\gamma(F_2) = G(L:F_2) \text{ est un sous-groupe de } G(L:F_1) = \gamma(F_1),$$

ce qui justifie la relation (7.2).

Soit x un élément de $\gamma'(H_2) = Inv_L(H_2)$, alors

$$\big((\forall \sigma \in H_2,\ \sigma(x) = x) \ \text{ et } \ H_1 \subseteq H_2\big) \Longrightarrow x \in \gamma'(H_1) = Inv_L(H_1),$$

d'où la relation (7.3).

Quels que soient $F \in \mathcal{F}$ et $H \in \mathcal{H}$, on a

$$x \in F \Longrightarrow \big(\forall \sigma \in \gamma(F),\ \sigma(x) = x\big) \Longrightarrow x \in \gamma' \circ \gamma(F);$$

$$\sigma \in H \Longrightarrow \big(\forall x \in \gamma'(H),\ \sigma(x) = x\big) \Longrightarrow \sigma \in \gamma \circ \gamma'(H);$$

on déduit les relations (7.4).

Par hypothèse $F \in \mathcal{F}$, alors la relation (7.4) implique

$$K \subseteq F \subseteq \gamma' \circ \gamma(F) \subseteq L;$$

en utilisant la relation (7.2), avec $F_2 := \gamma' \circ \gamma(F)$ et $F_1 = F$, on obtient

$$\gamma \circ \gamma' \circ \gamma(F) \subseteq \gamma(F),$$

et, en appliquant (7.4) au groupe $H := \gamma(F)$, on a

$$\gamma(F) \subseteq \gamma \circ \gamma' \circ \gamma(F);$$

ce qui entraîne la relation (7.5).

L'hypothèse $H \in \mathcal{H}$ implique, d'après (7.4), $H \subseteq \gamma \circ \gamma'(H)$, et l'application de (7.3) donne

$$\gamma' \circ \gamma \circ \gamma'(H) \subseteq \gamma'(H).$$

D'autre part, la relation (7.4) appliquée à $F := \gamma'(H)$, entraîne

$$\gamma'(H) \subseteq \gamma' \circ \gamma \circ \gamma'(H),$$

d'où la relation (7.6). □

Définition 7.8. Dans le contexte précédent, le couple (γ, γ') définit ce qu'on appelle la **correspondance de Galois** associée à l'extension de corps $L : K$.

Nous résumons les résultats de la Prop. 7.7, par le tableau suivant,

$$\begin{array}{rcccc} K & \subseteq & F & \subseteq & L \\ G(L:K) & \supseteq & G(L:F) & \supseteq & \{id_L\} \\ Inv_L(G(L:K)) & \subseteq & Inv_L(G(L:F)) & \subseteq & L \\ G(L:K) & \supseteq & G(L:F) & \supseteq & \{id_L\} \end{array}$$

dans lequel les éléments des lignes 2, 3 et 4 sont respectivement, les images par γ, $\gamma' \circ \gamma$ et $\gamma \circ \gamma' \circ \gamma$ des éléments de la $1^{ère}$ ligne.

Remarque 7.9. a) D'une façon générale, si $\mathcal{U}$ et $\mathcal{V}$ désignent deux ensembles partiellement ordonnés et si $\gamma : \mathcal{U} \longrightarrow \mathcal{V}$, $\gamma' : \mathcal{V} \longrightarrow \mathcal{U}$ forment un couple d'applications satisfaisant aux propriétés de la Prop. 7.7, on dit que le couple (γ, γ') définit une *correspondance de Galois* entre $\mathcal{U}$ et $\mathcal{V}$.
b) Les relations (7.4) de la Prop. 7.7 montrent qu'en général, le couple (γ, γ') *ne définit pas* une bijection de $\mathcal{F}$ sur $\mathcal{H}$. En particulier, on a, généralement,

$$K \subsetneq Inv_L(G(L:K)) = \gamma' \circ \gamma(K).$$

Par exemple, pour $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt[3]{2})$, on a (Cf. Exemple 7.4, 4))

$$\gamma(\mathbb{Q}) = G(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{id_{\mathbb{Q}(\sqrt[3]{2})}\}$$
$$\text{d'où} \quad \gamma' \circ \gamma(\mathbb{Q}) = \mathbb{Q}(\sqrt[3]{2}) \supsetneq \mathbb{Q}.$$

La Théorie de Galois établit une corrélation entre certaines propriétés des extensions de corps et certaines propriétés de leurs groupes de Galois. De ce point de vue, les extensions de corps $L : K$ les plus « intéressantes » seront celles pour lesquelles la correspondance de Galois (γ, γ') définit une bijection entre les ensembles $\mathcal{F}$ et $\mathcal{H}$ (Th. 7.30).

2. Théorème fondamental de Galois

Dans toute l'étude qui suit, les résultats du Ch.3, concernant les notions d'extension normale, de clôture normale et d'extension séparable *sont essentiels ; nous les complétons, de plus, par les propriétés et notions développées dans le paragraphe* **A.** *ci-dessous.*

A. K-monomorphismes – Degré de séparabilité

A un corps K donné, on associe une clôture algébrique $\overline{K}$ et toute extension algébrique de K sera considérée dans $\overline{K}$.

Définition 7.10. Soit L et M deux extensions d'un même corps K ; alors tout monomorphisme φ de L dans M (Rem. 1.9) tel que $\varphi_{/K} = id_K$ est appelé un **K-monomorphisme** de L dans M.

Remarque 7.11. Les notations seront celles de la définition 7.10.
a) Lorsqu'il n'y a aucune ambiguïté possible, la *restriction surjective* d'un K-monomorphisme $\varphi : L \hookrightarrow M$ (c'est-à-dire le K-isomorphisme de L sur $\varphi(L)$ qui, à tout $x \in L$, associe $\varphi(x)$) sera encore notée φ.
b) Si $\varphi : L \hookrightarrow M$ est un monomorphisme (resp. K-monomorphisme) de L dans M, alors φ est un isomorphisme (resp. K-isomorphisme) si et seulement si φ est surjectif.
c) Si $K \subseteq L \subseteq M$ et si $[L : K]$ est *fini*, alors tout K-monomorphisme $\varphi : L \hookrightarrow M$ tel que $\varphi(L) \subseteq L$ est un K-isomorphisme de L, donc un élément du groupe $G(L : K)$.
En effet, φ est K-linéaire et injectif, par suite, $dim_K L = [L : K] < \infty$ et $\varphi(L) \subseteq L$ impliquent $\varphi(L) = L$, donc φ surjectif.
d) Si φ est un K-monomorphisme de L dans M et si $f(X) \in K[X]$ a une racine α dans L, alors

$$\hat{\varphi}(f(X)) = f(X) \text{ dans } M[X] \quad \text{et} \quad \varphi(\alpha) \text{ est racine de } f(X) \text{ dans } M.$$

En effet, supposons $f(X) = \sum_{0\le i\le m} a_i X^i$ dans $K[X]$, alors

$$\big(\varphi(a_i) = a_i, \forall i (0 \le i \le m)\big) \Longrightarrow \hat{\varphi}\Big(\sum_{0\le i\le m} a_i X^i\Big) = \sum_{0\le i\le m} \varphi(a_i) X^i = f(X).$$

On en déduit que : ($f(X) = (X-\alpha)g(X)$ dans $L[X]$) implique

$$\hat{\varphi}(f(X)) = (X - \varphi(\alpha))\hat{\varphi}(g(X)) = f(X) \text{ dans } M[X],$$

donc $\varphi(\alpha)$ est racine de $f(X)$ dans M.
En appliquant ce résultat au cas où $f(X) = Irr_K(\alpha, X)$, on en déduit que $\varphi(\alpha)$ est un *conjugué* de α dans M (Déf. 2.18).

Proposition 7.12. 1) *Soit $L : K$ une extension de corps* de degré fini, *alors L est une extension normale de K si et seulement si, quelle que soit l'extension M de L, tout K-monomorphisme de L dans M est un K-automorphisme de L, donc un élément de $G(L : K)$.*
2) *Si $L : K$ est une extension normale, de degré fini et si F est un corps intermédiaire : $K \subseteq F \subseteq L$ alors, pour tout K-monomorphisme $\varphi : F \hookrightarrow L$, il existe $\sigma \in G(L : K)$ tel que $\sigma_{/F} = \varphi$.*
En particulier, si des éléments α et β de L sont racines d'un même polynôme irréductible et unitaire de $K[X]$, il existe $\sigma \in G(L : K)$ tel que $\sigma(\alpha) = \beta$.

Démonstration. 1) Par hypothèse, $L : K$ est normale, de degré fini et $K \subset L \subset M$.
Soit φ un K-monomorphisme de L dans M. Etant donné un élément α de L, posons $p_\alpha(X) := Irr_K(\alpha, X)$; alors, d'après la Rem. 7.11, d), $\varphi(\alpha)$ est une racine de $p_\alpha(X)$ dans M. Mais L étant une extension normale de K, $p_\alpha(X)$ est scindé sur L, donc $\varphi(\alpha) \in L$. On en déduit que $\varphi(L) \subseteq L$; de plus, $L : K$ étant de degré fini, $\varphi(L) = L$, donc $\varphi \in G(L : K)$ (Rem. 7.11, c)).
Réciproquement, supposons $L : K$ de degré fini et telle que quels que soient l'extension M de L et le K-monomorphisme φ de L dans M, on ait $\varphi(L) = L$.
Par hypothèse $L : K$ est de degré fini, donc algébrique. On suppose $[L : K] > 1$, on a alors (Th. 2.29),

$$L = K(\alpha_1, \ldots, \alpha_m), \quad m \in \mathbb{N}^* \text{ et } \forall i,\ 1 \le i \le m,\ \alpha_i \text{ algébrique sur} K.$$

Pour tout i, $1 \le i \le m$, soit $p_i(X) := Irr_K(\alpha_i, X)$; posons

$$f(X) := \prod_{1\le i\le m} p_i(X).$$

Soit M un corps de décomposition de $f(X)$ sur K contenant L.
Supposons $M \neq L$; il existe alors, au moins un polynôme $p_i(X)$, $1 \le i \le m$, ayant une racine $\alpha_i' \in M \setminus L$; admettons que $p_1(X)$ vérifie cette propriété. D'après le Th. 2.16, il existe un K-isomorphisme μ de $K(\alpha_1)$ sur $K(\alpha_1')$ tel que $\mu(\alpha_1) = \alpha_1'$.
Or, M est corps de décomposition de $f(X)$ sur $K(\alpha_1)$ et sur $K(\alpha_1')$, donc il existe un automorphisme η de M prolongeant μ (Th. 3.8) ;

$$(\eta_{/K(\alpha_1)} = \mu \text{ et } \mu_{/K} = id_{/K}) \Longrightarrow \eta_{/K} = id_{/K}.$$

Ainsi, $\eta_{/L}$ est un K-monomorphisme de L dans M, donc l'hypothèse implique $\eta(L) = L$, d'où, $\eta(\alpha_1) = \alpha_1' \in L$. On en conclut que $M = L$.
Ainsi L est corps de décomposition de $f(X)$ sur K, donc L est une extension normale sur K (Th. 3.15).

2) Le corps L est une extension de K, normale, de degré fini, donc L est corps de décomposition, sur K, d'un polynôme $f(X) \in K[X] \setminus K$.
L'hypothèse $K \subseteq F \subseteq L$ implique que L est aussi corps de décomposition de $f(X)$ sur F.
Etant donné un K-monomorphisme φ, de F dans L, la restriction surjective de φ que, pour plus de précision, nous noterons ici φ_1, est un K-isomorphisme de F sur $\varphi(F) \subseteq L$; d'autre part (Rem. 7.11, d)),

$$f(X) \in K[X] \Longrightarrow \hat{\varphi}(f(X)) = \hat{\varphi_1}(f(X)) = f(X);$$

on en déduit que L est corps de décomposition de $f(X)$ sur $\varphi(F)$.
Par suite (Th. 3.8), il existe un automorphisme σ de L qui prolonge φ_1, donc $\sigma_{/F} = \varphi_1$.
On en déduit que

$$(\sigma_{/K} = \varphi_{/K} = id_{/K} \Longrightarrow \sigma \in G(L:K)) \text{ et } \sigma_{/F} = \varphi.$$

En particulier, si des éléments α et β de L sont racines d'un même polynôme irréductible de $K[X]$, alors (Th. 2.16), il existe un K-isomorphisme μ de $K(\alpha)$ sur $K(\beta)$ tel que $\mu(\alpha) = \beta$.
Soit j l'injection canonique de $K(\beta)$ dans L; $j \circ \mu$ est un K-monomorphisme de $K(\alpha)$ dans L :

$$K(\alpha) \xrightarrow{\mu} K(\beta) \xrightarrow{j} L.$$

Par suite, il existe $\sigma \in G(L:K)$ tel que $\sigma_{/K(\alpha)} = j \circ \mu$, donc $\sigma(\alpha) = \beta$. □

Proposition 7.13. *Soit $L:K$ une extension de corps* de degré fini *et N la clôture normale de $L:K$ contenue dans $\overline{K}$; alors*
1) *N est obtenue par l'adjonction à K de l'ensemble des racines, dans $\overline{K}$, des polynômes irréductibles de $K[X]$, ayant une racine dans L.*
2) *Tout K-monomorphisme de L dans $\overline{K}$ est un K-monomorphisme de L dans N.*

Démonstration. La proposition est triviale, lorsque $L = K$ (Cf. Exemple 3.14), on suppose donc $[L:K] > 1$.
1) Désignons par K' l'extension de K obtenue par l'adjonction de l'ensemble, noté $\mathcal{R}$, des racines des polynômes irréductibles de $K[X]$ ayant une racine dans L. On a

$$\mathcal{R} \subset \overline{K} \quad \text{et} \quad K \subset L \subseteq K' \subseteq N \subseteq \overline{K}.$$

En effet, quel que soit $\alpha \in L$, α est racine de $p_\alpha(X) = Irr_K(\alpha, X)$, d'où $L \subseteq K'$; d'autre part, l'extension $N : K$ est normale, donc tout polynôme irréductible de $K[X]$ ayant une racine dans $L \subseteq N$ est scindé sur N, ce qui entraîne $K' \subseteq N$.
Or (voir la preuve du Th. 3.17) si l'on écrit

$$L = K(\alpha_1, \ldots, \alpha_m) \quad \text{et} \quad \forall i (1 \leq i \leq m), p_i(X) = Irr_K(\alpha_i, X),$$

alors, N est corps de décomposition, sur K, de $f(X) = \prod_{1 \leq i \leq m} p_i(X)$. Mais la définition de K' implique que $f(X)$ est scindé sur K', d'où $N = K'$ (Th. 3.3).

2) Soit φ un K-monomorphisme de L dans $\overline{K}$.
Quel que soit $\alpha \in L \setminus K$, si $p_\alpha(X) := Irr_K(\alpha, X)$, alors $\varphi(\alpha)$ est une racine de $p_\alpha(X)$ dans $\overline{K}$ (Rem 7.11, d)). Par suite $\varphi(\alpha) \in N$, d'où $\varphi(L) \subseteq N$. □

Définition 7.14. Etant donné une extension de corps $L : K$, de degré fini, le cardinal de l'ensemble des K-monomorphismes de L dans $\overline{K}$ est appelé **degré de séparabilité** de $L : K$ et est noté $[L:K]_s$.

Proposition 7.15. *Soit $L : K$ une extension de corps,* normale et de degré fini *; alors,*

$$[L : K]_s = |\, G(L : K)\,| . \tag{7.7}$$

Démonstration. D'après le 2) de la Prop. 7.13, si $[L : K]$ est fini, alors $[L : K]_s$ est le cardinal de l'ensemble des K-monomorphismes de L dans N, où N est la clôture normale de $L : K$ contenue dans $\overline{K}$.
Lorsque $L : K$ est *normale, de degré fini*, alors $L = N$, donc $[L : K]_s$ est le cardinal de l'ensemble des K-automorphismes de L, d'où
$[L : K]_s = |\, G(L : K)\,| .$ □

Proposition 7.16. *Pour tout $\alpha \in \overline{K}$, $[K(\alpha) : K]_s$ est égal au nombre de racines* distinctes *du polynôme $Irr_K(\alpha, X)$, dans $\overline{K}$; de plus,*

$$[K(\alpha) : K]_s \leq [K(\alpha) : K]$$
$$\textit{et} \qquad [K(\alpha) : K]_s = [K(\alpha) : K] \iff \alpha \textit{ est séparable sur } K.$$

Démonstration. 1°) Posons $p_\alpha(X) := Irr_K(\alpha, X)$.
La clôture normale N de $K(\alpha) : K$, contenue dans $\overline{K}$, est le corps de décomposition de $p_\alpha(X)$ dans $\overline{K}$ (Rem. 3.18, b)).
Si $p_\alpha(X)$ a r racines distinctes, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$, dans $\overline{K}$, on a

$$r \leq deg\, p_\alpha(X) = [K(\alpha) : K] \quad \text{et} \quad N = K(\alpha_1, \alpha_2, \ldots, \alpha_r).$$

Compte tenu de la Prop. 7.13 et de la Rem. 7.11, c), étant donné un
K-monomorphisme φ, de $K(\alpha)$ dans $\overline{K}$, il existe $i\,(1 \leq i \leq r)$ tel que

$$\varphi(\alpha) = \alpha_i.$$

Réciproquement, quel que soit $i\,(1 \leq i \leq r)$, il existe un K-isomorphisme φ_i, de $K(\alpha)$ sur $K(\alpha_i)$ tel que $\varphi_i(\alpha) = \alpha_i$ (Th. 2.16). Notons μ_i l'injection canonique de $K(\alpha_i)$ dans $\overline{K}$:

$$K(\alpha) \xrightarrow{\varphi_i} K(\alpha_i) \xrightarrow{\mu_i} \overline{K};$$

alors $\mu_i \circ \varphi_i$ est un K-monomorphisme de $K(\alpha)$ dans $\overline{K}$, ce qui entraîne

$$[K(\alpha) : K]_s = r \leq [K(\alpha) : K].$$

2°) Compte tenu du résultat précédent, on a

$$\begin{aligned} [K(\alpha) : K]_s = [K(\alpha) : K] &\iff r = deg\, p_\alpha(X) \\ &\iff p_\alpha(X) \text{ séparable sur } K, \\ &\iff \alpha \text{ séparable sur } K. \end{aligned}$$ □

Proposition 7.17. *Soit $L : K$ une extension de corps* de degré fini, *alors $[L : K]_s$ est fini ; on a*

$$[L : K]_s \leq [L : K]$$
$$\textit{et} \qquad [L : K]_s = [L : K] \iff L \textit{ est séparable sur } K.$$

Démonstration. Si $[L : K] = 1$, alors $L = K$ et l'injection canonique de K dans $\overline{K}$ est l'unique K-monomorphisme de K dans $\overline{K}$.
Pour $[L : K] = n > 1$, on raisonne par récurrence sur n.
Soit N la clôture normale de $L : K$ contenue dans $\overline{K}$.

On sait (voir la preuve du Th. 3.17) que N est corps de décomposition sur K d'un polynôme non constant $f(X)$ de $K[X]$, dont tout diviseur, irréductible et unitaire dans $K[X]$, a une racine dans $L \setminus K$. Soit $p(X)$ un tel diviseur de $f(X)$, ayant une racine α dans L, donc

$$p(X) = Irr_K(\alpha, X).$$

N est aussi corps de décomposition de $f(X)$ sur $K(\alpha)$ et on a

$$[L : K(\alpha)] < [L : K].$$

Appliquons l'hypothèse de récurrence à l'extension $L : K(\alpha)$; il existe alors un nombre fini de $K(\alpha)$-monomorphismes de L dans N, que l'on note $\rho_1, \ldots, \rho_q$, où

$$q := [L : K(\alpha)]_s \leq [L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]}.$$

D'autre part, posons $r := deg\, p$, alors le nombre de racines *distinctes* de $p(X)$ dans N est $r' \leq r = [K(\alpha) : K]$ et d'après la Prop. 7.16, on a

$$r' = [K(\alpha) : K]_s.$$

Soit $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_{r'}$, les r' racines distinctes de $p(X)$ dans N, alors (Prop. 7.12.) il existe $\sigma_1, \sigma_2, \ldots, \sigma_{r'}$ dans $G(N : K)$ tels que

$$\sigma_i(\alpha) = \alpha_i, \ \forall i (1 \leq i \leq r').$$

Montrons que les seuls K-monomorphismes de L dans N sont les

$$\varphi_{ij} := \sigma_i \circ \rho_j, \ 1 \leq i \leq r', \ 1 \leq j \leq q.$$

En effet, soit φ un K-monomorphisme de L dans N, alors $\varphi(\alpha)$ est une racine de $p(X)$ dans N, donc il existe $i (1 \leq i \leq r')$ tel que $\varphi(\alpha) = \alpha_i$.
$\psi := \sigma_i^{-1} \circ \varphi$ est un $K(\alpha)$-monomorphisme de L dans N, donc il existe $j (1 \leq j \leq q)$ tel que $\psi = \rho_j$, d'où $\varphi = \sigma_i \circ \rho_j = \varphi_{ij}$. On en déduit que $[L : K]_s = qr'$, d'où

$$[L : K]_s = [L : K(\alpha)]_s [K(\alpha) : K]_s ; \tag{7.8}$$

alors, $([L : K(\alpha)]_s \leq [L : K(\alpha)]$ et $[K(\alpha) : K]_s \leq [K(\alpha) : K]) \Longrightarrow [L : K]_s \leq [L : K]$.
Si $L : K$ est de degré fini et séparable, alors L est une extension simple de K (Th. 3.30). Supposons $L = K(\alpha)$; d'après la Prop. 7.16,

$$L : K \text{ séparable} \Longrightarrow \alpha \text{ séparable sur } K \Longrightarrow [L : K]_s = [L : K].$$

Réciproquement, supposons $[L : K] < \infty$ et $[L : K]_s = [L : K]$.
$L : K$ non séparable implique l'existence d'un élément $\alpha \in L$ non séparable sur K, donc tel que (Prop. 7.16)

$$[K(\alpha) : K]_s < [K(\alpha) : K].$$

Par suite (Rel. (7.8)),

$$[L : K]_s = [L : K(\alpha)]_s [K(\alpha) : K]_s < [L : K(\alpha)][K(\alpha) : K] = [L : K],$$

entraîne une contradiction avec l'hypothèse, d'où L séparable sur K. □

Corollaire 7.18. *Pour tout $\alpha \in \overline{K}$, on a*

$$\alpha \text{ séparable sur } K \Longleftrightarrow K(\alpha) \text{ séparable sur } K.$$

Ce résultat est une conséquence des Prop. 7.16 et 7.17.

Théorème 7.19. *Une extension de corps $L : K$ est séparable si et seulement si le corps L est obtenu par l'adjonction à K d'une famille d'éléments séparables sur K.*

Démonstration. Supposons $L = K(\Lambda)$, où $\Lambda = \{\lambda_i\}_{i\in I}$, I étant un ensemble non vide quelconque.

1) Si $L = K(\Lambda)$ est séparable sur K, alors, par définition, quel que soit $i \in I$, λ_i est séparable sur K.

2) Réciproquement, supposons que pour tout $i \in I$, λ_i est séparable sur K et montrons que $L = K(\Lambda)$ est séparable sur K.

Soit $\alpha \in L = K(\Lambda)$; il existe alors une famille finie d'éléments de Λ, $\{\lambda_{i_1}, \ldots, \lambda_{i_m}\}$, où $m \in \mathbb{N}^*$, telle que $\alpha \in K(\lambda_{i_1}, \ldots, \lambda_{i_m})$.

Si $m = 1$, alors, $\alpha \in K(\lambda_{i_1})$ et λ_{i_1} étant, par hypothèse, séparable sur K, l'extension $K(\lambda_{i_1}) : K$ est séparable (Cor. 7.18), donc α est séparable sur K.

Supposons $m > 1$; par hypothèse, λ_{i_m} est séparable sur K, donc sépérable sur $K(\lambda_{i_1}, \ldots, \lambda_{i_{m-1}})$, par suite (Prop. 7.16)

$$[K(\lambda_{i_1}, \ldots, \lambda_{i_m}) : K(\lambda_{i_1}, \ldots, \lambda_{i_{m-1}})]_s = [K(\lambda_{i_1}, \ldots, \lambda_{i_m}) : K(\lambda_{i_1}, \ldots, \lambda_{i_{m-1}})].$$

De même pour tout $j\,(1 < j \leq m)$, on a

$$[K(\lambda_{i_1}, \ldots, \lambda_{i_j}) : K(\lambda_{i_1}, \ldots, \lambda_{i_{j-1}})]_s = [K(\lambda_{i_1}, \ldots, \lambda_{i_j}) : K(\lambda_{i_1}, \ldots, \lambda_{i_{j-1}})].$$

Compte tenu de la relation (7.8), on obtient

$$[K(\lambda_{i_1}, \ldots, \lambda_{i_m}) : K]_s = [K(\lambda_{i_1}, \ldots, \lambda_{i_m}) : K].$$

Ainsi $K(\lambda_{i_1}, \ldots, \lambda_{i_m})$ est séparable sur K, d'où α séparable sur K.

On en conclut que L est séparable sur K. □

Théorème 7.20. *Une extension de corps $L : K$ est normale, de degré fini et sépérable, si et seulement si L est corps de décomposition sur K d'un polynôme séparable de $K[X]$.*

Démonstration. On sait que si $L : K$ est normale, de degré fini et séparable, alors L est corps de décomposition sur K d'un polynôme séparable de $K[X]$ (Prop. 3.30).

Réciproquement, supposons L corps de décomposition sur K d'un polynôme séparable $f(X) \in K[X]$; alors L est obtenu par l'adjonction à K des racines distinctes de $f(X)$ dans L (Rem. 3.6) :

$$L = K(\alpha_1, \ldots, \alpha_m).$$

Le polynôme $f(X)$ étant séparable sur K, chacune de ses racines distinctes $\alpha_i, 1 \leq i \leq m$, est séparable sur K, donc L est séparable sur K (Th. 7.19). □

En conclusion de ce paragraphe, on obtient la propriété essentielle, suivante.

Théorème 7.21. *Si $L : K$ est une extension de corps* normale *et de* degré fini, *alors le groupe de Galois de $L : K$ est fini et*

$$|\, G(L:K) \,| \leq [L:K]. \tag{7.9}$$

Si de plus l'extension $L : K$ est séparable, *alors*

$$|\, G(L:K) \,| = [L:K] \quad \textit{et} \quad K = Inv_L(G(L:K)). \tag{7.10}$$

Démonstration. L'extension $L : K$ est normale, de degré fini, alors compte tenu des Prop. 7.15 et 7.17, on obtient

$$| G(L:K) | = [L:K]_s \leq [L:K].$$

Si, de plus, l'extension $L : K$ est séparable, la Prop. 7.17 implique

$$| G(L:K) | = [L:K].$$

Il reste à prouver que si $L : K$ est normale, de degré fini et séparable, alors $K = Inv_L(G(L:K))$.
Posons $F := Inv_L(G(L:K)) = \gamma' \circ \gamma(K)$, où (γ, γ') est la correspondance de Galois associée à l'extension $L : K$; alors (Prop. 7.6) :

$$K \subseteq F \subseteq L \text{ et } \gamma(F) = G(L:F) \text{ est un sous-groupe de } G(L:K).$$

De plus (Prop. 7.7, relation (7.5)),

$$F = \gamma' \circ \gamma(K) \Longrightarrow \gamma(F) = \gamma \circ \gamma' \circ \gamma(K) = \gamma(K) = G(L:K),$$
$$\text{d'où} \quad G(L:F) = G(L:K).$$

Or L est corps de décomposition sur K d'un polynôme *séparable* $f(X) \in K[X]$ (Th. 7.20), donc L est aussi corps de décomposition de $f(X)$ sur F. Le polynôme $f(X)$, qui est séparable sur K, est aussi séparable sur F, par suite, comme précédemment, la Prop. 7.17 implique

$$| G(L:F) | = [L:F].$$

On en déduit que $[L:K] = [L:F]$, d'où $F = K$. □

B. Extensions galoisiennes, de degré fini

Définition 7.22. On dit qu'une extension de corps $L : K$ est **galoisienne** (ou que L est galoisienne sur K) si
i) L est algébrique sur K ;
ii) $K = Inv_L(G(L:K))$.

Nous n'étudierons, dans ce chapitre, que les extensions *galoisiennes, de degré fini.* Il existe cependant des extensions galoisiennes de degré infini, par exemple $\overline{\mathbb{Q}} : \mathbb{Q}$ (voir Ex. **6.** à la fin du chapitre).

Remarque 7.23. Une extension de degré fini est algébrique (Th. 2.26), donc $L : K$ est une *extension galoisienne, de degré fini*, si et seulement si elle vérifie :

$$[L:K] < \infty \text{ et } K = Inv_L(G(L:K)).$$

Le Th. 7.21 entraîne l'assertion suivante :

Théorème 7.24. *Toute extension de corps $L : K$, de degré fini, normale et séparable, est galoisienne, de degré fini ; de plus, le groupe de Galois $G(L:K)$ est fini et*

$$| G(L:K) | = [L:K].$$

Le Th. 7.26 (*Théorème d' Artin*) permettra d'établir une réciproque du Th. 7.24 ; une partie de sa démonstration consiste à prouver le résultat suivant, que nous appellerons *Lemme d'Artin.*

Lemme 7.25. Lemme d' Artin
Soit L un corps et G un sous-groupe fini *du groupe Aut L des automorphismes de L. Si l'on pose* $K := Inv_L(G)$, *alors*

$$L : K \text{ est une extension de degré fini et } [L:K] \leq |\, G \,|\,.$$

Démonstration. Soit $n := |\, G \,|$; pour démontrer le lemme, il suffit de prouver que pour tout entier $m > n$, m éléments non nuls de L sont linéairement dépendants sur K.
Supposons $G = \{\sigma_1 = id_L, \sigma_2, \ldots, \sigma_n\}$; étant donné $m > n$ dans $\mathbb{N}$ et $a_1, a_2, \ldots, a_m$ non nuls dans L, considérons le système linéaire et homogène (S) de n équations à m inconnues dans L, dont la $i^{ème}$ équation $(1 \leq i \leq n)$ s'écrit

$$\sum_{1 \leq j \leq m} \sigma_i(a_j) X_j = 0. \tag{7.11}$$

L'hypothèse $m > n$ implique que le système (S) a des solutions *non nulles* $(x_1, x_2, \ldots, x_m) \in L^m$; parmi celles-ci, choisissons une solution, pour laquelle le nombre des $x_j \neq 0$ est *minimal* ; une telle solution non nulle sera dite *minimale*.
Moyennant, éventuellement, une permutation des inconnues $X_j, 1 \leq j \leq m$, on peut supposer $x_1 \neq 0$; alors

$$x_1^{-1}(x_1, x_2, \ldots, x_m) = (1, x_1^{-1}x_2, \ldots, x_1^{-1}x_m)$$

est encore une solution du système (S) ; par suite, dans la solution minimale choisie initialement, on peut supposer que $x_1 = 1$. On a $1 \in K$, démontrons qu'alors, tous les éléments $x_j, 2 \leq j \leq m$, de la solution minimale considérée, sont dans K.
Supposons qu'il existe $j, 2 \leq j \leq m$, tel que $x_j \in L \setminus K$; par exemple, supposons $x_2 \notin K$; il existe alors au moins un entier $k (1 \leq k \leq n)$ tel que $\sigma_k(x_2) \neq x_2$. Pour tout $i (1 \leq i \leq n)$, on a

$$\sigma_k\Big(\sum_{1 \leq j \leq m} \sigma_i(a_j) x_j\Big) = 0 = \sum_{1 \leq j \leq m} \big(\sigma_k \circ \sigma_i(a_j)\big)\sigma_k(x_j). \tag{7.12}$$

G étant un groupe,

$$\sigma_k \in G \Longrightarrow \sigma_k G = G \Longrightarrow \{\sigma_k \circ \sigma_i\}_{1 \leq i \leq n} = \{\sigma_i\}_{1 \leq i \leq n}.$$

On en déduit que,

$$\forall i (1 \leq i \leq n), \sum_{1 \leq j \leq m} \sigma_i(a_j)\sigma_k(x_j) = 0;$$

donc $(1 = \sigma_k(1), \sigma_k(x_2), \ldots, \sigma_k(x_m))$ est une solution non nulle du système (S), par suite, $(0, \sigma_k(x_2) - x_2, \ldots, \sigma_k(x_m) - x_m)$ en est une autre, ce qui contredit la *minimalité* de la solution $(1, x_2, \ldots, x_m)$.
Par suite, dans la solution minimale $(1, x_2, \ldots, x_m)$ du système (S), tous les $x_j, 2 \leq j \leq m$, sont dans K.
Montrons qu'alors, les éléments $a_j, 1 \leq j \leq m$, de L^* sont linéairement dépendants sur K. En effet, on a $\sigma_1 = id_L$, donc la première équation du système (S) donne

$$\sum_{1 \leq j \leq m} a_j x_j = 0 = \sum_{1 \leq j \leq m} x_j a_j,$$

où les x_j sont non tous nuls dans K (en particulier, $x_1 = 1$). On en conclut que

$$dim_K L = [L:K] \leq n = |\, G \,|\,. \qquad \square$$

Théorème 7.26. Théorème d' Artin
Etant donné un corps L et un sous-groupe fini *G du groupe Aut L des automorphismes de L, si l'on pose* $K = Inv_L(G)$, *alors L est une extension de K, de degré fini, normale et séparable telle que*

$$[L:K] = |\, G \,|, \quad G(L:K) = G, \quad \textit{donc } K = Inv_L(G(L:K)).$$

Démonstration. D'après le *Lemme d' Artin* (lemme 7.25) , l'extension $L : K$ est de degré fini et $[L : K] \leq | G |$; L est donc algébrique sur K (Th. 2.26).
Soit $\alpha \in L$ et $p(X) := Irr_K(\alpha, X)$. Supposons

$$p(X) = \sum_{0 \leq i \leq r} a_i X^i, \quad \text{dans} \quad K[X] \setminus K.$$

Pour tout $i (0 \leq i \leq r)$ et tout $\sigma \in G$,

$$a_i \in K = Inv_L(G) \Longrightarrow \sigma(a_i) = a_i ;$$

alors, quel que soit $\sigma \in G$,

$$p(\alpha) = \sum_{0 \leq i \leq r} a_i \alpha^i = 0 \Longrightarrow \sum_{0 \leq i \leq r} a_i (\sigma(\alpha))^i = 0,$$

donc $\sigma(\alpha)$ est racine de $p(X)$. Posons $\Omega_\alpha = \{\sigma(\alpha) \, ; \, \sigma \in G\}$.
Le groupe G étant fini, par hypothèse, l'ensemble Ω_α est une partie finie de L telle que $| \Omega_\alpha | \leq | G |$.
D'autre part, quel que soit $\tau \in G$, $\tau G = G$ entraîne $\tau(\Omega_\alpha) = \Omega_\alpha$, donc $\tau_{/\Omega_\alpha}$ est une *permutation* des éléments de Ω_α. Posons

$$s := | \Omega_\alpha | \quad \text{et} \quad \Omega_\alpha = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s\}, \text{ où } 1 \leq s \leq | G | .$$

Les $\alpha_i (1 \leq i \leq s)$ sont s racines *distinctes* de $p(X)$ dans L, donc

$$s \leq r = deg\, p \quad \text{et} \quad q(X) := \prod_{1 \leq i \leq s} (X - \alpha_i) \text{ divise } p(X) \text{ dans } L[X].$$

Tout élément $\tau \in G$ se prolonge en un automorphisme $\hat{\tau}$ de $L[X]$ et

$$\hat{\tau}(q(X)) = \prod_{1 \leq i \leq s} (X - \tau(\alpha_i)), \text{ dans } L[X].$$

Or τ est une permutation de $\{\alpha_1, \ldots, \alpha_s\}$, d'où

$$\forall \tau \in G, \ \hat{\tau}(q(X)) = q(X).$$

On en déduit que les coefficients du polynôme $q(X)$ sont dans $Inv_L(G) = K$, donc $q(X) \in K[X] \setminus K$. D'autre part, $p(X)$ étant irréductible et unitaire dans $K[X]$,

$$q(X) \text{ divise } p(X) \Longrightarrow q(X) = p(X) \Longrightarrow p(X) = \prod_{1 \leq i \leq s} (X - \alpha_i).$$

On en conclut que, quel que soit $\alpha \in L$, $p(X) := Irr_K(\alpha, X)$ est scindé sur L et n'a que des racines simples dans L, donc L est normale et séparable sur K. De plus, L étant de degré fini sur K, d'après le Th. 7.21, le groupe $G(L : K)$ est fini et plus précisément,

$$| G(L : K) | = [L : K] \ ; \ K = Inv_L(G(L : K)).$$

Utilisons les propriétés de la correspondance de Galois (γ, γ') associée à l'extension $L : K$ (Prop. 7.7) ; on a

$$K = Inv_L(G) = \gamma'(G) \quad \text{et} \quad \gamma(K) = G(L : K);$$
$$(7.4) \Longrightarrow G \subseteq \gamma \circ \gamma'(G) = \gamma(K) = G(L : K),$$
$$\text{d'où} \qquad | G | \leq | G(L : K) | = [L : K].$$

D'après le lemme 7.25, on a $[L : K] \leq | G |$ par suite, $[L : K] = | G |$.
Les groupes G et $G(L : K)$ étant finis,

$$\big(| G | = | G(L : K) | \quad \text{et} \quad G \subseteq G(L : K)\big) \Longrightarrow G = G(L : K). \qquad \square$$

Théorème 7.27. *Pour une extension de corps $L : K$, les trois conditions suivantes sont équivalentes :*
1) *$L : K$ est une extension galoisienne, de degré fini.*
2) *$L : K$ est de degré fini, normale et séparable.*
3) *Le groupe $G(L : K)$ est fini et $K = Inv_L(G(L : K))$.*
De plus, dans ces conditions on a

$$| G(L : K) | = [L : K].$$

Démonstration. D'après les théorèmes 7.24 et 7.26, on a 2) $\Longleftrightarrow$ 3)
et chacune de ces deux conditions implique $| G(L : K) | = [L : K]$.
D'autre part (Rem 7.23), la condition 1) est équivalente à

$$[L : K] < \infty \text{ et } K = Inv_L(G(L : K)).$$

Le théorème 7.24 donne donc aussi 2) $\Longrightarrow$ 1). Démontrons que 1) $\Longrightarrow$ 3), ce qui entraînera l'équivalence des trois conditions énoncées. Compte tenu de l'hypothèse 1), il suffit de prouver que le groupe $G(L : K)$ est fini.
On suppose $[L : K] > 1$; l'hypothèse implique $L : K$ algébrique et de degré fini, donc le corps L est obtenu par l'adjonction à K d'un nombre fini d'éléments, algébriques sur K (Th. 2.29) ; posons

$$L = K(\alpha_1, \ldots, \alpha_m),\ m \in \mathbb{N}^*, \text{ où, } \forall i (1 \leq i \leq m), \alpha_i \text{ est algébrique sur } K.$$

Pour tout $i (1 \leq i \leq m)$, posons $p_i(X) = Irr_K(\alpha_i, X)$ et considérons

$$f(X) = \prod_{1 \leq i \leq m} p_i(X), \quad \text{dans } K[X] \setminus K.$$

Si $f(X)$ a r racines (distinctes ou confondues) dans L, alors $\alpha_1, \ldots, \alpha_m$ font partie de ces racines, d'où $r \geq m$; en notant $\{\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_r\}$ l'ensemble de toutes les racines (distinctes ou confondues) de $f(X)$ dans L, on peut écrire, dans $L(X)$:

$$f(X) = g(X) \prod_{1 \leq i \leq r} (X - \alpha_i),$$

où $g(X) \in L[X]$ et n'a pas de racine dans L.
Pour tout $\sigma \in G(L : K)$, soit $\hat{\sigma}$ l'isomorphisme de $L[X]$ prolongeant σ ; alors,

$$\hat{\sigma}(f(X)) = f(X) = \hat{\sigma}(g(X)) \prod_{1 \leq i \leq r} (X - \sigma(\alpha_i)).$$

On en déduit que, pour tout $i (1 \leq i \leq r)$, $\sigma(\alpha_i)$ est encore racine de $f(X)$ dans L, donc σ permute les éléments $\alpha_1, \alpha_2, \ldots, \alpha_r$ de L, alors

$$\prod_{1 \leq i \leq r} (X - \sigma(\alpha_i)) = \prod_{1 \leq i \leq r} (X - \alpha_i) \Longrightarrow \hat{\sigma}(g(X)) = g(X) \Longrightarrow g(X) \in K[X],$$

car $K = Inv_L(G(L : K))$, par hypothèse.
Soit E un corps de décomposition de $f(X)$ sur K, contenant $L = K(\alpha_1, \ldots, \alpha_m)$,
$1 \leq m \leq r$; alors, l'extension $E : K$ est normale, de degré fini (Th. 3.15), de plus (Th. 7.21), le groupe $G(E : K)$ est fini et

$$| G(E : K) | \leq [E : K].$$

Soit $\eta \in G(E : K)$ et $\hat{\eta}$ l'isomorphisme de $E[X]$ prolongeant η. Les polynômes $f(X)$ et $g(X)$ étant dans $K[X]$,

$$\hat{\eta}(f(X)) = f(X), \qquad \hat{\eta}(g(X)) = g(X),$$

$$\text{d'où, } \quad \hat{\eta}\Big(\prod_{1 \leq i \leq r} (X - \alpha_i)\Big) = \prod_{1 \leq i \leq r} (X - \eta(\alpha_i)) = \prod_{1 \leq i \leq r} (X - \alpha_i).$$

Ainsi, quel que soit $i\,(1 \leq i \leq r)$, $\eta(\alpha_i) \in L$, par suite,

$$L = K(\alpha_1, \ldots, \alpha_m) \Longrightarrow \eta(L) \subseteq L.$$

On en déduit que $\eta_{/L} \in G(L:K)$ (Rem. 7.11, c)). Montrons alors, que

$$\begin{aligned} \phi : G(E:K) &\longrightarrow G(L:K) \\ \eta &\longmapsto \eta_{/L} \end{aligned}$$

est une application surjective. E peut être considéré comme corps de décomposition de $f(X)$ sur L ; alors tout $\sigma \in G(L:K)$ se prolonge en un K-automorphisme η de E (Th. 3.8) ; $\eta \in G(E:K)$ et $\eta_{/L} = \sigma$, donc l'application ϕ est surjective. On en déduit que

$$G(E:K) \text{ fini} \Longrightarrow G(L:K) \text{ fini},$$

d'où 1) $\Longrightarrow$ 3).
D'autre part, puisque 3) $\Longrightarrow$ 2), on remarque que, dans le contexte ci-dessus, on a nécessairement, $L = E$ et $f(X)$ séparable sur K. □

Corollaire 7.28. *1) Une extension de corps $L : K$ est galoisienne, de degré fini si et seulement si L est corps de décomposition sur K d'un polynôme séparable de $K[X]$.*
2) Toute extension galoisienne, de degré fini, est une extension simple, algébrique (la réciproque est fausse – voir exemple ci-dessous).

Démonstration. 1) : la propriété énoncée découle directement des Th. 7.20 et 7.27.
2) : le Th. 7.27 montre que toute extension galoisienne, de degré fini est séparable, c'est donc une extension algébrique simple, d'après le *Théorème de l'élément primitif* (Th. 3.31). □

Exemple 7.29. 1) Reprenons les exemples 7.4 ; il est immédiat que les extensions $\mathbb{C} : \mathbb{R}$ et $\mathbb{Q}(\sqrt{3}) : \mathbb{Q}$ sont galoisiennes, de degré fini (Cor. 7.28, 1)).
Par contre, l'extension $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ n'est pas une extension galoisienne, car ce n'est pas une extension normale (Cf. exemples 3.19) ; on a d'ailleurs,

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \quad \text{et} \quad |\, G(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) \,| = 1.$$

Cet exemple montre qu'une extension simple, algébrique n'est pas nécessairement galoisienne (Cf. Cor. 7.28, 2)).

2) Pour un entier $n > 1$, considérons la $n^{ème}$ extension cyclotomique de $\mathbb{Q}$, c'est-à-dire (Déf. 6.10) :

$$\mathbb{Q}(\omega), \quad \text{où } \omega \text{ est une racine } n^{ème} \text{ primitive de l'unité de } \mathbb{Q}.$$

$\mathbb{Q}(\omega)$ est corps de décomposition sur $\mathbb{Q}$ du polynôme séparable $X^n - 1$
de $\mathbb{Q}[X]$ (Prop. 6.8), donc l'extension $\mathbb{Q}(\omega) : \mathbb{Q}$ est galoisienne, de degré fini (Cor. 7.28.).
On en déduit que (Th. 6.19 et Th. 7.27)

$$|\, G(\mathbb{Q}(\omega) : \mathbb{Q}) \,| = [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n).$$

Déterminons les éléments du groupe $G := G(\mathbb{Q}(\omega) : \mathbb{Q})$.
Tout élément $\sigma \in G$ étant un automorphisme de $\mathbb{Q}(\omega)$ tel que $\sigma_{/\mathbb{Q}} = id_{\mathbb{Q}}$, la donnée de $\sigma(\omega)$ détermine σ et $\sigma(\omega)$ est nécessairement une racine $n^{ème}$ primitive de l'unité de $\mathbb{Q}$.
Il en résulte que tout élément σ de G est une permutation de l'ensemble Ω_n des racines $n^{ème}$ primitives de l'unité. Or, étant donné $\omega \in \Omega_n$, on a

$$\Omega_n = \{\omega^k \,;\, 1 \leq k \leq n-1,\ k \wedge n = 1\},$$

et quel que soit $k' \in \mathbb{N}$, $\omega^{k'} = \omega^k \iff k' \equiv k \pmod{n}$.
On en déduit que, pour tout $\sigma \in G$, il existe un unique entier k tel que

$$1 \leq k \leq n-1,\ k \wedge n = 1 \quad \text{et} \quad \sigma(\omega) = \omega^k.$$

Pour ω fixé dans Ω_n, notons σ_k l'unique élément de G tel que $\sigma_k(\omega) = \omega^k$.
Soit $\omega^j \in \Omega_n$, alors $j \neq k \Longrightarrow \sigma_j \neq \sigma_k$ et

$$\sigma_j \circ \sigma_k(\omega) = \omega^{kj} = \omega^{jk} = \sigma_k \circ \sigma_j(\omega).$$

Le groupe de Galois $G(\mathbb{Q}(\omega) : \mathbb{Q})$ est donc un groupe *abélien* ([12], Déf. 1.5) ; de plus, G_n désignant le groupe des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (Cf. Ex.**1.**, Ch. 6), on vérifie facilement que l'application

$$g : G(\mathbb{Q}(\omega) : \mathbb{Q}) \longrightarrow G_n \text{ telle que } g(\sigma_k) = \bar{k},\ \forall \sigma_k \in G(\mathbb{Q}(\omega) : \mathbb{Q}),$$

est un isomorphisme de groupes, d'où l'énoncé suivant.

Quel que soit l'entier $n > 1$, le groupe de Galois de la $n^{ème}$ extension cyclotomique de $\mathbb{Q}$, est isomorphe au groupe G_n des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Théorème 7.30. *Pour une extension de corps $L : K$, les deux conditions suivantes sont équivalentes :*
1) $L : K$ est galoisienne, de degré fini.
2) $L : K$ est de degré fini et la correspondance de Galois définit une bijection de l'ensemble $\mathcal{F}$ des corps intermédiaires sur l'ensemble $\mathcal{H}$ des sous-groupes de $G(L : K)$.

Démonstration. Soit (γ, γ') le couple d'applications définissant la correspondance de Galois associée à l'extension $L : K$ (Déf. 7.8).
1) $\Longrightarrow$ 2) : L'hypothèse implique que le groupe $G(L : K)$ est fini (Th. 7.27). Soit H un sous-groupe de $G(L : K)$; H est alors un sous-groupe *fini* du groupe *Aut* L des automorphismes du corps L.
Posons $F = Inv_L(H) = \gamma'(H)$; d'après le Théorème d'Artin (Th. 7.26), on a $H = G(L : F)$, donc

$$H = G(L : Inv_L(H)) = \gamma \circ \gamma'(H), \text{ d'où } \gamma \circ \gamma' = id_{\mathcal{H}}.$$

Considérons maintenant, un élément quelconque $F \in \mathcal{F}$; on a

$$K \subseteq F \subseteq L.$$

On déduit de l'hypothèse 1) (Cor. 7.28) que L est corps de décomposition, sur K, d'un polynôme séparable $f(X) \in K[X]$. Mais L est aussi corps de décomposition de $f(X)$ sur F ; par suite (Th. 7.27),

$$F = Inv_L(G(L : F)) = \gamma' \circ \gamma(F), \text{ d'où } \gamma' \circ \gamma = id_{\mathcal{F}}.$$

2) $\Longrightarrow$ 1) : $[L : K]$ fini implique L algébrique sur K et

$$\gamma' \circ \gamma = id_{\mathcal{F}} \Longrightarrow K = Inv_L(G(L : K)),$$

donc $L : K$ est galoisienne, de degré fini. □

Remarque 7.31. Le Th. 7.30 permet de donner une autre justification à la propriété 2) du Cor. 7.28 ; en effet, si $L : K$ est galoisienne, de degré fini, alors le groupe $G(L : K)$ est fini (Th. 7.27), donc il n'a qu'un nombre fini de sous-groupes et la correspondance de Galois associée à $L : K$ étant une bijection (Th. 7.30), il n'existe qu'un nombre fini de corps intermédiaires, ainsi, $L : K$ est une extension simple (Th. 2.30).

C. Théorème fondamental de Galois

Rappel de notations concernant les groupes :
Etant donné un groupe G et un sous-groupe H de G,
$[G : H]$ désigne *l'indice* de H dans G ([12], p.76). Si G est fini, alors

$$| G | = | H | [G : H].$$

$H \lhd G$ exprime que H est *normal* (ou *distingué*) dans G ([12], p.136).
Dans ce cas, le *groupe quotient* de G par H sera noté G/H ([12], p.137).

Théorème 7.32. Théorème fondamental de Galois
Soit $L : K$ une extension de corps galoisienne, *de* degré fini. *Si F est un corps intermédiaire pour cette extension, alors*
1) *$L : F$ est une extension galoisienne, de degré fini.*
2) $[F : K] = [G(L : K) : G(L : F)]$.
3) *Pour l'extension de degré fini $F : K$, les trois conditions suivantes sont équivalentes :*
i) *$F : K$ est une extension normale.*
ii) $G(L : F) \lhd G(L : K)$.
iii) *$F : K$ est une extension galoisienne.*
De plus, dans ces conditions, on a $G(F : K) \simeq G(L : K)/G(L : F)$.

Démonstration. 1) $(K \subseteq F \subseteq L$ et $[L : K] < \infty) \Longrightarrow [L : F] < \infty$, donc $L : F$ est algébrique, de degré fini. D'autre part, $L : K$ est galoisienne, de degré fini, d'où (Th. 7.30),

$$F = \gamma' \circ \gamma(F) = Inv_L(G(L : F)).$$

Ainsi, $L : F$ est galoisienne, de degré fini (Rem. 7.23).

2) $L : K$ et $L : F$ étant galoisiennes, de degré fini, les groupes $G(L : K)$ et $G(L : F)$ sont finis (Th. 7.27) et

$$| G(L : K) | = [L : K], \quad | G(L : F) | = [L : F].$$
$$\text{Par suite,} \quad [L : K] = [L : F][F : K] \iff | G(L : K) | = | G(L : F) | \, [F : K];$$
$$\text{d'où} \quad [F : K] = [G(L : K) : G(L : F)].$$

3) On a $(K \subseteq F \subseteq L$ et $[L : K] < \infty) \Longrightarrow [F : K] < \infty$.
i) $\Longrightarrow$ *ii)* : Soit $\sigma \in G(L : K)$; alors $\sigma_{/F}$ est un K-monomorphisme de F dans L. Par hypothèse, l'extension de degré fini $F : K$ est normale, donc (Prop. 7.12), $\sigma_{/F} \in G(F : K)$.

$$\varphi : G(L : K) \longrightarrow G(F : K)$$
$$\sigma \longmapsto \sigma_{/F}$$

est alors un morphisme de groupes et

$$Ker\,\varphi = \{\sigma \in G(L : K) \,;\, \sigma_{/F} = id_F\} = G(L : F) \quad \Longrightarrow \quad G(L : F) \lhd G(L : K).$$

ii) $\Longrightarrow$ *iii)* : D'après la propriété 1), l'extension $L : F$ est galoisienne, de degré fini. Posons $H = G(L : F)$; en tenant compte de l'hypothèse *ii)* et du Th. 7.27, on a

$$H \lhd G(L : K) \quad \text{et} \quad F = Inv_L(H);$$

$$\text{alors,} \quad \forall \sigma \in G(L : K), \quad \sigma H \sigma^{-1} = H \Longrightarrow F = Inv_L(\sigma H \sigma^{-1}).$$
$$Inv_L(\sigma H \sigma^{-1}) = \{x \in L \,;\, \forall \tau \in H, \, \sigma\tau\sigma^{-1}(x) = x\}$$
$$= \{x \in L \,;\, \forall \tau \in H, \, \tau(\sigma^{-1}(x)) = \sigma^{-1}(x)\}$$
$$= \{x \in L \,;\, \sigma^{-1}(x) \in Inv_L(H)\}$$
$$= \sigma(Inv_L(H)) = \sigma(F),$$
$$\text{d'où,} \quad G(L : F) \lhd G(L : K) \iff \forall \sigma \in G(L : K), \, \sigma(F) = F,$$
$$\iff \forall \sigma \in G(L : K), \, \sigma_{/F} \in G(F : K).$$

En considérant de nouveau, le morphisme de groupes

$$\varphi : G(L : K) \longrightarrow G(F : K)$$
$$\sigma \longmapsto \sigma_{/F},$$

on obtient : $Inv_F(Im\varphi) = \{x \in F\ ;\ \forall \sigma \in G(L:K),\ \sigma(x) = x\} = K$.
L'extension $L : K$ étant galoisienne, de degré fini, le groupe $G(L : K)$ est fini, par suite $Im\varphi$ est un sous-groupe fini de $G(F : K) \subseteq Aut F$.
L'application du Théorème d' Artin (Th. 7.26) donne

$$|\, Im\varphi\,| = [F : K] \text{ et } Im\varphi = G(F : K), \quad \text{d'où} \quad K = Inv_F(G(F : K)).$$

On en conclut que l'extension de degré fini $F : K$ est galoisienne et

$$Im\varphi \simeq G(L : K)/Ker\varphi \iff G(F : K) \simeq G(L : K)/G(L : F).$$

iii) $\Longrightarrow$ *i)* : Si l'extension de degré fini $F : K$ est galoisienne, alors $F : K$ est une extension normale (Th. 7.27). □

Remarque 7.33. Dans de nombreux ouvrages, le théorème, dit « *Théorème fondamental de Galois* », regroupe les théorèmes 7.30 et 7.32 ; c'est en vue d'un exposé plus clair des résultats concernés et de leurs preuves, que l'on a préféré les séparer en deux énoncés.

3. Applications de la Théorie de Galois

A. Rappels concernant les groupes finis

Si G est un groupe fini, le cardinal de G, appelé *ordre* de G, sera noté $o(G)$.
1°) Si $o(G) > 1$ et si p est un nombre premier divisant $o(G)$, il existe alors n et s uniques dans $\mathbb{N}^*$, tels que

$$o(G) = sp^n \quad et \quad p \nmid s.$$

Dans ce cas ([12], Th. de Sylow), quel que soit l'entier $r (1 \leq r \leq n)$ il existe au moins un sous-groupe de G, d'ordre p^r.
Pour $r = n$, un sous-groupe de G, d'ordre p^n est appelé un p-sous-groupe de Sylow de G.
Si S est un p-sous-groupe de Sylow de G, alors $[G : S]$ désignant l'indice de S dans G, on a

$$[G : S] = s, \quad \text{donc} \quad p \nmid [G : S].$$

2°) Si $o(G) = p^r$, où p est un nombre premier et $r > 0$, on dit que G est un p-groupe fini et dans ce cas, il existe ([12], Ch. VII) une famille $\{G_i\}_{1 \leq i \leq r}$ de sous groupes de G telle que

$$(1) = G_0 \subset G_1 \subset \cdots \subset G_{r-1} \subset G_r = G \tag{7.13}$$

$$\text{et} \quad \forall i (1 \leq i \leq r),\ o(G_i) = p^i,\ G_{i-1} \lhd G_i. \tag{7.14}$$

Cette propriété exprime que tout p-groupe fini est résoluble ([12], Prop. 7.35).

B. Construction des polygones réguliers

On suppose connue, la notion de polygone régulier, à n côtés et n sommets, pour tout entier $n \geq 3$; on notera P_n un tel polygone.
En particulier, P_3 est le triangle équilatéral, P_4 est le carré, P_5 est le pentagone (régulier), P_6 est l'hexagone (régulier).
Dès l'antiquité, les Grecs savaient construire, *par la règle et le compas*, (Cf. Ch. 2) les polygones P_n, pour $n = 3, 5, 15$ et un polygone P_{2n}, connaissant P_n. Puis, pendant environ 2000 ans, aucun progrès ne fut fait à ce sujet. Mais le 30 mars 1796, Gauss découvrit, en le prouvant ([24]), que le polygone régulier à 17 côtés était constructible par la règle et

le compas. Il n'avait que 19 ans ! Sa joie fut telle, qu'il décida ce jour-là, de consacrer sa vie aux mathématiques, alors que jusque là, il hésitait encore entre cette discipline et la philosophie.
Ce paragraphe a pour but la caractérisation des entiers $n \geq 3$ pour lesquels le polygone P_n est *constructible par la règle et le compas* ; c'est l'objet du Th. 7.40, justement appelé *Théorème de Gauss*.
Pour alléger le texte, nous dirons qu'un polygone P_n est *constructible*, s'il est constructible par la règle et le compas.

Remarque 7.34. On rappelle que dans le « plan complexe », c'est-à-dire le plan affine euclidien $\mathbb{R}^2$ rapporté à un repère orthonormé Oxy, les images des racines $n^{èmes}$ de l'unité, dans $\mathbb{C}$ (Ch. 6), forment les sommets d'un polygone P_n.
Il en résulte qu'un polygone P_n est constructible, si et seulement si on sait construire, dans le plan affine, orthonormé $\mathbb{R}^2$, le point M de coordonnées $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$, à partir des points $(0,0)$ et $(0,1)$,donc l'angle $\widehat{Ox,OM} = \frac{2\pi}{n}$, défini à $2k\pi$ près (Cf. Ch. 2).

La construction des polygones P_3, P_4, P_6 est supposée connue.
Si l'on considère un polygone P_n, il est entendu que $n \geq 3$.

Lemme 7.35. *Si P_n est un polygone constructible, il en est de même de P_{2n}. En particulier, tout polygone P_{2^r}, $r \geq 2$ dans $\mathbb{N}$, est constructible.*

Démonstration. Dire que le polygone P_n est constructible, c'est dire que, dans le plan $\mathbb{R}^2$, le point M du cercle trigonométrique tel que

$$\widehat{Ox,OM} = \frac{2\pi}{n}$$

est constructible (Rem. 7.34) ; alors, sachant construire la bissectrice d'un angle par la règle et le compas, on en déduit le point M' du cercle trigonométrique tel que

$$\widehat{Ox,OM'} = \frac{2\pi}{2n},$$

d'où le polygone P_{2n}.

En particulier, ayant construit le cube, c'est à dire $P_4 = P_{2^2}$, on peut construire P_{2^3} et par récurrence sur r, on prouve que tout polygone P_{2^r} est constructible, pour tout entier $r \geq 2$. □

Lemme 7.36. *Soit m et n dans $\mathbb{N}^*$.*
1) *Si le polygone P_n est constructible et si $m \mid n$ et $m \geq 3$, alors le polygone P_m est constructible.*
2) *Si $m \wedge n = 1$ et si P_m et P_n sont constructibles, alors P_{mn} aussi.*

Démonstration. 1) Le cas $m = n$ étant sans intérêt, on suppose $m \neq n, m \mid n$, et $m \geq 3$, donc il existe un entier $d > 1$ tel que $n = dm$.
On construit alors P_m à partir de P_n en joignant les sommets du polygone P_n, « d à d ».
En particulier, si $n = 2m$, $m \geq 3$, on construit P_m à partir de P_n en joignant « 2 à 2 » les sommets de P_n.

2) Si $m \wedge n = 1$, il existe alors a, b dans $\mathbb{Z}$ (Th. de Bezout) tels que $am + bn = 1$, d'où

$$\frac{1}{mn} = a\frac{1}{n} + b\frac{1}{m}.$$

On en déduit que si l'on sait construire P_m et P_n, donc, sur le cercle trigonométrique, les points d'angle polaire $\frac{2\pi}{m}$ et $\frac{2\pi}{n}$, alors on sait construire le point d'angle polaire $a\frac{2\pi}{n}+b\frac{2\pi}{m}$, puisque a et b sont des entiers ; d'où la construction de P_{mn}. □

Proposition 7.37. *Soit $n=2^r p_1^{k_1}p_2^{k_2}\dots p_s^{k_s}\geq 3$, dans $\mathbb{N}^*$, où $r\geq 0$ et pour $1\leq j\leq s$, les p_j, sont des nombres premiers impairs, distincts, les $k_j>0$; alors P_n est constructible si et seulement si $P_{p_j^{k_j}}$ est constructible, pour tout $j(1\leq j\leq s)$.*

Ce résultat se déduit directement des lemmes 7.35 et 7.36

On est ainsi ramené à étudier la construction des polygones P_{p^k}, pour p premier *impair*, $k\in\mathbb{N}^*$.

Lemme 7.38. *Soit p un nombre premier impair et $k\in\mathbb{N}^*$; si le polygone P_{p^k} est constructible, alors nécessairement, $k=1$ et $p-1$ est une puissance de 2.*

Démonstration. La construction du polygone P_{p^k} équivaut à la construction du point $M(\cos\frac{2\pi}{p^k},\sin\frac{2\pi}{p^k})$, image dans le plan complexe, de la racine

$p^{k^{ème}}$ primive de l'unité, $\omega=\cos\frac{2\pi}{p^k}+i\sin\frac{2\pi}{p^k}$, où $i^2=-1$, dans $\mathbb{C}$.

De l'application du Th. 2.42, avec $K_0=\mathbb{Q}$ et $\mathcal{P}_0=\{(0,0),(1,0)\}$, on déduit que, si le point M est constructible, alors

$$[\mathbb{Q}(\cos\tfrac{2\pi}{p^k},\sin\tfrac{2\pi}{p^k}):\mathbb{Q}] \quad \text{est une puissance de 2.}$$

$$\text{Supposons} \quad [\mathbb{Q}(\cos\tfrac{2\pi}{p^k},\sin\tfrac{2\pi}{p^k}):\mathbb{Q}]=2^r,\ r\in\mathbb{N}^*;$$

$$\text{alors,} \quad [\mathbb{Q}(\cos\tfrac{2\pi}{p^k},\sin\tfrac{2\pi}{p^k},i):\mathbb{Q}]=2^{r+1}.$$

$$\text{Par suite,} \quad \omega\in\mathbb{Q}(\cos\tfrac{2\pi}{p^k},\sin\tfrac{2\pi}{p^k},i)\Longrightarrow[\mathbb{Q}(\omega):\mathbb{Q}]\mid 2^{r+1},$$

donc $[\mathbb{Q}(\omega):\mathbb{Q}]$ est une puissance de 2. Or (Th. 6.19),

$$[\mathbb{Q}(\omega):\mathbb{Q}]=\varphi(p^k)=p^{k-1}(p-1)$$

et par hypothèse, p est impair, donc $p^{k-1}(p-1)$ est une puissance de 2 implique

$$k=1 \quad \text{et} \quad p-1 \text{ est une puissance de 2.}$$

□

On remarque qu'en particulier, les nombres premiers $p=3, p=5$, sont tels que $p-1$ est une puissance de 2 ; le Théorème de Gauss (Th. 7.40) précisera l'expression des nombres premiers p tels que le polygône P_p est constructible.

Le lemme suivant utilise le Th. 2.49.

Lemme 7.39. *Soit K_0 le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points d'une partie $\mathcal{P}_0$ de l'espace affine, orthonormé $\mathbb{R}^2$, contenant $(0,0)$ et $(1,0)$.*
Si $L\subset\mathbb{R}$ est une extension normale *de K_0 telle que $[L:K_0]=2^r$, où $r\in\mathbb{N}^*$, alors tout point de coordonnées $(x,y)\in L\times L$ peut être construit à partir de $\mathcal{P}_0$.*

Démonstration. $K_0 \subset \mathbb{R} \Longrightarrow car K_0 = 0$.
Par suite, le corps K_0 est parfait. On en déduit que l'extension normale, de degré fini $L : K_0$ est séparable, donc galoisienne de degré fini (Th. 7.27) ; alors, si $G := G(L : K_0)$,

$$[L : K_0] = 2^r \Longrightarrow o(G) = 2^r ;$$

G est un 2-groupe fini. On en déduit (voir Rappels, par. **A.** précédent) qu'il existe une famille $\{G_i\}_{1 \leq i \leq r}$ de sous-groupes de G telle que

$$(1) = G_0 \subset G_1 \subset \cdots \subset G_{r-1} \subset G_r = G$$
$$\text{et} \quad \forall i (1 \leq i \leq r),\ o(G_i) = 2^i,\ G_{i-1} \lhd G_i, \text{ donc } [G_i : G_{i-1}] = 2.$$

En posant, pour tout $i (1 \leq i \leq r)$, $K_i = Inv_L(G_{r-i})$, on obtient, en application du Théorème fondamental de Galois (Th. 7.32), une chaîne finie de corps intermédiaires entre $K_0 = Inv_L(G_r)$ et $L = Inv_L(G_0)$, telle que

$$K_0 \subset K_1 \subset \cdots \subset K_r = L \qquad \text{et} \qquad \forall i (1 \leq i \leq r), [K_i : K_{i-1}] = 2.$$

Par suite, tout point dont les coordonnées sont dans L, est constructible à partir de $\mathcal{P}_0$ (Th.2.49.). □

Théorème 7.40. Théorème de Gauss
Le polygone P_n peut être construit par la règle et le compas si et seulement si

$$n = 2^r p_1 p_2 \cdots p_s, \tag{7.15}$$

où r, s sont des entiers positifs ou nuls et pour $s \geq 1$, les p_j, $1 \leq j \leq s$, sont des nombres premiers distincts tels que

$$p_j = 2^{2^{r_j}} + 1, \quad r_j \in \mathbb{N}. \tag{7.16}$$

Démonstration. Supposons le polygone P_n constructible et

$$n = 2^r p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \geq 3, \quad \text{dans } \mathbb{N}.$$

r et s sont des entiers positifs ou nuls et (lemme 7.38) pour $s \geq 1$,

$$\forall j (1 \leq j \leq s),\ k_j = 1 \quad \text{et} \quad p_j - 1 \text{ est une puissance de 2;}$$

Par suite, pour tout $j (1 \leq j \leq s)$, il existe $\alpha_j \in \mathbb{N}^*$ tel que

$$p_j - 1 = 2^{\alpha_j} \quad \text{et} \quad n = 2^r p_1 \cdots p_r \text{ (Rel. (7.15)).}$$

Pour $1 \leq j \leq s$, supposons que α_j ait un diviseur *impair*, $a > 1$.
Il existe alors $d \in \mathbb{N}^*$, tel que $\alpha_j = da$, d'où

$$p_j = (2^d)^a + 1 = (2^d + 1)\Big(\sum_{0 \leq l \leq a-1} (-1)^l 2^{dl}\Big),$$

ce qui est contraire à l'hypothèse p_j premier. On en déduit que pour tout $j (1 \leq j \leq s)$, α_j est une puissance de 2, d'où la relation (7.16) :

$$p_j = 2^{2^{r_j}} + 1, \quad r_j \in \mathbb{N}.$$

Réciproquement, démontrons que pour un entier $n \geq 3$ satisfaisant aux conditions (7.15) et (7.16), le polygone P_n est constructible.

Compte tenu de la Prop. 7.37, il suffit de montrer que, pour tout $j (1 \leq j \leq s)$, le polygone P_{p_j} est constructible. On est ramené à prouver que, d'une façon générale, si p est un nombre premier tel que $p = 2^\alpha + 1$ et α est une puissance de 2, alors le polygone P_p est constructible. Il s'agit de montrer que, pour un tel nombre premier p, on peut construire par la règle et le compas, l'image M de la racine $p^{ème}$ de l'unité, $\omega = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p} \in \mathbb{C}$.

On remarque que la connaissance du point H de coordonnées $(\cos\frac{2\pi}{p}, 0)$ suffit pour construire le point M, donc le polygone P_p. Posons $K = \mathbb{R} \cap \mathbb{Q}(\omega)$; on a

$$\mathbb{Q} \subset K \subset \mathbb{Q}(\omega) \quad \text{et} \quad \cos\frac{2\pi}{p} = \frac{\omega + \omega^{-1}}{2} \in K ;$$

alors, $\mathbb{Q}(\omega) = K(i)$, où $i^2 = -1$ dans $\mathbb{C}$, implique

$$[\mathbb{Q}(\omega) : K] = [K(i) : K] = 2.$$

Mais ω est une racine $p^{ème}$ primitive de l'unité de $\mathbb{Q}$, donc

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(p) = p - 1 = 2^\alpha ;$$

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\omega) : K][K : \mathbb{Q}] \Longrightarrow [K : \mathbb{Q}] = 2^{\alpha - 1}.$$

L'extension $\mathbb{Q}(\omega) : \mathbb{Q}$ est galoisienne de degré fini et son groupe de Galois est abélien (Exemple 7.29, 2)), d'où

$$G(\mathbb{Q}(\omega) : K) \lhd G(\mathbb{Q}(\omega) : \mathbb{Q}).$$

D'après le Théorème fondamental de Galois (Th. 7.32), K est alors une extension *normale* de $\mathbb{Q}$ et d'après le lemme 7.39, le point $H(\cos\frac{2\pi}{p}, 0)$ est constructible à partir des points $(0,0)$ et $(0,1)$. □

Remarque 7.41. a) Le Théorème de Gauss nous ramène à un problème de Théorie des Nombres, à savoir :

Pour quelles valeurs de $n \in \mathbb{N}$, *l'entier* $F_n := 2^{2^n} + 1$, *appelé* $n^{ème}$ **nombre de Fermat**, *est-il un nombre premier* ?

L'appellation « nombre de Fermat » est justifiée par le fait que dès 1640, le mathématicien Pierre Fermat note que

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

sont des nombres premiers.

Fermat avait conjecturé que, quel que soit n, F_n était premier, mais en 1732, Euler démontra que F_5 n'était pas un nombre premier, plus précisément ([38]),

$$F_5 = 641 \times 6700417.$$

Aujourd'hui, malgré tous les moyens mis en oeuvre par les spécialistes de la question, on ne connaît toujours pas de nombre de Fermat *premier*, autre que les F_n, $0 \leq n \leq 4$, signalés par Pierre de Fermat.

La recherche de la factorialité ou de la primalité des nombres de Fermat reste un problème d'actualité pour les théoriciens des nombres.

Il existe une liste (qui s'allonge progressivement) de nombres de Fermat, dont on a prouvé qu'ils n'étaient pas premiers, on dit que ce sont des nombres de Fermat *composés*. Mais la factorisation complète de la plupart d'entre eux n'est pas connue, car les nombres de Fermat croissent très vite, ce qui rend difficile la recherche de leurs facteurs premiers. Actuellement, les seuls nombres de Fermat composés, dont a obtenu la factorisation complète, sont

$$F_5,\ F_6,\ F_7,\ F_8,\ F_9 \text{ et } F_{11}.$$

La factorisation de F_7 n'est connue que depuis 1971 et celle de F_8, depuis 1982 ([38]).

b) Le Théorème de Gauss pose un second problème, qui est celui de la méthode géométrique de construction des polygones théoriquement constructibles par la règle et le compas.
On considère essentiellement les polygones P_p, où p est un nombre premier de Fermat.
Pour P_5 la méthode est élémentaire (Cf. Ex. **19.**, Ch. 7).
Pour P_{17} il existe plusieurs méthodes de construction ([45]), dont la première fut publiée par Huguenin en 1803.
La construction géométrique des polygones P_{257} et P_{65537} n'est pas vraiment d'un grand intérêt, signalons cependant, que
– pour P_{257}, un procédé de construction a été publié en 1832, par Richelot ;
– pour P_{65537}, Bell ([6]) raconte qu'une méthode de construction aurait été trouvée par un américain, au bout de 20 années de recherche !
En Allemagne, le Professeur Hermes von Lingen a travaillé 10 ans sur la question ; ses manuscrits sont probablement conservés à Göttingen.

C. Une preuve du Théorème fondamental de l'Algèbre

Ce théorème a déjà été démontré au chapitre 5 (Th. 5.3). La preuve donnée ici utilise les proprétés des extensions galoisiennes.

1/ Préliminaires

Lemme 7.42. *Soit K un corps de* caractéristique 0. *S'il existe un nombre* premier p *tel que, quelle que soit l'extension de degré fini L de K, $L \neq K$, on ait $p \mid [L:K]$, alors $[L:K]$ est une puissance de p.*

Démonstration. Le corps K est de caractéristique 0, donc K est un corps parfait (Déf. 3.25). Etant donné une extension $L:K$ telle $[L:K] < \infty$ et $L \neq K$, soit N une clôture normale de $L:K$; alors $N:K$ est une extension galoisienne, de degré fini (Th. 7.27) et d'après l'hypothèse du lemme, p divise $[N:K]$.
Posons $G = G(N:K)$; G est un groupe fini (Th. 7.27) et

$$o(G) = [N:K] \Longrightarrow p \mid o(G).$$

On en déduit (Cf. Rappels, par. **A.** précédent) que $o(G) = sp^n$ où s et n sont dans $\mathbb{N}^*$ et $p \nmid s$. Supposons $s \neq 1$.
Soit S un p-sous-groupe de Sylow de G. L'extension $N:K$ est galoisienne, de degré fini, donc la correspondance de Galois définit une bijection de l'ensemble des sous-groupes de G, sur l'ensemble des sous-corps de N contenant K (Th. 7.30). D'après le Théorème fondamental de Galois (Th. 7.32),

$$K \subseteq Inv_N(S) \subseteq N \Longrightarrow [Inv_N(S):K] = [G:S].$$

L'hypothèse du lemme implique que $p \mid [Inv_N(S):K]$ or, S est un p-sous-groupe de Sylow de G, donc $p \nmid [G:S] = s$, d'où une contradiction. Par suite $s = 1$, donc

$$[N:K] = o(G) \text{ est une puissance de } p ;$$

alors $[L:K] \mid [N:K] \Longrightarrow [L:K]$ est une puissance de p. □

Lemme 7.43. *Pour toute extension L de* $\mathbb{R}$,

$$(L \neq \mathbb{R} \text{ et } [L:\mathbb{R}] < \infty) \Longrightarrow [L:\mathbb{R}] \text{ est une puissance de } 2.$$

Démonstration. Soit $L \neq \mathbb{R}$ une extension de degré fini sur $\mathbb{R}$, donc algébrique sur $\mathbb{R}$ (Th. 2.26). Soit $\alpha \in L \setminus \mathbb{R}$ et $p_\alpha := Irr_{\mathbb{R}}(\alpha, X)$. Tout polynôme de $\mathbb{R}[X]$, de degré impair ayant une racine réelle (Propriété P_1, Ch. 5.1.), le degré du polynôme irréductible $p_\alpha(X)$ est nécessairement pair. Par suite $[\mathbb{R}(\alpha):\mathbb{R}] = deg\, p_\alpha$ est pair et

$$[\mathbb{R}(\alpha):\mathbb{R}] \mid [L:\mathbb{R}] \Longrightarrow [L:\mathbb{R}] \text{ pair.}$$

D'après le lemme 7.42, $[L:\mathbb{R}]$ est alors une puissance de 2. □

2/ Preuve du Théorème fondamental de l'algèbre

Montrons que le corps $\mathbb{C}$ des nombres complexes n'a pas d'extension algébrique propre (Cf. Th. 5.1).

Supposons qu'il existe une extension L de $\mathbb{C}$ telle que

$$[L:\mathbb{C}] < \infty \quad \text{et} \quad L \neq \mathbb{C}.$$

Cette hypothèse implique que L est algébrique sur $\mathbb{C}$ (Th. 2.26) ; on en déduit que L est algébrique sur $\mathbb{R}$ (Th. 2.31). Soit N une clôture normale de L sur $\mathbb{R}$. On a

$$\mathbb{R} \subset \mathbb{C} \subset L \subseteq N$$

et N est une extension de $\mathbb{R}$ de degré fini (Th. 3.17), normale et séparable, car $\mathbb{R}$ est un corps parfait, donc $N:\mathbb{R}$ est galoisienne, de degré fini (Th. 7.27). D'après le lemme 7.43, $[N:\mathbb{R}]$ est une puissance de 2 ; supposons

$$[N:\mathbb{R}] = 2^n, n \geq 1.$$

Soit $G := G(N:\mathbb{R})$, alors $o(G) = 2^n$ (Th. 7.27).

$$\big([N:\mathbb{R}] = 2^n \text{ et } [\mathbb{C}:\mathbb{R}] = 2\big) \Longrightarrow [N:\mathbb{C}] = 2^{n-1}.$$

L'hypothèse $L \neq \mathbb{C}$ implique $N \neq \mathbb{C}$ et $N:\mathbb{C}$ est une extension galoisienne de degré fini. Posons $H := G(N:\mathbb{C})$; H est un sous-groupe de G et

$$o(H) = [N:\mathbb{C}] = 2^{n-1} > 1.$$

Par suite, H contient au moins un sous-groupe H' d'ordre 2^{n-2} (voir Rappels, par. **A.**, Th. de Sylow). Posons $F := Inv_N(H')$, on a $\mathbb{R} \subset \mathbb{C} \subset F \subset N$, et

$$[H:H'] = 2 \Longrightarrow H' \lhd H \quad ([12], \text{Prop. } 4.14)$$

Le Théorème fondamental de Galois (Th. 7.32) implique alors

$$[F:\mathbb{C}] = [H:H'] = 2 \quad \text{et} \quad F:\mathbb{C} \text{ galoisienne.}$$

On en déduit (Cor 7.28) qu'il existe $\beta \in F \setminus \mathbb{C}$ tel que

$$F = \mathbb{C}(\beta) \quad \text{et} \quad deg\, Irr_{\mathbb{C}}(\beta, X) = 2.$$

Or, dans $\mathbb{C}[X]$, tout polynôme de degré 2 est scindé (Ch. 5, Rem. 5.4 et Ex. **1.**), par suite $\beta \in \mathbb{C}$, d'où une contradiction avec ce qui précède, donc avec l'hypothèse $L \neq \mathbb{C}$.

En conclusion : $\mathbb{C}$ est algébriquement clos.

4. Norme et Trace

Notations et Rappels

Etant donné une extension de corps $L:K$ de degré fini, on pose $[L:K] = n \geq 1$ et on note $[L:K]_s$ son degré de séparabilité (Déf. 7.14). Toute extension algébrique de L sera supposée contenue dans une clôture algébrique de K fixée, $\overline{K}$.

$\varphi : L \hookrightarrow \overline{K}$ désignera un K-monomorphisme de L dans $\overline{K}$.

Soit M la clôture normale de L sur K, dans $\overline{K}$; alors, $M:K$ est de degré fini, galoisienne sur K (Th. 7.27 et tout K-monomorphisme de L dans $\overline{K}$ est un K-monomorphisme de L dans M (Prop. 7. 13), de plus (Prop. 7.17, 7.15, 7.12),

$$1)\, L:K \text{ séparable} \iff [L:K]_s = [L:K].$$

$$2)\, L:K \text{ normale} \Longrightarrow [L:K]_s = \mid G(L:K) \mid .$$

$$3) \forall \varphi : L \hookrightarrow \overline{K}, \exists \sigma \in G(M:K), \text{ tel que } \sigma_{/L} = \varphi.$$

A. Notions de Norme et Trace

La propriété 1), rappelée ci dessus, justifie la définition suivante.

Définition 7.44. Soit $L : K$ une extension de corps séparable, de degré fini $n \geq 1$; notons $\{\varphi_i\}_{1\leq i\leq n}$ l'ensemble des K-monomorphismes de L dans $\overline{K}$, alors, pour tout α dans L,

$$N_{L:K}(\alpha) = \prod_{1\leq i\leq n} \varphi_i(\alpha) \quad \text{et} \quad T_{L:K}(\alpha) = \sum_{1\leq i\leq n} \varphi_i(\alpha) \tag{7.17}$$

sont, respectivement, appelés la **norme** et la **trace** de α sur K.

Remarque 7.45. Les hypothèses et les notations sont celles de la définition 7.44.
a) Si aucune ambiguïté n'est possible, la norme et la trace d'un élément α de L, sur K, seront respectivement notées, $N(\alpha)$ et $T(\alpha)$.
b) D'après le rappel 3), M étant la clôture normale de L sur K, quel que soit $i (1 \leq i \leq n)$, il existe $\sigma_i \in G(M : K)$ tel que $\sigma_{i/L} = \varphi_i$, d'où

$$\forall \alpha \in L, \quad N(\alpha) = \prod_{1\leq i\leq n} \sigma_i(\alpha) \quad \text{et} \quad T(\alpha) = \sum_{1\leq i\leq n} \sigma_i(\alpha). \tag{7.18}$$

c) Les notions de norme et trace seront utiles dans les Ch. 8 et 9.

Proposition 7.46. *Si $L : K$ est une extension de corps* galoisienne, *de degré fini $n \geq 1$, et si $G(L : K) = \{\sigma_i\}_{1\leq i\leq n}$, alors, pour tout $\alpha \in L$,*

$$N(\alpha) = \prod_{1\leq i\leq n} \sigma_i(\alpha) \quad \textit{et} \quad T(\alpha) = \sum_{1\leq i\leq n} \sigma_i(\alpha). \tag{7.19}$$

Démonstration. L'extension galoisienne $L : K$, de degré fini $n \geq 1$, est séparable et normale (Th. 7.27), donc L s'identifie à sa clôture normale M et les formules (7.19) se déduisent des formules (7.18). □

Remarque 7.47. On suppose $[L : K] = n \geq 1$ et $L : K$ séparable ; les notations sont celles de la Déf. 7.44 et de la Rem. 7.45
a) Soit $\alpha \in L$ et $p_\alpha(X) := Irr_K(\alpha, X)$. M étant une clôture normale de L sur K, pour tout i, $1 \leq i \leq n$, $\varphi_i(\alpha)$ est une racine de $p_\alpha(X)$ dans M (Rem. 7.11, d)), c'est-à-dire un *conjugué* de α dans M (Déf 2.18).
On a nécessairement, $1 \leq r := deg\, p_\alpha(X) \leq n$ et L est séparable sur K, donc $p_\alpha(X)$ a exactement r racines distinctes dans M.
Cela signifie que le nombre des $\varphi_i(\alpha)$, $1 \leq i \leq n$, *distincts* dans M, est $r \leq n$.
D'autre part, quels que soient $\sigma \in G(M : K)$ et $i (1 \leq i \leq n)$, $\sigma \circ \varphi_i$ est un K-monomorphisme de L dans M et $i \neq j \Longrightarrow \sigma \circ \varphi_i \neq \sigma \circ \varphi_j$, d'où

$$\forall \sigma \in G(M : K), \quad \{\sigma \circ \varphi_i\}_{1\leq i\leq n} = \{\varphi_i\}_{1\leq i\leq n}.$$

On en déduit que,

$$\forall \alpha \in L, \forall \sigma \in G(M : K), \ \sigma(N(\alpha)) = N(\alpha) \quad \text{et} \quad \sigma(T(\alpha)) = T(\alpha).$$

Or, l'extension $M : K$ est galoisienne, donc $Inv_K G(M : K) = K$, d'où

$$\forall \alpha \in L, \quad N(\alpha) \in K \quad \text{et} \quad T(\alpha) \in K.$$

Ainsi N et T sont des applications de L dans K.

b) Les hypothèses de la Déf 7.44. impliquent que, dans les formules (7.17), les morphismes φ_i, $(1 \leq i \leq n)$ sont distincts, injectifs, donc non nuls ; en conséquence,

$$N(\alpha) = 0 \iff \alpha = 0 \quad \text{et} \quad T(0) = 0.$$

Mais l'application T, de L dans K, n'est pas nulle. En effet,

$$T = 0 \iff \sum_{1\le i\le n} \varphi_i = 0.$$

Or, d'après le Lemme de Dedekind (Lemme 7.48, ci-dessous)

$$\sum_{1\le i\le n} \varphi_i = 0 \Longrightarrow \varphi_i = 0,\ \forall i (1 \le i \le n),$$

ce qui est impossible dans le contexte de la Déf. 7.44.

Lemme 7.48. Lemme de Dedekind
Quels que soient les corps K et L, toute famille de morphismes distincts, non nuls de K dans L, $\Phi = \{\varphi_i\}_{i\in I}$, où I est un ensemble non vide, quelconque, est linéairement indépendante *sur L.*

Démonstration. Supposons la famille Φ linéairement *dépendante* sur L.
Nécessairement, il existe au moins une sous-famille finie Φ' de Φ, linéairement *dépendante* sur L; posons $\Phi' = \{\varphi_{i_1}, \dots, \varphi_{i_n}\}$; $n \in \mathbb{N}^*$.
On peut supposer que Φ' est *minimale*, c'est-à-dire que toute sous-famille *propre* de Φ' est linéairement indépendante sur L.
L'hypothèse implique qu'il existe des éléments $\alpha_1, \dots, \alpha_n$, non tous nuls dans L, tels que

$$\sum_{1\le k\le n} \alpha_k \varphi_{i_k} = 0.$$

La minimalité de la famille finie Φ' implique qu'aucun α_k, $(1 \le k \le n)$, n'est nul. En particulier, $\alpha_1 \neq 0$ permet d'écrire

$$\varphi_{i_1} = \sum_{2\le k\le n} \alpha'_k \varphi_{i_k}, \quad \text{où} \quad \forall k (2 \le k \le n),\ \alpha'_k = -\alpha_k \alpha_1^{-1}. \tag{7.20}$$

En utilisant (7.20), on obtient :

$$\forall x \in K,\ \varphi_{i_1}(x) = \sum_{2\le k\le n} \alpha'_k \varphi_{i_k}(x); \tag{7.21}$$

$$\forall x, y \in K,\ \varphi_{i_1}(xy) = \varphi_{i_1}(x)\varphi_{i_1}(y) = \sum_{2\le k\le n} \alpha'_k \varphi_{i_k}(x)\varphi_{i_k}(y) \tag{7.22}$$

$$= \Big(\sum_{2\le k\le n} \alpha'_k \varphi_{i_k}(x)\Big)\varphi_{i_1}(y). \tag{7.23}$$

(7.22) et (7.23) entraînent que, quels que soient x, y dans K,

$$0 = \sum_{2\le k\le n} \alpha'_k \big(\varphi_{i_1}(y) - \varphi_{i_k}(y)\big)\varphi_{i_k}(x). \tag{7.24}$$

Or, la minimalité de la famille Φ' implique que $\{\varphi_{i_k}\}_{2\le k\le n}$ est linéairement indépendante sur L; on en déduit que

$$(7.24) \Longrightarrow \alpha'_k(\varphi_{i_1}(y) - \varphi_{i_k}(y)) = 0,\ \forall k (2 \le k \le n),\ \forall y \in K.$$

$$\text{alors,}\quad \forall k (2 \le k \le n),\ \alpha'_k \neq 0 \Longrightarrow \varphi_{i_k} = \varphi_{i_1},$$

ce qui contredit l'hypothèse. □

Proposition 7.49. *Soit $L : K$ une extension de corps séparable, de degré fini $n \geq 1$, alors la norme N et la trace T de L sur K, vérifient les propriétés suivantes. Quels que soient α, β dans L et λ dans K,*

$$\begin{aligned} N(\alpha\beta) &= N(\alpha)N(\beta) & T(\alpha+\beta) &= T(\alpha)+T(\beta) \\ N(\lambda\alpha) &= \lambda^n N(\alpha) & T(\lambda\alpha) &= \lambda T(\alpha) \\ N(\lambda) &= \lambda^n & T(\lambda) &= n\lambda. \end{aligned}$$

Preuve laissée au lecteur.

Remarque 7.50. Les hypothèses étant celles de la Prop. 7.49, on sait que l'application T, de L dans K, n'est pas nulle (Rem. 7.47, b)). Montrons qu'il existe $\gamma \in L$ tel que $T(\gamma) = 1$. En effet, soit $\alpha \in L$, tel que $T(\alpha) \neq 0$. Posons $\lambda := T(\alpha)$ et $\gamma = \lambda^{-1}\alpha$; alors (Prop. 7.49),

$$T(\gamma) = \lambda^{-1}T(\alpha) = \lambda^{-1}\lambda = 1.$$

Proposition 7.51. Formules de transitivité
Soit $L : K$ une extension de corps de degré fini, séparable, et F un corps intermédiaire ; alors pour tout $\alpha \in L$, on a

$$N_{L:K}(\alpha) = N_{F:K}(N_{L:F}(\alpha)) \quad et \quad T_{L:K}(\alpha) = T_{F:K}(T_{L:F}(\alpha)). \tag{7.25}$$

Démonstration. L'extension $L : K$ étant séparable, il en est de même des extensions $L : F$ et $F : K$ (Th. 3.29).
Soit $M \subseteq \overline{K}$, la clôture normale de L sur K. On a $K \subseteq F \subseteq L \subseteq M$ et M est galoisienne, de degré fini sur K.
M est une extension normale de F, donc tout K-monomorphisme de F dans $\overline{K}$ est un K-monomorphisme de F dans M. Posons $m := [F : K]$; puisque l'extension $F : K$ est séparable, on a aussi $m = [F : K]_s$.
Notons $\{\varphi_i\}_{1\leq i\leq m}$ l'ensemble des K-monomorphismes de F dans M ; alors (Prop. 7.12), quel que soit $i (1 \leq i \leq m)$, il existe $\sigma_i \in G(M : K)$ tel que $\sigma_{i/F} = \varphi_i$ et pour tout $\beta \in F$,

$$N_{F:K}(\beta) = \prod_{1\leq i\leq m} \sigma_i(\beta) \quad \text{et} \quad T_{F:K}(\beta) = \sum_{1\leq i\leq m} \sigma_i(\beta). \tag{7.26}$$

Posons $n := [L : F]$; alors $n = [L : F]_s$, puisque $L : F$ est séparable ; soit $\{\psi_j\}_{1\leq j\leq n}$, l'ensemble des F-monomorphismes de L dans M.
Etant donné $\tau : L \hookrightarrow M$, $\tau_{/F}$ est un K-monomorphisme de F dans M, donc il existe un unique i, $1 \leq i \leq m$, tel que $\tau_{/F} = \varphi_i = \sigma_{i/F}$, où $\sigma_i \in G(M : K)$; par suite,

$$\forall \beta \in F, \quad \sigma_i^{-1} \circ \tau(\beta) = \sigma_i^{-1} \circ \sigma_i(\beta) = \beta,$$

donc $\sigma_i^{-1} \circ \tau$ est un F-monomorphisme de L dans M ; par suite, il existe un unique j, $1 \leq j \leq n$, tel que $\sigma_i^{-1} \circ \tau = \psi_j$, d'où $\tau = \sigma_i \circ \psi_j$. Or,

$$([L : F] = n, [F : K] = m) \Longrightarrow [L : K] = mn = [L : K]_s,$$

car $L : K$ est séparable ; donc l'ensemble des K-monomorphimes distincts de L dans M est

$$\{\sigma_i \circ \psi_j \,;\, 1 \leq i \leq m,\ 1 \leq j \leq n\}.$$

$$\forall \alpha \in L,\ N_{L:F}(\alpha) = \prod_{1\leq j\leq n} \psi_j(\alpha), \quad T_{L:F}(\alpha) = \sum_{1\leq j\leq n} \psi_j(\alpha).$$

$N_{L:F}(\alpha), T_{L:F}(\alpha)$ sont des éléments de F ; d'où (Rel. (7.25)),

$$N_{F:K}(N_{L:F}(\alpha)) = \prod_{1\leq i\leq m} \sigma_i\Big(\prod_{1\leq j\leq n} \psi_j(\alpha)\Big) = \prod_{(i,j)} \sigma_i \circ \psi_j(\alpha) = N_{L:K}(\alpha).$$

$$T_{F:K}(N_{L:F}(\alpha)) = \sum_{1\leq i\leq m} \sigma_i\Big(\sum_{1\leq j\leq n} \psi_j(\alpha)\Big) = \sum_{(i,j)} \sigma_i \circ \psi_j(\alpha) = T_{L:K}(\alpha). \qquad \square$$

Exemple 7.52. Soit $\mathbb{Q}(\alpha)$ une extension simple algébrique de $\mathbb{Q}$; posons $p_\alpha(X) := Irr_{\mathbb{Q}}(\alpha, X)$ et $n := deg\, p_\alpha$.
$\mathbb{Q}$ étant un corps parfait (Déf. 3.25), α est séparable sur $\mathbb{Q}$, d'où (Th. 7.16),

$$[\mathbb{Q}(\alpha) : \mathbb{Q}]_s = [\mathbb{Q}(\alpha) : \mathbb{Q}] = n.$$

Notons $\varphi_1, \varphi_2, \ldots \varphi_n$, les n K-monomorphismes de $\mathbb{Q}(\alpha)$ dans $\overline{\mathbb{Q}}$.
Soit E un corps de décomposition de $p_\alpha(X)$ sur $\mathbb{Q}$; alors (Prop. 7.12), quel que soit i, $1 \leq i \leq n$, il existe $\sigma_i \in G(E : \mathbb{Q})$ tel que

$$\sigma_{i/\mathbb{Q}(\alpha)} = \varphi_i.$$

Soit $\theta \in \mathbb{Q}(\alpha)$; les hypothèses impliquent que $\{\alpha^i, 0 \leq i \leq n-1\}$ est une base de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$, d'où

$$\theta = \sum_{0 \leq i \leq n-1} a_i \alpha^i, \quad \text{où, pour tout } i (0 \leq i \leq n-1),\ a_i \in \mathbb{Q}.$$

En posant, quel que soit k, $1 \leq k \leq n$, $\varphi_k(\alpha) = \beta_k$, on obtient

$$\varphi_k(\theta) = \sum_{0 \leq i \leq n-1} a_i \beta_k{}^i \text{ ; d'où}$$

$$N(\theta) = \prod_{1 \leq k \leq n} \varphi_k(\theta) = \prod_{1 \leq k \leq n} \Big(\sum_{0 \leq i \leq n-1} a_i \beta_k{}^i \Big) \tag{7.27}$$

$$T(\theta) = \sum_{1 \leq k \leq n} \varphi_k(\theta) = \sum_{1 \leq k \leq n} \Big(\sum_{0 \leq i \leq n-1} a_i \beta_k{}^i \Big). \tag{7.28}$$

B. Quelques applications des notions de norme et trace

Théorème 7.53. *Soit $L : K$ une extension galoisienne, de degré fini $n > 1$, telle que le groupe de Galois $G(L : K)$ est* cyclique, *engendré par σ ; alors pour $\alpha \in L$, on a*

$$T(\alpha) = 0 \iff \exists \beta \in L \ \text{ tel que } \ \alpha = \beta - \sigma(\beta),$$

où T est l'application trace de L dans K.

Démonstration. Les hypothèses impliquent que le groupe $G(L : K)$ est cyclique d'ordre $n = [L : K]$ (Th. 7.27), engendré par σ, donc

$$G(L : K) = \{\sigma^i, \quad 0 \leq i \leq n-1\}.$$

Soit $\beta \neq 0$ dans L ; on alors $\alpha := \beta - \sigma(\beta) \neq 0$, car $\sigma \neq id_L$.

$$\begin{aligned} T(\alpha) &= (id_L + \sigma + \sigma^2 + \cdots + \sigma^{n-1})(\alpha) \\ &= \big(\beta - \sigma(\beta)\big) + \big(\sigma(\beta) - \sigma^2(\beta)\big) + \cdots + \big(\sigma^{n-1}(\beta) - \sigma^n(\beta)\big) \\ &= 0, \quad \text{car } \sigma^n = id_L. \end{aligned}$$

Réciproquement, supposons $\alpha \in L$ tel que $T(\alpha) = 0$.
On sait qu'il existe $\gamma \in L$, tel que $T(\gamma) = 1$ (Rem. 7.50). Posons

$$\forall i (0 \leq i \leq n-2), \quad d_i := \big(\alpha + \sigma(\alpha) + \cdots + \sigma^i(\alpha)\big)\sigma^i(\gamma)$$
$$\text{et} \qquad \beta := d_0 + d_1 + \cdots + d_{n-2}.$$

Pour $n \geq 2$,

$$(i = n-2 \text{ et } T(\alpha) = 0) \Longrightarrow \sigma(d_{n-2}) = -\alpha\sigma^{n-1}(\gamma).$$

Pour $n > 2$,

$$\begin{aligned} (0 \leq i \leq n-3) &\Longrightarrow \sigma(d_i) = \big(\sigma(\alpha) + \cdots + \sigma^{i+1}(\alpha)\big)\sigma^{i+1}(\gamma) \\ &\Longrightarrow d_{i+1} - \sigma(d_i) = \alpha\sigma^{i+1}(\gamma), \\ \text{d'où, } \beta - \sigma(\beta) &= d_0 + \big(d_1 - \sigma(d_0)\big) + \cdots + \big(d_{n-2} - \sigma(d_{n-3})\big) - \sigma(d_{n-2}) \\ &= \alpha\gamma + \alpha\sigma(\gamma) + \cdots + \alpha\sigma^{n-1}(\gamma) \\ &= \alpha, \quad \text{car } T(\gamma) = 1. \end{aligned}$$

□

En application de ce théorème on obtient une description d'une extension galoisienne de degré p, sur un corps K de caractéristique p.

Théorème 7.54. *Soit K un corps de caractéristique $p \neq 0$. Si L est une extension galoisienne de K telle que $[L:K] = p$, alors $L = K(u)$, le polynôme $Irr_K(u,X)$ étant de la forme $X^p - X - a$.*

Démonstration. Les hypothèses impliquent que $|\, G(L:K) \,| = p$, donc le groupe $G(L:K)$ est cyclique, puisque p est un nombre premier ([12], Prop. 3.9).
Soit σ un générateur du groupe $G(L:K)$, T étant l'application trace de L dans K, on a

$$T(1) = \sum_{0 \leq i \leq p-1} \sigma^i(1) = p.1 = 0, \quad \text{dans } K.$$

D'après le Th. 7.52, il existe $\beta \in L$ tel que $1 = \beta - \sigma(\beta)$.
En posant $u = -\beta$, on a $\sigma(u) - u = 1$ et par suite,

$$\sigma(u) = u + 1 \Longrightarrow \sigma(u^p) = \big(\sigma(u)\big)^p = (1+u)^p = 1 + u^p.$$

On en déduit que $a := u^p - u$ est invariant par σ, générateur du groupe $G(L:K)$; donc $a \in Inv_L(G(L:K) = K$, car $L:K$ est galoisienne.
D'autre part, p étant un nombre premier, il n'existe aucun corps intermédiaire entre K et L (autre que K et L), donc nécessairement, $L = K(u)$ et $X^p - X - a = Irr_K(u,X)$. □

Théorème 7.55. *Soit $L:K$ une extension de corps galoisienne, de degré fini $n > 1$. Si le groupe $G(L:K)$ est cyclique, engendré par σ, alors pour $\alpha \in L$, on a*

$$N(\alpha) = 1 \iff \exists \beta \in L \quad \textit{tel que} \quad \alpha = \beta\big(\sigma(\beta)\big)^{-1},$$

où N est l'application norme de L dans K.

Démonstration. Soit $\beta \neq 0$ dans L et $\alpha := \beta\big(\sigma(\beta)\big)^{-1}$; on a $\alpha \neq 1$, car $\sigma \neq id_L$.
Pour des raisons de commodité, on écrira α sous la forme $\dfrac{\beta}{\sigma(\beta)}$; alors

$$\begin{aligned} N(\alpha) &= \alpha\sigma(\alpha)\ldots\sigma^{n-1}(\alpha) \\ &= \frac{\beta}{\sigma(\beta)}\frac{\sigma(\beta)}{\sigma^2(\beta)}\cdots\frac{\sigma^{n-1}(\beta)}{\sigma^n(\beta)} \\ &= \frac{\beta}{\sigma^n(\beta)} = 1, \quad \text{car} \quad \sigma^n = id_L. \end{aligned}$$

Réciproquement, supposons $\alpha \in L$ tel que $N(\alpha) = 1$, donc $\alpha \neq 0$.
Etant donné $x \in L$, posons

$$\begin{aligned} &\forall i (0 \leq i \leq n-1), \qquad d_i = \big(\alpha\sigma(\alpha)\ldots\sigma^i(\alpha)\big)\sigma^i(x); \\ &\text{alors,} \qquad d_0 = \alpha x, \qquad d_{n-1} = N(\alpha)\sigma^{n-1}(x) = \sigma^{n-1}(x) \\ &\text{et} \qquad \forall i (1 \leq i \leq n-2), \qquad d_i = \alpha\sigma(d_{i-1}). \end{aligned}$$

Soit $\beta := d_0 + d_1 + \cdots + d_{n-1}$.
Vérifions qu'il existe $x \in L$, tel que l'on ait $\beta \neq 0$. En effet, en posant

$$\begin{aligned} &\forall i (0 \leq i \leq n-1), \quad \lambda_i := \alpha\sigma(\alpha)\ldots\sigma^i(\alpha), \quad \text{dans } L, \\ &\text{on a} \qquad \beta = \sum_{0 \leq i \leq n-1} \lambda_i \sigma^i(x). \end{aligned}$$

Or, d'après le lemme de Dedekind (Lem. 7.48), les K-automorphismes σ^i, $0 \leq i \leq n-1$, sont linéairement indépendants sur L ; par suite,

$$(\beta = 0, \forall x \in L) \implies \lambda_i = 0, \forall i (0 \leq i \leq n-1);$$

mais, $\lambda_0 = \alpha = 0$, est contraire à l'hypothèse ; il est donc possible de choisir $x \in L$ tel que $\beta \neq 0$. Dans ce cas, on a $\sigma(\beta) \neq 0$ et

$$\begin{aligned} \sigma(\beta) &= \sigma(d_0) + \sigma(d_1) + \cdots + \sigma(d_{n-1}) \\ &= \alpha^{-1}(d_1 + d_2 + \cdots + d_{n-1}) + \sigma^n(x); \end{aligned}$$

$$\sigma^n(x) = x = \alpha^{-1} d_0 \implies \sigma(\beta) = \alpha^{-1}(d_0 + d_1 + \cdots + d_{n-1}) = \alpha^{-1}\beta,$$

d'où $\alpha = \beta\big(\sigma(\beta)\big)^{-1} = \beta\sigma(\beta^{-1})$. □

Théorème 7.56. *Soit $L : K$ une extension galoisienne, de degré fini p, où p est un* nombre premier. *On suppose que le corps K est de caractéristique 0 ou $q \neq p$, et que le polynôme $X^p - 1$ est scindé sur K ; on a alors $L = K(\alpha)$ et le polynôme $Irr_K(\alpha, X)$ est de la forme $X^p - a$.*

Démonstration. Les hypothèses impliquent que le corps K contient le groupe cyclique U_p, d'ordre p, des racines $p^{èmes}$ de l'unité (Prop. 6.4) ; p étant un nombre premier, tout $\omega \neq 1$, dans U_p, est un générateur du groupe et on peut écrire, pour un ω donné,

$$U_p = \{\omega^i \,;\, 0 \leq i \leq p-1\}.$$

Par ailleurs, l'extension $L : K$ est galoisienne, donc

$$[L : K] = p \implies |\, G(L : K) \,| = p;$$

par suite, le groupe $G(L : K)$ est cyclique ; désignons par σ l'un de ses générateurs.
Soit N l'application norme de L dans K et $\omega \neq 1$ dans $U_p \subset K$; alors (Prop. 7.49),

$$\omega \in K \implies N(\omega) = \omega^p = 1.$$

On en déduit (Th. 7.54.) qu'il existe $\alpha \in L$, tel que $\omega = \alpha\big(\sigma(\alpha)\big)^{-1}$.
On note que $\omega \neq 1 \implies \sigma(\alpha) \neq \alpha$, donc $\alpha \notin K = Inv_K(G(L : K))$.

$$\sigma(\alpha) = \omega^{-1}\alpha \implies \sigma(\alpha^p) = \big(\sigma(\alpha)\big)^p = \omega^{-p}\alpha^p = \alpha^p, \text{ car } \omega^{-p} = 1.$$

Par suite, $\alpha^p \in Inv_K(G(L : K) = K$; posons $a := \alpha^p$.
L'hypothèse $(car K = 0$ ou $car K = q \neq p)$ implique que le polynôme $X^p - a$ est séparable sur K. Les p racines distinctes de $X^p - a$ sont alors les $\omega^i\alpha$, pour $0 \leq i \leq p-1$, par suite $K(\alpha)$ est corps de décomposition sur K, de $X^p - a$.
On a montré ci-dessus, que $\alpha \notin K$, d'où $K \subsetneq K(\alpha) \subseteq L$.
Or, $[L : K] = p$ et p est premier, donc il n'existe aucun corps intermédiaire entre K et L (autre que K ou L), on en déduit que $L = K(\alpha)$ et $X^p - a = Irr_K(\alpha, X)$. □

5. Exercices

1. Enoncer cinq propriétés équivalentes à

$L : K$ est une extension galoisienne, de degré fini.

2. Soit K un corps de caractéristique 0 et $n > 1$ dans $\mathbb{N}$. On suppose que le polynôme $X^n - 1$ est scindé sur K.
Soit $f(X) := X^n - a$, où $a \in K^*, a \neq 1$.
1°) Vérifiez que si α est une racine de $f(X)$ dans une extension de K, alors l'extension $K(\alpha) : K$ est galoisienne, de degré fini (voir Ex. **2.**, Ch. 6).
2°) Prouver que le groupe $G(K(\alpha) : K)$ est abélien [voir Exemple 7.29, 2)].

3. 1°) On considère les extensions de corps suivantes

$$\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}; \quad \mathbb{Q}(\sqrt[3]{5}, i) : \mathbb{Q}(i), \text{ où } i^2 = -1, \text{ dans } \mathbb{C};$$
$$\mathbb{Q}(\sqrt[3]{5}, j) : \mathbb{Q}; \quad \mathbb{Q}(\sqrt[3]{5}, j) : \mathbb{Q}(j), \text{ où } j^3 = 1, j \neq 1, \text{ dans } \mathbb{C}.$$

Pour chaque extension,
– trouver son degré ;
– préciser si l'extension est galoisienne ou non ;
– déterminer son groupe de Galois, en définissant chacun des éléments de ce groupe.
Lorsque le cardinal du groupe de Galois est différent de 1, préciser la structure de ce groupe (est-il abélien ? est-il cyclique ? ou isomorphe à un groupe symétrique ?).
2°) Répondre aux mêmes questions que précédemment, au sujet des extensions suivantes.

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}, i) : \mathbb{Q}(i); \quad \mathbb{Q}(\sqrt{3}, \sqrt[3]{5}, i) : \mathbb{Q}; \quad \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5}, j) : \mathbb{Q}.$$

4. Soit K un corps tel que $car K \neq 2$. On note $\overline{K}$ une clôture algébrique de K.
1°) On considère un polynôme unitaire $f(X) \in K[X]$, de degré $n > 1$. Soit $E \subset \overline{K}$ un corps de décomposition de $f(X)$ sur K. On suppose que $f(X)$ n'a que des racines simples dans E ; on les notera $\alpha_1, \alpha_2, \ldots, \alpha_n$. On pose

$$\Delta := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j), \quad D := \Delta^2, \quad G_f = G(E : K).$$

a) Justifier les propriétés suivantes.
i) $E : K$ est une extension galoisienne de degré fini.
ii) $D \in K$.
iii) Lorsque σ décrit G_f, il n'y a, dans E, que deux valeurs possibles pour $\sigma(\Delta)$ et $[K(\Delta) : K] = 1$ ou 2.
b) Soit $H := \{\sigma \in G_f \,;\, \sigma(\Delta) = \Delta\}$. Montrer que H est un sous-groupe *normal* de G_f et préciser l'indice $[G_f : H]$.
Prouver que H et $K(\Delta)$ se correspondent dans la correspondance de Galois associée à l'extension $E : K$.
c) Vérifier que le groupe G_f est isomorphe à un sous-groupe du groupe symétrique $\mathcal{S}_n$. Montrer que si $f(X)$ est irréductible dans $K[X]$, alors n divise l'ordre du groupe G_f.
2°) Dans $K[X]$, on considère $f(X) = X^3 + pX + q$ et on suppose $f(X)$ irréductible sur K et séparable.
On conserve les mêmes notations que dans le 1°).
a) Montrer que, suivant la valeur de $[K(\Delta) : K]$, on a

$$G_f \simeq \mathcal{S}_3 \quad \text{ou} \quad G_f \simeq \mathcal{A}_3 \text{ (groupe alterné).}$$

Dans chaque cas, préciser quel est le sous-groupe H de G_f.
b) Vérifier que $D = -4p^3 - 27q^2$ ([13], Ch. 8).
c) Dans le cas où $f(X) = X^3 - 7X + 14$, déterminer le groupe G_f (à un isomorphisme près).

5. Etant donné une extension de corps $L : K$, de *degré fini*, soit E et F deux corps intermédiaires. On pose

$$EF := \{ \sum_{1 \leq i \leq n} x_i y_i \,;\, n \in \mathbb{N}^*, x_i \in E, y_i \in F, \forall i (1 \leq i \leq n).$$

(n décrit $\mathbb{N}$)

1°) Prouver que EF est un sous-corps de L. [voir Ex. **5.**, Ch. 1].
Vérifier que EF est le sous-corps de L engendré par $E \cup F$.
2°) On suppose que l'extension $L : K$ est *galoisienne*.
a) Prouver que les extensions $E : K$, $F : K$, $EF : F$ et $EF : K$ sont galoisiennes.
b) Soit $\sigma \in G(EF : F)$ et $\sigma_{/E}$ la restriction de σ à E.
Montrer que $\sigma_{/E} \in G(E : E \cap F)$. Vérifier que l'application

$$\psi : G(EF : F) \longrightarrow G(E : E \cap F)$$
$$\sigma \longmapsto \sigma_{/E}$$

est un morphisme *injectif* de groupes.
Démontrer que $\{\alpha \in E\ ;\ \tau(\alpha) = \alpha,\ \forall \tau \in Im\,\psi\} = E \cap F$.
En déduire que ψ est un isomorphisme de groupes.
Montrer que l'extension de degré fini $E : E \cap F$ est galoisienne.
3°) On suppose toujours $L : K$ galoisienne.
Soit $\{L_1, L_2, \ldots, L_n\}$ une famille de corps intermédiaires, $n \geq 2$, dans $\mathbb{N}$. On pose

$$L' := L_1 L_2 \ldots L_n,$$

où L' est défini par récurrence sur n, à partir du cas $n = 2$ (Cf. 1°)).
a) Vérifier que L' est le sous-corps de L engendré par $\bigcup_{1 \leq i \leq n} L_i$.
b) Prouver que si, quel que soit i, $1 \leq i \leq n$, $L_i : K$ est une extension normale, alors $L' : K$ est galoisienne.

6. Pour tout corps K, $\overline{K}$ désigne une clôture algébrique de K.
1°) Soit $G := G(\overline{\mathbb{Q}} : \mathbb{Q})$ et $K := Inv_{\overline{\mathbb{Q}}}(G)$. On a $\mathbb{Q} \subseteq K \subseteq \overline{\mathbb{Q}}$.
On suppose qu'il existe un élément $\alpha \in K \setminus \mathbb{Q}$. Montrer que le polynôme $Irr_{\mathbb{Q}}(\alpha, X)$ est alors, nécessairement, de degré 1.
En conclure que l'extension, de degré infini (Rem. 5.11.), $\overline{\mathbb{Q}} : \mathbb{Q}$ est galoisienne.
2°) Montrer de même que, pour tout nombre premier p, l'extension $\overline{\mathbb{F}_p} : \mathbb{F}_p$, où $\mathbb{F}_p$ est le corps à p éléments, est galoisienne et n'est pas de degré fini (voir Rem. 5.2.).
3°) Vérifier que pour tout corps *parfait* K, l'extension $\overline{K} : K$ est galoisienne.

7. Soit $L : K$ une extension de corps de *degré infini*.
1°) Le but de cette question est de prouver que $L : K$ est galoisienne si et seulement si $L : K$ est normale et séparable.
a) On suppose $L : K$ normale et séparable.
Prouver que $K = Inv_L(G(L : K))$ [utiliser la même méthode que dans le 1°) de l'ex. **6.** précédent] ; en conclure que l'extension $L : K$ est galoisienne.
b) On suppose $L : K$ galoisienne. Soit $G := G(L : K)$.
Etant donné $\alpha \in L \setminus K$, soit $R = \{\sigma(\alpha)\ ;\ \sigma \in G\}$.
Montrer que l'ensemble R est fini. On pose $R = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$,
où, les α_i, $1 \leq i \leq r$, sont deux à deux distincts et $\alpha_1 = \alpha$.
Soit $g(X) := (X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_r)$ dans $L[X]$.
Montrer que $g(X) \in K[X]$; en déduire que $Irr_K(\alpha, X) = g(X)$.
En conclure que l'extension $L : K$ est normale et séparable.
2°) Prouver que si $L : K$, de degré infini, est galoisienne, alors, quel que soit le corps F tel que $K \subseteq F \subseteq L$, l'extension $L : F$ est galoisienne.

8. Etant donné une extension de corps $L : K$, on considère l'ensemble $\mathcal{F}$ des corps intermédiaires et l'ensemble $\mathcal{H}$ des sous-groupes de $G(L : K)$.

On ne fait aucune hypothèse sur le degré de l'extension $L : K$.
Soit (γ, γ') la correspondance de Galois associée à $L : K$.
On dira qu'un corps $F \in \mathcal{F}$ (resp. un sous-groupe $H \in \mathcal{H}$) est **fermé** si

$$\gamma' \circ \gamma(F) = F \quad (\text{resp. } \gamma \circ \gamma'(H) = H).$$

Soit $\overline{\mathcal{F}}$ (resp. $\overline{\mathcal{H}}$) l'ensemble des éléments fermés de $\mathcal{F}$ (resp. $\mathcal{H}$).
1°) Vérifier que

$$\forall F \in \mathcal{F},\ \gamma(F) \in \overline{\mathcal{H}} \quad \text{et} \quad \forall H \in \mathcal{H},\ \gamma'(H) \in \overline{\mathcal{F}}.$$

2°) On considère les applications

$$\begin{array}{ccc} \gamma_1 : \overline{\mathcal{F}} \longrightarrow \overline{\mathcal{H}} & & \gamma'_1 : \overline{\mathcal{H}} \longrightarrow \overline{\mathcal{F}} \\ F \longmapsto \gamma(F) & & H \longmapsto \gamma'(H). \end{array}$$

a) Prouver que γ_1, γ'_1 sont des bijections telles que $\gamma_1^{-1} = \gamma'_1$.
b) Justifier l'assertion : « $L : K$ est galoisienne, de degré fini, si et seulement si $\mathcal{F} = \overline{\mathcal{F}}$ et $\mathcal{H} = \overline{\mathcal{H}}$. »
c) On suppose que l'extension $L : K$ est galoisienne, de *degré infini*. Prouver que $\mathcal{F} = \overline{\mathcal{F}}$ (voir l'Ex. **7.**, 2°)).
3°) Soit p un nombre premier. On considère l'extension galoisienne, de degré infini $\overline{\mathbb{F}_p} : \mathbb{F}_p$ (Cf. Ex. **6.**, ci-dessus). Soit $G := G(\overline{\mathbb{F}_p} : \mathbb{F}_p)$ et σ l'application

$$\begin{array}{c} \overline{\mathbb{F}_p} \longrightarrow \overline{\mathbb{F}_p} \\ x \longmapsto x^p. \end{array}$$

a) Vérifier que $\sigma \in G$.
b) Soit H le sous-groupe de G engendré par σ.
(γ, γ') désignant la correspondance de Galois associée à l'extension $\overline{\mathbb{F}_p} : \mathbb{F}_p$, déterminer $\gamma'(H)$ et $\gamma \circ \gamma'(H)$.
En considérant un élément $\alpha \in \overline{\mathbb{F}_p} \setminus \mathbb{F}_p$ et un automorphisme $\tau \in G(\overline{\mathbb{F}_p} : \mathbb{F}_p(\alpha))$, prouver que $H \neq G$. En déduire que $\mathcal{H} \neq \overline{\mathcal{H}}$.
En conclure, qu'en général, pour une extension galoisienne, de degré infini, la correspondance de Galois ne définit pas une bijection.

9. Soit un corps K. Toutes les extensions algébriques de K seront considérées dans une clôture algébrique de K donnée, $\overline{K}$.
1°) Soit L une extension algébrique de K (*on ne fait aucune hypothèse sur le degré de* $L : K$).
Démontrer l'équivalence des trois propriétés suivantes :
a) $L : K$ est une extension normale.
b) $\forall \sigma \in G(\overline{K} : K),\ \sigma_{/L} \in G(L : K)$.
c) $G(L : K) = \{\sigma_{/L}\ ;\ \sigma \in G(\overline{K} : K)\}$.
[Prouver que $a) \Longrightarrow b) \Longrightarrow c) \Longrightarrow a)$; voir la Prop. 7.12]
2°) I étant un ensemble non vide, quelconque, soit $\Phi := \{f_i(X)\}_{i \in I}$ une famille de polynômes *séparables* de $K[X]$ (Déf. 3.35.).
Soit L l'extension de K obtenue par l'adjonction de toutes les racines des polynômes $f_i(X)$, $i \in I$, prises dans $\overline{K}$.
a) Vérifier que L est une extension séparable de K (Th. 7.19.).
b) Soit $\alpha \in L$; justifier l'existence d'un corps F tel que

$$K \subseteq F \subseteq L,\ \alpha \in F,\ F : K \text{ est galoisienne de degré fini.}$$

En déduire que L est une extension normale de K.

c) Montrer que les résultats précédents impliquent que, quel que soit le degré de L sur K, l'extension $L : K$ est galoisienne (dans le cas du degré infini, voir l'Ex. **7.**, ci-dessus).

10. Cet exercice utilise la notion de groupe opérant sur un ensemble ([12], Ch. 5). On rappelle qu'un groupe G opère *transitivement* sur un ensemble X, par

$$G \times X \longrightarrow X$$
$$(g,x) \longmapsto g.x,$$

si quels que soient x, y dans X, il existe, au moins, un élément $g \in G$ tel que $y = g.x$.
Etant donné un corps K, $\overline{K}$ désigne une clôture algébrique de K.
Soit $f(X)$ un polynôme unitaire de $K[X]$ tel que $deg\, f = n \geq 1$; soit $E \subset \overline{K}$ un corps de décomposition de $f(X)$ sur K. On suppose que $f(X)$ n'a que des racines *simples* dans E ; on les note $r_1, \ldots, r_n$. On pose

$$R := \{r_1, \ldots, r_n\} \quad \text{et} \quad G := G(E : K).$$

1°) Montrer que l'extension $E : K$ est galoisienne, de degré fini.
2°) Vérifier que, quel que soit $\sigma \in G$, $\sigma_{/R}$ est une permutation de R ; en déduire que G opère sur R et que l'on peut identifier G à un sous-groupe du groupe symétrique S_n ([12], Ch. 3), de telle façon que l'on puisse écrire

$$\forall \sigma \in G,\ \forall i (1 \leq i \leq n),\ \sigma(r_i) = r_{\sigma(i)}.$$

3°) Démontrer que le polynôme unitaire $f(X)$ est irréductible dans $K[X]$ si et seulement si le groupe G opère transitivement sur R.

11. Les hypothèses générales et les notations sont celles de l'Ex. **10.** précédent et les résultats de cet Ex. **10.** seront supposés connus.
1°) Soit $\tilde{K} := K(X_1, \ldots, X_n)$ et $\tilde{E} := E(X_1, \ldots, X_n)$ les corps des fractions rationnelles à n indéterminées, respectivement sur K et E.
a) Montrer que $\tilde{E}$ est corps de décomposition de $f(X)$ sur $\tilde{K}$.
b) Soit $\tilde{G} := G(\tilde{E} : \tilde{K})$. Prouver que, quel que soit $\tilde{\sigma} \in \tilde{G}$, $\sigma = \tilde{\sigma}_{/E}$ (restriction de $\tilde{\sigma}$ à E) appartient à G et que l'application

$$\psi : \tilde{G} \longrightarrow G$$
$$\tilde{\sigma} \longmapsto \sigma = \tilde{\sigma}_{/E}$$

est un isomorphisme de groupes ; on pourra alors identifier $\tilde{G}$ à G (sous-groupe du groupe symétrique S_n).
2°) Sachant que $E : K$ est une extension galoisienne, de degré fini (Ex. **10.**, ci-dessus), montrer qu'il en est de même, pour $\tilde{E} : \tilde{K}$.
3°) Etant donné $\tau \in S_n$, on pose, dans $\tilde{E}$,

$$u_\tau := \sum_{1 \leq i \leq n} r_{\tau(i)} X_i \quad \text{et} \quad U := \{u_\tau\ ;\ \tau \in S_n\}.$$

a) Vérifier que : $\tau_1 \neq \tau_2$, dans $S_n \Longrightarrow u_{\tau_1} \neq u_{\tau_2}$, dans $\tilde{E}$ et que G (sous-groupe de S_n) opère sur U, par

$$G \times U \longrightarrow U$$
$$(\sigma, u_\tau) \longmapsto u_{\sigma \circ \tau}.$$

Soit Ω_{u_τ}, la G-orbite de u_τ, dans cette action ([12], Déf. 5.13) :

$$\Omega_{u_\tau} = \{\sigma(u_\tau) = u_{\sigma \circ \tau}\ ;\ \sigma \in G\}.$$

Prouver que, quel que soit $\tau \in S_n$, $card(\Omega_{u_\tau}) = card(G)$.
Soit H_{u_τ} le stabilisateur de u_τ, dans l'action de G sur U ([12], Déf. 5.19). Montrer que $H_{u_\tau} = (e)$, où e est l'élément unité de G.
Démontrer que $\tilde{E} = \tilde{K}(u_\tau)$, quel que soit $\tau \in S_n$.
b) Pour tout $\tau \in S_n$, on pose $p_\tau(X) := Irr_{\tilde{K}}(u_\tau, X)$.
Prouver que $p_\tau(X) = \prod_{\sigma \in G} (X - \sum_{1 \leq i \leq n} r_{\sigma \circ \tau(i)} X_i)$, dans $\tilde{E}[X]$.
4°) On pose $\varphi(X) = \prod_{\tau \in S_n} (X - u_\tau)$, dans $\tilde{E}[X]$.
a) Démontrer que $\varphi(X) \in K[X_1, \ldots, X_n, X] = \tilde{K}[X]$.
b) Prouver que tout diviseur irréductible de $\varphi(X)$, dans $\tilde{K}[X]$, est de la forme $p_\tau(X)$, où $\tau \in S_n$.
c) On note Γ le groupe des automorphismes de l'anneau des polynômes $K[X_1, \ldots, X_n, X]$, à $n+1$ indéterminées sur K. On considère l'application

$$\delta : S_n \longrightarrow \Gamma$$
$$\sigma \longmapsto \sigma' := \delta(\sigma), \text{ tel que}$$

$\sigma'_{/K} = id_K$; $\sigma'(X) = X$; $\sigma'(X_i) = X_{\sigma(i)}, \forall\, i\, (1 \leq i \leq n)$.
Démontrer que $\sigma \in G$ si et seulement si $\sigma' = \delta(\sigma)$ laisse invariant tout diviseur irréductible de $\varphi(X)$ dans $K[X_1, \ldots, X_n, X]$.

12. Une extension de corps $L : K$ est dite **cyclique** , si $L : K$ est *galoisienne* et $G(L : K)$ est un groupe *cyclique* [c-à-d. monogène fini ([12], Ch. 3)].
Question préliminaire : Vérifier que toute extension cyclique est de degré fini.

Pour tout corps K, on pose $K^* := K \setminus \{0\}$.
Soit p un nombre premier et $\mathbb{F}_q$ un corps de cardinal $q = p^r$, $r \in \mathbb{N}^*$.
(Les Th. 7.53 et 7.55 pourront être utiles.)
1°) Pour un entier $m > 1$, on considère le corps $\mathbb{F}_{q^m}$ à q^m éléments.
Montrer que l'extension $\mathbb{F}_{q^m} : \mathbb{F}_q$ est cyclique.
[Considérer $\sigma : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}$ telle que $\forall\, \alpha \in \mathbb{F}_{q^m}$, $\sigma(\alpha) = \alpha^q$.]
2°) A tout $\alpha \in \mathbb{F}_{q^m}$, on associe sa norme

$$N(\alpha) := N_{\mathbb{F}_{q^m} : \mathbb{F}_q}(\alpha).$$

a) Vérifier que $\alpha \in \mathbb{F}_{q^m}^* \Longrightarrow N(\alpha) \in \mathbb{F}_q^*$ et que l'application $N : \mathbb{F}_{q^m}^* \longrightarrow \mathbb{F}_q^*$ est un morphisme de groupes.
b) Démontrer que le sous-groupe $KerN$ de $\mathbb{F}_{q^m}^*$ est d'ordre $\dfrac{q^m - 1}{q - 1}$.
En déduire que, quel que soit l'entier $m > 1$, tout élément de $\mathbb{F}_q^*$ est la norme d'un élément de $\mathbb{F}_{q^m}^*$.
3°) A tout $\alpha \in \mathbb{F}_{q^m}$, on associe sa trace

$$T(\alpha) := T_{\mathbb{F}_{q^m} : \mathbb{F}_q}(\alpha).$$

a) Vérifier que l'application $T : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$, qui à tout $\alpha \in \mathbb{F}_{q^m}$ associe $T(\alpha)$, est un morphisme de groupes additifs.
b) Déterminer l'ordre du sous-groupe $KerT$ de $\mathbb{F}_{q^m}$.
En déduire que, quel que soit l'entier $m > 1$, tout élément de $\mathbb{F}_q$ est la trace d'un élément de $\mathbb{F}_{q^m}$.

13. On suppose connue la notion d'extension *cyclique* définie dans l'Ex. **12.** précédent.

Soit K un corps de caractéristique $p \neq 0$. On note $\mathbb{F}_p$ le sous-corps premier de K.
Soit L une extension *galoisienne* de K telle $[L:K] = p$.
1°) Justifier les propriétés suivantes (voir les résultats du Ch. 7).
a) L'extension $L:K$ est cyclique ([12], Prop. 3.9).
b) $T_{L:K}(x) = 0, \forall x \in K$.
c) σ étant un générateur du groupe $G(L:K)$, il existe $u \in L$ tel que

$$\sigma(u) = u+1, \quad L = K(u) \text{ et}$$
$$Irr_K(u,X) \text{ est de la forme } X^p - X - a.$$

2°) a) Soit $v = \alpha u + \beta$ où $\alpha \in \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ et $\beta \in K$.
Démontrer que $L = K(v)$ et que le polynôme $Irr_K(v,X)$ est de la forme $X^p - X - b$.
b) On suppose, réciproquement, que v est un élément de L tel que $L = K(v)$.
Prouver qu'il existe $\alpha \in \mathbb{F}_p$ et $\beta \in K$ tels que $v = \alpha u + \beta$.

14. K étant un corps de caractéristique $p \neq 0$, soit $f(X) = X^p - X - c$, dans $K[X]$ et E un corps de décomposition de $f(X)$ sur K.
1°) Vérifier que $f(X)$ n'a que des racines simples dans E.
2°) a) Soit $u \in E$ une racine de $f(X)$; trouver toutes les racines de $f(X)$, dans E.
b) On suppose que $u \in E \setminus K$ est une racine de $f(X)$. Prouver que

$$E = K(u),\ E:K \text{ est une extension cyclique et } f(X) = Irr_K(u,X).$$

(Cf. Ex. **12.** précédent)
c) En conclure qu'un polynôme de $K[X]$, de la forme $X^p - X - c$, est soit irréductible, soit scindé sur K.

15. Soit un corps K tel que $car K = p \neq 0$. On considère une *extension cyclique* (Cf. Ex. **12.** précédent) $L:K$ telle que $[L:K] = p^s$, $s > 1$ dans $\mathbb{N}$.
1°) Justifier l'existence d'un unique corps F tel que

$$K \subset F \subset L,\ [F:K] = p^{s-1} \text{ et } F:K \text{ est cyclique.}$$

2°) a) Vérifier que $L:F$ est une extension cyclique.
Montrer que si σ est un générateur du groupe $G(L:K)$, alors $\tau := \sigma^{p^{s-1}}$ engendre $G(L:F)$.
Compte tenu des résultats de l'Ex. **13.** précédent, justifier l'existence d'un élément $w \in L$ tel que

$$\tau(w) = w+1,\ L = F(w) \text{ et}$$
$$Irr_F(w,X) \text{ est de la forme } X^p - X - \alpha.$$

b) On pose $p_K(X) := Irr_K(w,X)$.
Démontrer que $deg\, p_K(X) = p^s$; en conclure que $L = K(w)$.

16. Soit p un nombre premier et $a \in \mathbb{Q}^*$. On suppose que a n'a pas de racine $p^{ème}$ dans $\mathbb{Q}$ (voir Ex. **3.**, Ch.6).
1°) Soit $\alpha \in \overline{\mathbb{Q}}$, une racine $p^{ème}$ de a et ε_p une racine $p^{ème}$ *primitive* de l'unité.
a) Quel est le degré de l'extension $\mathbb{Q}(\alpha) : \mathbb{Q}$?
b) Vérifier que $\mathbb{Q}(\varepsilon_p, \alpha) : \mathbb{Q}$ est de degré fini et galoisienne.
c) Prouver que $[\mathbb{Q}(\varepsilon_p, \alpha) : \mathbb{Q}] = p(p-1)$. En conclure que $X^p - a$ est irréductible sur $\mathbb{Q}(\varepsilon_p)$.
d) On suppose $p \neq 2$. Soit $G := G(\mathbb{Q}(\varepsilon_p, \alpha) : \mathbb{Q})$; en choisissant deux éléments σ et τ dans deux sous-groupes convenables de G, montrer que le groupe G *n'est pas abélien.*
2°) Dans $\mathbb{Q}[X]$, on considère $X^4 - a$, avec $a > 0$.
a) Justifier l'existence d'une racine $4^{ème}$ de a, α, dans $\mathbb{R}$.
b) Démontrer que si a n'a pas de racine carrée dans $\mathbb{Q}$, alors $X^4 - a$ est irréductible sur

$\mathbb{Q}(i)$, où $i^2 = -1$ dans $\mathbb{C}$.
Montrer que dans ce cas, le groupe $G(\mathbb{Q}(i,\alpha) : \mathbb{Q})$ est *non abélien.*

17. Soit $\{p_1, p_2, \ldots, p_k\}$ une famille de *nombres premiers* distincts, où $k \in \mathbb{N}^*$.
Pour tout $j (1 \leq j \leq k)$, on note $\sqrt{p_j}$ la racine carrée *positive* de p_j dans $\mathbb{R}$ (Cf. App. A, Th. A.9.).
Etant donné un entier $n \geq 2$, on désigne par ε_n une racine $n^{ème}$ de l'unité, dans $\overline{\mathbb{Q}}$. On pose

$$T := \mathbb{Q}(\varepsilon_n, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}).$$

1°) a) Vérifier que l'extension $T : \mathbb{Q}$ est de degré fini et galoisienne.
b) Démontrer que le groupe $G(T : \mathbb{Q})$ est *abélien.*
2°) Soit $a > 0$ dans $\mathbb{Q}$ et $n > 2$ dans $\mathbb{N}$.
a) On suppose qu'il existe un nombre premier *impair* p tel que $p \mid a$. Démontrer que si a n'a pas de racine $p^{ème}$ dans $\mathbb{Q}$, alors a n'a pas de racine $p^{ème}$ dans T.
[On supposera qu'il existe $\alpha \in T$ tel que $\alpha^p = a$ et en considérant $G(\mathbb{Q}(\varepsilon_p, \alpha) : \mathbb{Q})$, on sera conduit à une contradiction (voir Ex. **16.** précédent).]
b) En supposant que $4 \mid n$, démontrer que, si a n'a pas de racine carrée dans $\mathbb{Q}$, alors a n'a pas de racine $4^{ème}$ dans T (voir Ex. **16.** précédent).
3°) Soit q un nombre premier quelconque. On suppose toujours $n > 2$.
a) Soit m un *diviseur* de n tel que $2 < m \leq n$.
Montrer, à l'aide des résultats précédents, que q n'a pas de racine $m^{ème}$ dans T [distinguer les cas où m a, ou n'a pas, de diviseur premier impair].
b) On pose $S := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k})$.
Compte tenu de l'hypothèse $m > 2$, montrer que q n'a pas de racine $m^{ème}$ dans S.
c) Démontrer, par récurrence sur n, que $[S : \mathbb{Q}] = 2^k$.
4°) On suppose $n > 2$ dans $\mathbb{N}$ et *n pair.*
Pour tout j, $1 \leq j \leq k$, $\sqrt[n]{p_j}$ désignant la racine $n^{ème}$ positive de p_j dans $\mathbb{R}$, on écrira aussi $\sqrt[n]{p_j}$ sous la forme $p_j^{\frac{1}{n}}$.
On considère l'ensemble

$$B_k = \{p_1^{\frac{r_1}{n}}, p_2^{\frac{r_2}{n}}, \ldots, p_k^{\frac{r_k}{n}}\},$$

où, pour tout j, $1 \leq j \leq k$, $0 \leq r_j \leq \frac{n}{2}$, dans $\mathbb{N}$.
a) Démontrer que $card\,(B_k) = (\frac{n}{2})^k$.
b) Prouver que $\mathbb{Q}(\sqrt[n]{p_1}, \sqrt[n]{p_2}, \ldots, \sqrt[n]{p_k}) = S(B_k)$, corps obtenu par l'adjonction à S, des éléments de B_k.
c) On pose $F_k := T(\sqrt[n]{p_1}, \sqrt[n]{p_2}, \ldots, \sqrt[n]{p_k})$.
En considèrant le polynôme $X^{\frac{n}{2}} - p_k^{\frac{1}{2}}$ dans $T[X]$, démontrer que

$$[F_k : F_{k-1}] = \frac{n}{2} \quad \text{(voir Ex. 17. précédent).}$$

En déduire que B_k est une base de F_k sur T.
d) Prouver que, pour tout entier $n > 2$ et *pair*, on a

$$[\mathbb{Q}(\sqrt[n]{p_1}, \sqrt[n]{p_2}, \ldots, \sqrt[n]{p_k}) : \mathbb{Q}] = n^k.$$

5°) Prouver que pour tout entier $n \geq 1$, on a

$$[\mathbb{Q}(\sqrt[n]{p_1}, \sqrt[n]{p_2}, \ldots, \sqrt[n]{p_k}) : \mathbb{Q}] = n^k.$$

18. Soit F_n le $n^{ème}$ nombre de Fermat (Rem. 7.41) :

$$F_n = 2^{2^n} + 1; \quad n \in \mathbb{N}.$$

Démontrer, par récurrence sur n, que

$$\forall n \in \mathbb{N}, \quad F_{n+1} = 2 + F_n F_{n-1} \cdots F_0.$$

En déduire que pour m et n dans $\mathbb{N}$,

$$m \neq n \Longrightarrow F_m \text{ et } F_n \text{ premiers entre eux.}$$

Montrer que ce résultat implique l'existence d'une infinité de nombres premiers.

19. *Construction du pentagone régulier*

Soit P_5 le pentagone régulier, inscrit dans le cercle trigonométrique du plan affine $\mathbb{R}^2$, identifié au plan complexe.

1°) Justifier les propriétés suivantes :

a) Pour construire (par la règle et le compas) le polygone P_5, il suffit de construire, dans le plan complexe, le point M d'affixe $\alpha := cos\frac{2\pi}{5} + i sin\frac{2\pi}{5}$.

b) α est une racine du polynôme $f(X)$ de $\mathbb{Q}[X]$, où

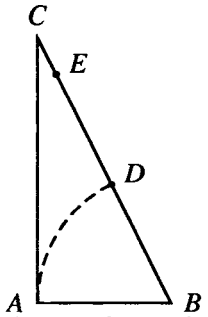
$$f(X) = X^4 + X^3 + X^2 + X + 1.$$

2°) Pour résoudre l'équation $f(X) = 0$, on pose $Y := X + \frac{1}{X}$.

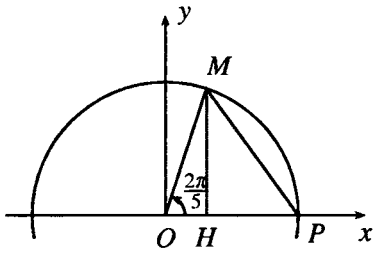
Calculer Y, en déduire que $cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$.

3°) On considère un triangle ABC, rectangle en A et tel que les longueurs des côtés vérifient $AB = 1$, $BC = 2$.

Construire, sur l'hypoténuse BC, le point E tel que $CE = \frac{\sqrt{5}-1}{4}$.



En déduire, la construction du point M, du cercle trigonométrique, d'angle polaire $\widehat{\overrightarrow{Ox}, \overrightarrow{OM}} = \frac{2\pi}{5}$.



Chapitre 8
Corps de nombres - Entiers algébriques

La connaissance des propriétés des *groupes abéliens libres de type fini* ([12], Ch. VIII) est nécessaire, pour ce chapitre.

1. Notion de corps de nombres

Définition 8.1. On appelle **corps de nombres** toute extension K de $\mathbb{Q}$, de degré fini.

Remarque 8.2. Soit K un corps de nombres tel que $[K:\mathbb{Q}] = n \geq 1$.
a) K est algébrique sur $\mathbb{Q}$, d'où $\mathbb{Q} \subseteq K \subset \overline{\mathbb{Q}} \subset \mathbb{C}$.
b) $\mathbb{Q}$ est un corps parfait, donc K est séparable sur $\mathbb{Q}$, par suite $K:\mathbb{Q}$ est une extension simple (Th. 3.31) ; supposons

$$K = \mathbb{Q}(\alpha) \quad \text{et} \quad p_\alpha(X) := Irr_{\mathbb{Q}}(\alpha, X).$$

Soit $E \subset \overline{\mathbb{Q}}$ un corps de décomposition de $p_\alpha(X)$ sur $\mathbb{Q}$; l'extension $E:\mathbb{Q}$ est galoisienne, de degré fini et les hypothèses impliquent

$$[K:\mathbb{Q}]_s = [K:\mathbb{Q}] = n = deg\, p_\alpha(X).$$

$\varphi_1, \varphi_2, \ldots, \varphi_n$ étant les $\mathbb{Q}$-monomorphismes de K dans $\overline{\mathbb{Q}}$, les éléments $\alpha_i := \varphi_i(\alpha)$, $1 \leq i \leq n$, sont, les n conjugués (Ch. 2 et Ch. 7) de α dans $\overline{\mathbb{Q}}$, c'est-à-dire les n racines distinctes de $p_\alpha(X)$ dans E, d'où, en posant $\varphi_1 := id_{/K}$,

$$E = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Exemple 8.3. 1) Les extensions suivantes sont des corps de nombres :
$\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{6})$, où $i^2 = -1$ dans $\mathbb{C}$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(j)$, où $j^3 = 1, j \neq 1$, dans $\mathbb{C}$.
2) Pour tout $n \in \mathbb{N}^*$, la $n^{ème}$ extension cyclotomique de $\mathbb{Q}$ (Ch.6) est un corps de nombres.

2. Discriminant d'une base d'un corps de nombres

Définition 8.4. Soit K un corps de nombres tel que $[K:\mathbb{Q}] = n \geq 1$.
Si $B := \{x_1, x_2, \ldots, x_n\}$ est une base de K sur $\mathbb{Q}$ et si $\varphi_1, \varphi_2, \ldots, \varphi_n$ désignent les $\mathbb{Q}$-monomorphismes de K dans $\overline{\mathbb{Q}}$, on appelle **discriminant** de la base B, l'élément de $\overline{\mathbb{Q}}$, noté $\Delta[x_1, x_2, \ldots, x_n]$ et défini par

$$\Delta[x_1, x_2, \ldots, x_n] := \left(\det(\varphi_i(x_j))\right)^2. \tag{8.1}$$

Changement de base
Les notations étant celles de la Déf. 8.4, soit $\{y_1, y_2, \ldots, y_n\}$ une autre base de K sur $\mathbb{Q}$; alors, pour tout j, $1 \leq j \leq n$,

$$y_j = \sum_{1 \leq i \leq n} c_{ij} x_i, \text{ où } c_{ij} \in \mathbb{Q},\ \forall i,\ 1 \leq i \leq n; \quad \det(c_{ij}) \neq 0.$$

Quels que soient l'élément y_j, $1 \leq j \leq n$, et le $\mathbb{Q}$-monomorphisme φ_k, $1 \leq k \leq n$, de K dans $\overline{\mathbb{Q}}$, on a

$$\varphi_k(y_j) = \sum_{1 \leq i \leq n} c_{ij}\varphi_k(x_i) \Longrightarrow \det\big(\varphi_k(y_j)\big) = \big(\det(c_{ij})\big)\big(\det(\varphi_k(x_i))\big),$$

$$\text{d'où,} \qquad \Delta[y_1, y_2, \ldots, y_n] = \big(\det(c_{ij})\big)^2 \Delta[x_1, x_2, \ldots, x_n]. \tag{8.2}$$

Remarque 8.5. Dans la formule de changement de base (8.2), $\big(det(c_{ij})\big)^2$ est le carré du déterminant de la matrice de passage de la base $\{x_1, \ldots, x_n\}$ à la base $\{y_1, \ldots, y_n\}$, d'où

$$\big(det(c_{ij})\big)^2 > 0, \quad \text{dans } \mathbb{Q}.$$

Théorème 8.6. *Soit $K = \mathbb{Q}(\alpha)$ un corps de nombres ; si $[K : \mathbb{Q}] = n$, quelle que soit la base $\{x_1, x_2, \ldots, x_n\}$ de K sur $\mathbb{Q}$,*

$$\Delta[x_1, x_2, \ldots, x_n] \in \mathbb{Q}^*.$$

Si tous les conjugués de α sont réels, on a alors $\Delta[x_1, x_2, \ldots, x_n] > 0$.

Démonstration. Pour prouver que $\Delta[x_1, x_2, \ldots, x_n] \in \mathbb{Q}^*$, il suffit de montrer (Rem. 8.5) que le discriminant d'une base particulière de K sur $\mathbb{Q}$, appartient à $\mathbb{Q}^*$.
Les hypothèses $K = \mathbb{Q}(\alpha)$ et $[K : \mathbb{Q}] = n$ entraînent que $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ forment une base de K sur $\mathbb{Q}$ (Th. 2.8).
Les φ_i, $1 \leq i \leq n$, étant les $\mathbb{Q}$-monomorphismes de K dans $\overline{\mathbb{Q}}$, posons

$$\begin{aligned} &\Delta := \Delta[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}] \quad \text{et} \quad \forall i,\ 1 \leq i \leq n,\ \alpha_i := \varphi_i(\alpha); \\ \text{alors,} \quad &\Delta = \big(\det(\varphi_i(\alpha^j))\big)^2 = \big(\det(\alpha_i^{\,j})\big)^2,\ 1 \leq i \leq n,\ 1 \leq j \leq n. \\ &= \big(V(\alpha_1, \alpha_2, \ldots, \alpha_n)\big)^2, \end{aligned}$$

où $V(\alpha_1, \alpha_2, \ldots, \alpha_n)$ désigne le *déterminant de Vandermonde* des α_i. Le calcul de ce déterminant ([13], Ex. **8.**, Ch. 8) nous donne

$$\Delta = (V(\alpha_1, \alpha_2, \ldots, \alpha_n))^2 = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \tag{8.3}$$

$V(\alpha_1, \alpha_2, \ldots, \alpha_n)$ est un polynôme à coefficients rationnels, *anti-symétrique* en $\alpha_1, \ldots, \alpha_n$, donc $\Delta = \big(V(\alpha_1, \alpha_2, \ldots, \alpha_n)\big)^2$ est un polynôme *symétrique* en les α_i, $1 \leq i \leq n$, qui sont les racines distinctes de $p_\alpha(X) = Irr_{\mathbb{Q}}(\alpha, X)$. Par suite ([13], Th. 8.14), il existe un polynôme

$$\phi \in \mathbb{Q}[X_1, X_2, \ldots, X_n] \text{ tel que } \Delta = \phi(s_1, s_2, \ldots, s_n),$$

où les s_k, $1 \leq k \leq n$, sont les polynômes symétriques élémentaires en $\alpha_1, \ldots, \alpha_n$ ([13], p.250). Supposons

$$p_\alpha(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0, \text{ dans } \mathbb{Q}[X],$$

alors les Relations entre les Coefficients et les Racines d'un polynôme ([13], p.259) donnent, avec $a_n = 1$,

$$s_1 = -a_{n-1},\ s_2 = a_{n-2},\ \ldots,\ s_k = (-1)^k a_{n-k},\ \ldots,\ s_n = (-1)^n a_0.$$

On en déduit que $\Delta \in \mathbb{Q}$ et d'après l'égalité (8.3), Δ est non nul, car les α_i sont deux à deux distincts. De plus, si tous les α_i, $1 \leq i \leq n$, sont réels, alors la relation (8.3) implique $\Delta > 0$. □

Remarque 8.7. Les notations étant celles de la preuve du Th. 8.6, l'égalité (8.3) montre que le discriminant Δ de la base $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ de K sur $\mathbb{Q}$ n'est autre que le *discriminant* des α_i, $1 \leq i \leq n$, tel qu'il a été défini dans "Eléments de Théorie des anneaux" ([13], p.250), ce qui, moyennant la formule du changement de base (8.2), justifie l'appellation « discriminant » utilisée dans la Déf. 8.4..
De plus, si l'on introduit la notion de *discriminant d'un polynôme* ([13], Déf. 8.50), alors, à partir du résultat ([13], Prop. 8.55) et de la relation (8.3) ci-dessus, on obtient

$$\Delta(1, \alpha, \alpha^2, \ldots, \alpha^n) = (-1)^{\frac{n(n-1)}{2}} \Delta(p_\alpha),$$

où $\Delta(p_\alpha) = \mathcal{R}(p_\alpha, p'_\alpha)$: résultant de p_α et de son polynôme dérivé p'_α.

3. Entiers algébriques

Définition 8.8. Un élément $\alpha \in \overline{\mathbb{Q}}$ est un **entier algébrique** s'il est racine d'un polynôme unitaire de $\mathbb{Z}[X]$.

Notations et Rappels.— Soit $\mathcal{A}$ l'ensemble des entiers algébriques, on a

$$\mathbb{Z} \subset \mathcal{A} \subset \overline{\mathbb{Q}} \subset \mathbb{C}.$$

A tout $\alpha \in \overline{\mathbb{Q}}$, on associe le morphisme d'anneaux unitaires

$$\begin{aligned} \lambda_\alpha : \mathbb{Z}[X] &\longrightarrow \overline{\mathbb{Q}} \\ f(X) &\longmapsto f(\alpha). \end{aligned}$$

On pose $\mathbb{Z}[\alpha] := Im\,\lambda_\alpha = \{f(\alpha)\ ;\ f(X) \in \mathbb{Z}[X]\}$.

On rappelle que la structure de groupe (additif) abélien coïncide avec la structure de $\mathbb{Z}$-module ([12], p.269). En particulier, un groupe (additif) abélien de type fini est un $\mathbb{Z}$-module de type fini.

Remarque 8.9. $\mathbb{Z}[\alpha]$ est un sous-anneau de $\overline{\mathbb{Q}}$, donc aussi de $\mathbb{C}$.
En particulier, $(\mathbb{Z}[\alpha], +)$ est un sous-groupe du groupe abélien $(\overline{\mathbb{Q}}, +)$ et, plus précisément, c'est le sous-$\mathbb{Z}$-module de $(\overline{\mathbb{Q}}, +)$ engendré par les α^i, $i \in \mathbb{N}$ (Cf. [12], Ch. VIII).

Théorème 8.10. *Compte tenu des notations définies précédemment, pour tout $\alpha \in \overline{\mathbb{Q}}$, les conditions suivantes sont équivalentes*
1) $\alpha \in \mathcal{A}$.
2) *Le groupe abélien $(\mathbb{Z}[\alpha], +)$ est de type fini.*
3) *Il existe un sous-anneau B de $\overline{\mathbb{Q}}$, contenant $\mathbb{Z}$ et α, qui est un groupe abélien de type fini.*

Démonstration. 1) $\Longrightarrow$ 2) Montrons que pour tout $\alpha \in \mathcal{A}$, le groupe abélien $(\mathbb{Z}[\alpha], +)$ est engendré par un nombre fini d'éléments ([12], Ch. VIII).
D'après la définition 8.8., $\alpha \in \mathcal{A}$ si et seulement s'il existe un nombre fini d'entiers, $c_0, c_1, \ldots, c_{n-1}$, non tous nuls dans $\mathbb{Z}$, tels que

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0. \tag{8.4}$$

On peut supposer que pour α fixé, le nombre n est minimal, donc, pour α non nul, on a $c_0 \neq 0$.

$$(8.4) \Longrightarrow \alpha^n = -(c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0).$$

Par suite, α^n appartient au sous-groupe de $(\mathbb{C},+)$ engendré par les $\alpha^i, 0 \leq i \leq n-1$, que l'on notera Γ. On en déduit que, d'une part, $\Gamma \subseteq \mathbb{Z}[\alpha]$ (Rem. 8.9.) et d'autre part, pour tout $j \in \mathbb{N}$, $\alpha^{n+j} \in \Gamma$, donc tout élément $f(\alpha) \in \mathbb{Z}[\alpha]$ appartient à Γ, ce qui entraîne $\mathbb{Z}[\alpha] = \Gamma$; ainsi le groupe abélien $(\mathbb{Z}[\alpha],+)$ est de type fini, engendré par $1, \alpha, \ldots, \alpha^{n-1}$.

2) $\Longrightarrow$ 3) Il suffit de prendre $B = \mathbb{Z}[\alpha]$.

3) $\Longrightarrow$ 1) Soit $\{x_1, \ldots, x_n\}$ une partie génératrice finie du groupe abélien B ; on a $B = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$ et B étant un sous-anneau de $\overline{\mathbb{Q}} \subset \mathbb{C}$,

$$\alpha \in B \Longrightarrow \alpha x_i \in B, \forall i, 1 \leq i \leq n, \quad \text{d'où,}$$

$$\forall i, 1 \leq i \leq n, \ \alpha x_i = \sum_{1 \leq j \leq n} a_{ij} x_j, \text{ où } a_{ij} \in \mathbb{Z}, \forall i, j.$$

Par suite, $(x_1, \ldots, x_n)$ est une solution du système homogène, que nous désignerons par (S), de n équations linéaires sur $\mathbb{Z} \subset \mathbb{Q}$, et n inconnues, dont la $i^{ème}$ équation est

$$\sum_{1 \leq j \leq n} (\delta_{ij}\alpha - a_{ij}) X_j = 0,$$

où δ_{ij} est le symbole de Kronecker ($\delta_{ij} = 0$ si $i \neq j$, et $\delta_{ii} = 1$).
Compte tenu des hypothèses, on peut supposer que les x_i, $1 \leq i \leq n$, sont non nuls, par suite, le déterminant du système homogène (S) est nul, donc,

$$det(\delta_{ij}\alpha - a_{ij}) = P(\alpha) = 0,$$

où $(-1)^n P(X)$ est le polynôme caractéristique de la matrice

$$A = (a_{ij})_{n \times n}, \text{ dans } M_n(\mathbb{Z}).$$

Le terme de plus haut degré du polynôme $P(X)$ étant X^n, on en déduit que α est racine du polynôme *unitaire* $P(X) \in \mathbb{Z}[X]$, donc $\alpha \in \mathcal{A}$ (Déf. 8.8). □

Théorème 8.11. *L'ensemble $\mathcal{A}$ des entiers algébriques est un sous-anneau unitaire de $\overline{\mathbb{Q}}$.*

Démonstration. On a $\mathbb{Z} \subset \mathcal{A}$; vérifions, d'autre part, que, quels que soient α et β dans $\mathcal{A}$, $\alpha + \beta$ et $\alpha\beta$ sont dans $\mathcal{A}$. Considérons

$$\mathbb{Z}[\alpha,\beta] := \{f(\alpha,\beta) \ ; \ f(X,Y) \in \mathbb{Z}[X,Y]\}.$$

$\mathbb{Z}[\alpha,\beta]$ est un sous-anneau de $\overline{\mathbb{Q}}$; montrons que $\mathbb{Z}[\alpha,\beta]$ est un $\mathbb{Z}$-module de type fini. Supposons que l'on ait, pour α et β,

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0, \ c_i \in \mathbb{Z}, \forall i, 0 \leq i \leq n-1 ;$$
$$\beta^m + d_{m-1}\beta^{m-1} + \cdots + d_1\beta + d_0 = 0, \ d_j \in \mathbb{Z}, \forall j, 0 \leq j \leq m-1.$$

On en déduit que, quel que soit $f(\alpha,\beta) \in \mathbb{Z}[\alpha,\beta]$,

$$f(\alpha,\beta) = \sum a_{ij}\alpha^i\beta^j, \ 0 \leq i \leq n-1, \ 0 \leq j \leq m-1, \ a_{ij} \in \mathbb{Z}, \forall i, j.$$

Par suite, le $\mathbb{Z}$-module $\mathbb{Z}[\alpha,\beta]$ est engendré par les éléments $\alpha^i\beta^j$, où $0 \leq i \leq n-1$ et $0 \leq j \leq m-1$, donc il est de type fini. Posons $B := \mathbb{Z}[\alpha,\beta]$; alors, l'équivalence des conditions 1) et 3) du Th. 8.10, implique que $\alpha + \beta$ et $\alpha\beta$ appartiennent à $\mathcal{A}$; on en conclut que $\mathcal{A}$ est un sous-anneau unitaire de $\overline{\mathbb{Q}}$. □

Définition 8.12. L'anneau $\mathcal{A}$ (Cf. Th. 8.11) est appelé **anneau des entiers algébriques.**

Théorème 8.13. *Un élément $\alpha \in \overline{\mathbb{Q}}$ est un entier algébrique si et seulement si le polynôme $Irr_{\mathbb{Q}}(\alpha,X) \in \mathbb{Z}[X]$.*

Démonstration. Posons $p_\alpha(X) := Irr_{\mathbb{Q}}(\alpha, X)$.
Si $p_\alpha(X) \in \mathbb{Z}[X]$, alors $\alpha \in \mathcal{A}$, car $p_\alpha(X)$ est unitaire.
Réciproquement, supposons $\alpha \in \mathcal{A}$; il existe alors un polynôme $f(X)$, *unitaire* dans $\mathbb{Z}[X]$, tel que $f(\alpha) = 0$.
On suppose que $f(X)$ est, dans $\mathbb{Z}[X]$, un polynôme de plus petit degré, annulé par α.

$$(f(X) \in \mathbb{Z}[X] \subset \mathbb{Q}[X]) \Longrightarrow p_\alpha(X) \mid f(X), \text{ dans } \mathbb{Q}[X] \Longrightarrow deg\, p_\alpha \leq deg\, f.$$

Dans $\mathbb{Q}[X]$, on peut écrire ([13], Lem. 5.106) $p_\alpha(X) = \frac{a}{b} q(X)$, où $\frac{a}{b} \in \mathbb{Q}^*$ et $q(X)$ est primitif dans $\mathbb{Z}[X]$ ([13], Déf. 5.102) ; alors, compte tenu de la minimalité du degré de $f(X)$,

$$(bp_\alpha(X) \in \mathbb{Z}[X] \quad \text{et} \quad bp_\alpha(\alpha) = 0) \Longrightarrow deg\, f \leq deg\, p_\alpha,$$

d'où $deg\, p_\alpha = deg\, f$. Par suite, dans $\mathbb{Q}[X]$,

$$p_\alpha(X) \mid f(X) \Longrightarrow f(X) = \lambda p_\alpha(X), \text{ où } \lambda \in \mathbb{Q}^*.$$

Les polynômes $f(X)$ et $p_\alpha(X)$ étant unitaires, on a $\lambda = 1$, donc $p_\alpha(X) \in \mathbb{Z}[X]$. □

Corollaire 8.14. $\mathcal{A} \cap \mathbb{Q} = \mathbb{Z}$.

Démonstration. On a $\mathbb{Z} \subseteq \mathcal{A} \cap \mathbb{Q}$ et d'après le Th. 8.13,

$$\alpha \in \mathcal{A} \cap \mathbb{Q} \Longrightarrow p_\alpha(X) = X - \alpha \Longrightarrow \alpha \in \mathbb{Z},$$

d'où le résultat énoncé. □

Corollaire 8.15. *Soit* $\alpha \in \mathcal{A}$.
1) *Tout conjugué de* α *appartient à* $\mathcal{A}$.
2) $N(\alpha) := N_{\mathbb{Q}(\alpha):\mathbb{Q}}(\alpha) \in \mathbb{Z}$ *et* $T(\alpha) := T_{\mathbb{Q}(\alpha):\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Démonstration. Le résultat 1) découle directement du Th. 8.13, puisque les conjugués de α sont, par définition, les racines de $p_\alpha(X)$.
2) $N(\alpha)$ et $T(\alpha)$ sont, respectivement, le produit et la somme des conjugués de α, donc des racines de $p_\alpha(X) \in \mathbb{Z}[X]$ (Th. 8.13) ; par suite, les Relations entre les Coefficients et les Racines d'un polynôme ([13], p.259) impliquent les résultats énoncés. □

Théorème 8.16. *Soit* $\alpha \in \overline{\mathbb{Q}}$ *; s'il existe un polynôme* unitaire $f(X)$, *dans* $\mathcal{A}[X]$, *tel que* $f(\alpha) = 0$, *alors* $\alpha \in \mathcal{A}$.

Démonstration. On suppose qu'il existe, dans $\mathcal{A}$, un nombre fini d'éléments $c_0, c_1, \ldots, c_{n-1}$, non tous nuls, tels que

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0. \tag{8.5}$$

Si $\alpha \neq 0$ et si l'entier n est minimal, alors on a $c_0 \neq 0$.
Chaque c_i étant un entier algébrique, pour tout i, $0 \leq i \leq n-1$, il existe un nombre fini d'entiers, $d_{i,0}, d_{i,1}, \ldots, d_{i,m_i-1}$, non tous nuls dans $\mathbb{Z}$, tels que

$$c_i^{m_i} + d_{i,m_i-1}c_i^{m_i-1} + \cdots + d_{i,1}c_i + d_{i,0} = 0. \tag{8.6}$$

Pour tout $c_i \neq 0$, on suppose l'entier m_i minimal ; d'où $d_{i,0} \neq 0$. Posons

$$\begin{aligned} B &:= \mathbb{Z}[c_0, \ldots, c_{n-1}] \\ &= \{f(c_0, \ldots, c_{n-1}) \,;\, f(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]\}. \end{aligned}$$

B est un sous-anneau unitaire de $\mathcal{A}$ et la relation (8.5) implique que α^n appartient au sous-B-module de $\overline{\mathbb{Q}}$ engendré par $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, que nous désignons par M.
Comme dans la preuve du Th. 8.10, on en déduit que toute puissance entière positive de α appartient à M, ce qui entraîne,

$$M = B[\alpha] = \{g(\alpha)\ ;\ g(X) \in B[X]\},\ \text{d'où}$$

$$\theta \in M \iff \theta = \sum_{0 \le l \le n-1} f_l(c_0, \ldots, c_{n-1})\alpha^l,$$

$$\forall l, 0 \le l \le n-1,\ f_l(c_0, \ldots, c_{n-1}) = \sum_j a_j c_0^{k_{j_0}} c_1^{k_{j_1}} \ldots c_{n-1}^{k_{j_{n-1}}},$$

où $j = (j_0, j_1, \ldots, j_{n-1}) \in \mathbb{N}^n$, les a_j étant presque tous nuls dans $\mathbb{Z}$.
Le groupe (additif) abélien $(M, +)$ est donc engendré par les

$$c_0^{k_{j_0}} c_1^{k_{j_1}} \ldots c_{n-1}^{k_{j_{n-1}}} \alpha^l,$$

pour lesquels, $0 \le l \le n-1$ et $\forall i, 0 \le i \le n-1, 0 \le k_{j_i} \le m_i - 1$ (Cf. Rel. (8.6)).
En conclusion, $M = \mathbb{Z}[c_0, \ldots, c_{n-1}][\alpha]$ est un sous-anneau unitaire de $\overline{\mathbb{Q}}$, contenant $\mathbb{Z}$ et α, et c'est un groupe additif abélien de type fini ; donc $\alpha \in \mathcal{A}$ (Th. 8.10). □

Proposition 8.17. 1) *Etant donné $\gamma \in \overline{\mathbb{Q}}$, il existe $c \in \mathbb{Z}^*$ tel que $c\gamma \in \mathcal{A}$.*
2) *$\overline{\mathbb{Q}}$ est le corps des fractions de $\mathcal{A}$.*

Démonstration. 1) On suppose $\gamma \neq 0$; γ est algébrique sur $\mathbb{Q}$; posons, dans $\mathbb{Q}[X]$,

$$p_\gamma(X) := Irr_{\mathbb{Q}}(\gamma, X) = X^r + \sum_{0 \le i \le r-1} \frac{a_i}{b_i} X^i.$$

Quel que soit i, $0 \le i \le r-1$, on a $(a_i, b_i) \in \mathbb{Z} \times \mathbb{Z}^*$ et $a_0 \neq 0$, car $p_\gamma(X)$ est irréductible sur $\mathbb{Q}$.
Soit c le *p.p.c.m.* positif des b_i, $0 \le i \le r-1$, dans $\mathbb{Z}$; pour tout i, il existe $s_i \in \mathbb{Z}^*$ tel que $c = b_i s_i$.
Posons, quel que soit i, $0 \le i \le r-1$, $a_i' := a_i s_i$, alors

$$p_\gamma(\gamma) = 0 \iff \gamma^r + \sum_{0 \le i \le r-1} \frac{a_i'}{c} \gamma^i = 0.$$

$$\iff (c\gamma)^r + \sum_{0 \le i \le r-1} c^{r-1-i} a_i' (c\gamma)^i = 0.$$

Par suite, l'élément $c\gamma$ de $\overline{\mathbb{Q}}$ est racine d'un polynôme unitaire de $\mathbb{Z}[X]$, donc $c\gamma \in \mathcal{A}$.
2) Notons $Fr\mathcal{A}$ le corps des fractions de $\mathcal{A}$.

$$\mathbb{Z} \subset \mathcal{A} \subset \overline{\mathbb{Q}} \Longrightarrow \mathbb{Q} \subset Fr\mathcal{A} \subseteq \overline{\mathbb{Q}}.$$

Soit $\gamma \in \overline{\mathbb{Q}}$; on suppose $\gamma \neq 0$. D'après la propriété 1), ci-dessus, il existe $c \in \mathbb{Z}^*$ tel que $c\gamma \in \mathcal{A}$; alors

$$\frac{1}{c} \in Fr\mathcal{A} \Longrightarrow \frac{1}{c} c\gamma = \gamma \in Fr\mathcal{A}\ ;$$

d'où, $Fr\mathcal{A} = \overline{\mathbb{Q}}$. □

4. Entiers algébriques d'un corps de nombres

A. Anneau des entiers algébriques d'un corps de nombres

Définition 8.18. Soit K un corps de nombres (Déf. 8.1) ; $\mathcal{A}$ étant l'anneau des entiers algébriques, l'anneau

$$\mathcal{D} := K \cap \mathcal{A}.$$

est appelé **anneau des entiers algébriques** du corps K.

Si aucune ambiguïté n'est possible, $\mathcal{D}$ pourra être simplement appelé l'anneau des **entiers** de K.

Remarque 8.19. L'anneau $\mathcal{D}$, sous-anneau du corps K, est un domaine d'intégrité ([13], Déf. 1.21) et

$$(\mathbb{Z} \subset \mathbb{Q} \subset K \quad \text{et} \quad \mathbb{Z} \subset \mathcal{A}) \Longrightarrow \mathbb{Z} \subset \mathcal{D}.$$

Théorème 8.20. *Si K est un corps de nombres, alors il existe un entier algébrique θ tel $K = \mathbb{Q}(\theta)$.*

Démonstration. On sait (Rem. 8.2) qu'il existe $\alpha \in \overline{\mathbb{Q}}$ tel que $K = \mathbb{Q}(\alpha)$.
Du 1) de la Prop. 8.17, on déduit qu'il existe $c \in \mathbb{Z}^*$ tel que

$$c\alpha \in \mathcal{A} \cap K = \mathcal{D}.$$

Montrons que $\mathbb{Q}(c\alpha) = \mathbb{Q}(\alpha) = K$.

$$c \in \mathbb{Z}^* \Longrightarrow c\alpha \in \mathbb{Q}(\alpha) \Longrightarrow \mathbb{Q}(c\alpha) \subseteq \mathbb{Q}(\alpha);$$
$$\alpha = \frac{1}{c} c\alpha \in \mathbb{Q}(c\alpha) \Longrightarrow \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(c\alpha),$$

d'où, en posant $\theta := c\alpha$, $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$, avec $\theta \in \mathcal{D}$. □

Définition 8.21. On appelle **corps quadratique** (ou **extension quadratique** de $\mathbb{Q}$) tout corps de nombres, de degré 2 sur $\mathbb{Q}$.

Proposition 8.22. *Tout corps quadratique K, est tel que $K = \mathbb{Q}(\sqrt{d})$, où $d \in \mathbb{Z}^* \setminus \{1\}$ et d n'est pas divisible par un carré $(\neq 1)$ dans $\mathbb{Z}$.*
Si $d > 1$, $\sqrt{d}$ désigne la racine carrée réelle, positive, de d.
Si $d \leq -1$, $\sqrt{d} := i\sqrt{|d|}$, où $i^2 = -1$, dans $\mathbb{C}$.

Démonstration. K est un corps de nombres, donc, d'après le Th. 8.20, il existe un entier algébrique θ tel que $K = \mathbb{Q}(\theta)$.
Soit $p_\theta(X) := Irr_{\mathbb{Q}}(\theta, X)$; par hypothèse, $[K : \mathbb{Q}] = 2$, d'où (Th. 8.13),

$$p_\theta(X) = X^2 + aX + b, \quad \text{où } a \text{ et } b \text{ sont dans } \mathbb{Z};$$

alors $\theta = \dfrac{-a \pm \sqrt{a^2 - 4b}}{2}$, où $\sqrt{a^2 - 4b}$ a la signification précisée dans l'énoncé.
Le polynôme $p_\theta(X)$ étant irréductible sur $\mathbb{Q}$, on a $\Delta := a^2 - 4b \neq 0$ et Δ n'est pas un carré dans $\mathbb{Z}$.
La factorisation dans $\mathbb{Z}$ entraîne qu'il existe m et d dans $\mathbb{Z}^*$ tels que $\Delta := a^2 - 4b = m^2 d$, où $d \in \mathbb{Z}^* \setminus \{1\}$ est non divisible par un carré. Par suite, compte tenu de la signification du symbole $\sqrt{d}$ donnée dans l'énoncé,

$$\theta = \frac{-a \pm m\sqrt{d}}{2};$$

d'où l'on déduit $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$. □

B. Bases entières d'un corps de nombres

Remarque 8.23. Pour tout corps de nombres K, il existe une base de K sur $\mathbb{Q}$ formée d'éléments de $\mathcal{D} = K \cap \mathcal{A}$.
En effet, si $[K:\mathbb{Q}] = n$ et si $\{\gamma_1, \ldots, \gamma_n\}$ est une base quelconque de K sur $\mathbb{Q}$, alors, d'après le 1) de la Prop. 8.17, quel que soit i, $1 \leq i \leq n$, il existe $c_i \in \mathbb{Z}^*$ tel que $c_i\gamma_i \in \mathcal{D}$.

$\{c_1\gamma_1, \ldots, c_n\gamma_n\}$ est alors une base de K sur $\mathbb{Q}$, formée d'éléments de $\mathcal{D}$.

Lemme 8.24. *Soit K un corps de nombres et $\mathcal{D} = \mathcal{A} \cap K$.*
Si $\{\theta_1, \ldots, \theta_n\}$ est une base de K sur $\mathbb{Q}$ telle que, quel que soit i, $1 \leq i \leq n$, $\theta_i \in \mathcal{D}$, alors $\Delta[\theta_1, \ldots, \theta_n] \in \mathbb{Z}^*$.

Démonstration. La Rem. 8.23 justifie l'existence d'une base de K sur $\mathbb{Q}$, vérifiant les hypothèses du lemme. Avec les notations de la Déf. 8.4, on a

$$\Delta[\theta_1, \ldots, \theta_n] = \big(det(\varphi_i(\theta_j))\big)^2 \in \mathbb{Q}^*.$$

j étant fixé ($1 \leq j \leq n$), pour $1 \leq i \leq n$, les $\varphi_i(\theta_j)$ sont les conjugués de θ_j, par suite (Cor. 8.15 et 8.14),

$$(\theta_j \in \mathcal{D} = \mathcal{A} \cap K) \Longrightarrow \varphi_i(\theta_j) \in \mathcal{A},$$

$$\text{d'où} \qquad \Delta[\theta_1, \ldots, \theta_n] \in \mathcal{A} \cap \mathbb{Q}^* = \mathbb{Z}^*. \qquad \square$$

Théorème 8.25. *Si K est un corps de nombres et $\mathcal{D}$ est l'anneau des entiers de K, alors $(\mathcal{D}, +)$ est un groupe* abélien libre *de rang fini $n := [K:\mathbb{Q}]$* ([12], Déf. 8.10).

Démonstration. D'après le Lem. 8.24, si tous les éléments d'une base de K sur $\mathbb{Q}$ sont des éléments de l'anneau $\mathcal{D}$, alors le discriminant de cette base est un entier non nul dans $\mathbb{Z}$.
Posons $n := [K:\mathbb{Q}]$ et considérons une base $\{\omega_1, \ldots, \omega_n\}$ de K sur $\mathbb{Q}$ telle que, quel que soit i, $1 \leq i \leq n$, $\omega_i \in \mathcal{D}$, et

$$|\,\Delta[\omega_1, \ldots, \omega_n]\,| \quad \text{minimal dans } \mathbb{N}^*. \tag{8.7}$$

Démontrons que tout élément $\theta \in \mathcal{D}$ s'écrit, de façon unique,

$$\theta = \sum_{1 \leq i \leq n} n_i\omega_i, \quad n_i \in \mathbb{Z}, \forall i,\ 1 \leq i \leq n. \tag{8.8}$$

S'il n'en était pas ainsi, il existerait $\theta \in \mathcal{D}$ tel que

$$\theta = \textstyle\sum_{1 \leq i \leq n} a_i\omega_i, \quad a_i \in \mathbb{Q}, \forall i,\ 1 \leq i \leq n,$$

les a_i n'étant pas tous dans $\mathbb{Z}$.
Supposons $a_1 \notin \mathbb{Z}$; il existe $a \in \mathbb{Z}$ et $r \in \mathbb{Q}$ tels que

$$a_1 = a + r \quad \text{et} \quad 0 < r < 1.$$

$$\text{Posons} \qquad \theta_1 = \theta - a\omega_1 \quad \text{et} \quad \theta_i = \omega_i, \forall i\,(2 \leq i \leq n).$$

$\{\theta_1, \ldots, \theta_n\}$ est encore une base de K, sur $\mathbb{Q}$, dont tous les éléments sont dans $\mathcal{D}$. Le déterminant de la matrice de passage de la base $\{\omega_1, \ldots, \omega_n\}$ à la base $\{\theta_1, \ldots, \theta_n\}$ est

$$\begin{vmatrix} a_1 - a & a_2 & a_3 & \ldots & a_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix} = a_1 - a = r.$$

La relation de changement de base (8.2) et la condition $0 < r < 1$ impliquent alors

$$|\Delta[\theta_1,\ldots,\theta_n]| = r^2\,|\Delta[\omega_1,\ldots,\omega_n]| < |\Delta[\omega_1,\ldots,\omega_n]|,$$

d'où une contradiction avec l'hypothèse (8.7).
La condition (8.8) exprime alors que $\{\omega_1,\ldots,\omega_n\}$ est une *base* du groupe abélien $(\mathcal{D},+)$, qui est donc *libre, de rang n* ([12], Th. 8.18). □

Définition 8.26. K étant un corps de nombres, une base $\{\omega_1,\ldots,\omega_n\}$ de K sur $\mathbb{Q}$, formée d'éléments $\omega_i \in \mathcal{D}$ et qui, de plus, est une base du groupe abélien libre $(\mathcal{D},+)$, est appelée une **base entière** de K.

Remarque 8.27. Toute base du groupe abélien (ou $\mathbb{Z}$-module) libre, $(\mathcal{D},+)$, est une base de K sur $\mathbb{Q}$.
En effet, supposons $n = [K:\mathbb{Q}]$; si $\{\omega_1,\ldots,\omega_n\}$ est une base de $(\mathcal{D},+)$, alors les ω_i sont linéairement indépendants sur $\mathbb{Z}$, donc sur $\mathbb{Q}$; ainsi $\{\omega_1,\ldots,\omega_n\}$ est une base de K sur $\mathbb{Q}$.
Par contre, une base de K, sur $\mathbb{Q}$, formée d'éléments de $\mathcal{D}$, n'est pas nécessairement une base entière de K.
Par exemple, si $K = \mathbb{Q}(\sqrt{5})$, alors $\{1,\sqrt{5}\}$ est une base de K sur $\mathbb{Q}$, où 1 et $\sqrt{5}$ sont des entiers de K. Cependant $\{1,\sqrt{5}\}$ n'est pas une base entière de K, puisque ce n'est pas une base du $\mathbb{Z}$-module $(\mathcal{D},+)$, car on a (Ex. **2.**, Ch. 8)

$$\mathcal{D} \neq \mathbb{Z}[\sqrt{5}] := \{a+b\sqrt{5}\,;\, a,b \text{ dans } \mathbb{Z}\}.$$

En effet, $\frac{1}{2}+\frac{1}{2}\sqrt{5}$ est racine du polynôme X^2-X-1, donc est un élément de $\mathcal{D}$, qui n'appartient pas à $\mathbb{Z}[\sqrt{5}]$.
La proposition suivante montrera que $\{1,\frac{1}{2}+\frac{1}{2}\sqrt{5}\}$ est une base entière de K.

Proposition 8.28. *K étant un corps de nombres, si $\{\theta_1,\ldots,\theta_n\}$ est une base de K sur $\mathbb{Q}$ telle que, pour tout i, $1 \le i \le n$, $\theta_i \in \mathcal{D}$ et si, de plus, $\Delta[\theta_1,\ldots,\theta_n]$* n'est pas divisible par un carré (> 1) *dans $\mathbb{Z}$, alors $\{\theta_1,\ldots,\theta_n\}$ est une base entière de K (mais la réciproque est fausse).*

Démonstration. Considérons une base entière $\{\beta_1,\ldots,\beta_n\}$ de K. Par hypothèse, pour tout i, $1 \le i \le n$, $\theta_i \in \mathcal{D}$, donc

$$\theta_i = \sum_{1\le j\le n} c_{ij}\beta_j, \text{ où } c_{ij} \in \mathbb{Z},\ \forall i,j \quad \text{et} \quad \det(c_{ij}) \neq 0.$$

La formule du changement de base (8.2) donne alors,

$$\Delta[\theta_1,\ldots,\theta_n] = \big(det(c_{ij})\big)^2\Delta[\beta_1,\ldots,\beta_n].$$

Or, $\Delta[\theta_1,\ldots,\theta_n] \in \mathbb{Z}^*$ (Lem. 8.24.) et n'est pas divisible par un carré (> 1), donc

$$\big(det(c_{ij})\big)^2 = 1.$$

Ainsi, le déterminant de la matrice de passage de la base $\{\beta_1,\ldots,\beta_n\}$ à la base $\{\theta_1,\ldots,\theta_n\}$ est égal à ± 1.
On en conclut que $\{\theta_1,\ldots,\theta_n\}$ est, comme $\{\beta_1,\ldots,\beta_n\}$, une base du groupe abélien libre $(\mathcal{D},+)$ ([12], p.298), donc une base entière de K. □

Exemple 8.29. Montrons que $B := \{1,\frac{1}{2}+\frac{1}{2}\sqrt{5}\}$ est une base entière de $K = \mathbb{Q}(\sqrt{5})$ (Cf. Rem 8.27). B est une base de K sur $\mathbb{Q}$, dont les éléments sont des entiers de K (Rem. 8.27) et

$$\Delta[1,\frac{1}{2}+\frac{1}{2}\sqrt{5}] = \left(\begin{vmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{5} \\ 1 & \frac{1}{2}-\frac{1}{2}\sqrt{5} \end{vmatrix}\right)^2 = 5.$$

D'après la Prop. 8.28, B est une base entière de $K = \mathbb{Q}(\sqrt{5})$.

Théorème 8.30. *Soit K un corps de nombres et $\mathcal{D}$ l'anneau des entiers algébriques de K.*
1) *K est le corps des fractions du domaine d'intégrité $\mathcal{D}$.*
2) *$\mathcal{D}$ est noethérien.*
3) *Tout idéal premier, non nul, de $\mathcal{D}$ est maximal.*

Démonstration. Soit $n := [K : \mathbb{Q}] \geq 1$.
1) $\mathcal{D}$ est un D.I. (Rem. 8.19) ; soit $K' := Fr\mathcal{D}$ son corps de fractions ([13], Déf. 5.2).

$$\mathbb{Z} \subseteq \mathcal{D} \Longrightarrow \mathbb{Q} \subseteq K' \subseteq K,$$

car K' est le plus petit corps contenant $\mathcal{D}$ ([13], Rem. 5.8)
Mais, d'après le Th. 8.20, il existe $\theta \in \mathcal{D}$ tel que $K = \mathbb{Q}(\theta)$; on a alors

$$K = \mathbb{Q}(\theta) \subseteq K', \text{ par suite, } K' = K \text{ ; donc } K = Fr\mathcal{D}.$$

2) Soit I un idéal non nul de $\mathcal{D}$.
$(I, +)$ est un sous-groupe de $(\mathcal{D}, +)$, donc $(I, +)$ est un groupe abélien libre de rang fini $m \leq n$ [(Th. 8.25) et ([12], Th. 8.54)].
Soit $\{x_1, \ldots, x_m\}$ une $\mathbb{Z}$-base de I ; alors, I est l'idéal $(x_1, \ldots, x_m)$ de $\mathcal{D}$, engendré les x_i, $1 \leq i \leq m$; ainsi, tout idéal de $\mathcal{D}$ est de type fini, donc $\mathcal{D}$ est un anneau noethérien.
3) Soit P un idéal premier ([13], Déf. 2.50) non nul, de $\mathcal{D}$.
On vérifie alors, que $P \cap \mathbb{Z}$ est un idéal premier, non nul de $\mathbb{Z}$, d'où $P \cap \mathbb{Z} = p\mathbb{Z}$, où p est un nombre premier. Par suite,

$$\mathbb{Z}/P \cap \mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \quad \text{est le corps fini de cardinal } p.$$

Notons δ l'injection canonique de $\mathbb{Z}$ dans $\mathcal{D}$ et considérons les surjections canoniques

$$\sigma : \mathbb{Z} \longrightarrow \mathbb{Z}/P \cap \mathbb{Z} \quad \text{et} \quad \tau : \mathcal{D} \longrightarrow \mathcal{D}/P.$$

On a $Ker(\tau \circ \delta) = P \cap \mathbb{Z}$ et δ injectif, donc il existe un morphisme *injectif* $\overline{\delta}$ de $\mathbb{Z}/P \cap \mathbb{Z}$ dans $\mathcal{D}/P$ tel que le diagramme suivant commute ([13], Lem. 2.37, Rem. 2.38)

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\delta} & \mathcal{D} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \tau} \\ \mathbb{Z}/P \cap \mathbb{Z} & \xrightarrow{\overline{\delta}} & \mathcal{D}/P \end{array}$$

donc $\tau \circ \delta = \overline{\delta} \circ \sigma$.
On en déduit que $\mathcal{D}/P$ contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$; on peut alors considérer $\mathcal{D}/P$ comme un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.
$\mathcal{D}$ étant un $\mathbb{Z}$-module de type fini (Th. 8.25), $\mathcal{D}/P$ est un espace vectoriel de dimension finie sur $\mathbb{Z}/p\mathbb{Z}$. Or, $\mathbb{Z}/p\mathbb{Z}$ est un corps fini, par suite, $\mathcal{D}/P$ est de cardinal fini.
Il en résulte que $\mathcal{D}/P$ est un *D.I.* fini, donc un corps ([13], Prop. 1.24) ; on en déduit que P est un idéal maximal de $\mathcal{D}$ ([13], Th. 2.62). □

Les propriétés de l'anneau des entiers algébriques d'un corps de nombres nous amènent à introduire, dans le paragraphe suivant, les notions d'anneau intégralement clos et d'anneau de Dedekind ([42]).

5. Anneaux intégralement clos – Anneaux de Dedekind

A. Généralisation de la notion d'entiers algébriques

On écrira couramment que A est un D.I. (resp. D.P.) pour exprimer que A est un domaine d'intégrité (resp. domaine principal) ([13], Ch. 5) ; on notera alors FrA le corps des frac-

tions de A ([13], Déf. 5.2).

Définition 8.31. Soit R un anneau unitaire commutatif ; si A est un sous-anneau unitaire de R, un élément $\alpha \in R$ est dit **entier sur** A s'il existe un polynôme unitaire, non constant $f(X) \in A[X]$ tel que $f(\alpha) = 0$.
L'anneau R sera dit **entier sur** A, si tout élément de R est entier sur A.

Les hypothèses de la Déf. 8.31, impliquent que $A[\alpha] = \{f(\alpha)\ ;\ f(X) \in A[X]\}$ est un sous-anneau de R.

Proposition 8.32. *Dans le contexte de la Def.* 8.31,
1) *Les trois conditions suivantes sont équivalentes,*
– *i) L'élément α de R est entier sur A.*
– *ii) Le groupe abélien $(A[\alpha], +)$ est de type fini.*
– *iii) Il existe un sous-anneau B de R, contenant A et α, tel que le groupe $(B, +)$ est de type fini.*
2) *L'ensemble, noté A', des éléments de R, entiers sur A, est un sous-anneau de R, appellé* **fermeture intégrale** *de A dans R.*

Même démonstration que pour les Th. 8.10 et 8.11.

B. Anneaux intégralement clos

Définition 8.33. Soit A un D.I. et $K := FrA$.
a) L'anneau A' des entiers de K sur A (c'est-à-dire la fermeture intégrale de A dans FrA) est appelé la **clôture intégrale** de A dans K.
b) Si $A = A'$, on dit que A est un anneau **intégralement clos**.

Exemple 8.34. L'anneau $\mathbb{Z}$ est intégralement clos, car la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}$ est $\mathcal{A} \cap \mathbb{Q} = \mathbb{Z}$ (Cor. 8.14).

Théorème 8.35. *Si K est un corps de nombres* (Déf. 8.1)*, alors l'anneau $\mathcal{D} = \mathcal{A} \cap K$ est intégralement clos.*

Démonstration. $\mathcal{D}$, sous-anneau du corps K, est un D.I. et K est le corps des fractions de $\mathcal{D}$ (Th. 8.30).
Vérifions que tout élément α de K, entier sur $\mathcal{D}$, appartient à $\mathcal{D}$.
En effet, $\alpha \in K$ implique $\alpha \in \overline{\mathbb{Q}}$ et si α est entier sur $\mathcal{D}$, il existe alors, un polynôme unitaire $f(X) \in \mathcal{D}[X]$ tel que $f(\alpha) = 0$. Or, $\mathcal{D} = \mathcal{A} \cap K$, par suite,
$f(X) \in \mathcal{A}[X]$, donc $\alpha \in \mathcal{A}$ (Th. 8.16), d'où $\alpha \in \mathcal{A} \cap K = \mathcal{D}$. □

Proposition 8.36. *Tout anneau factoriel est intégralement clos.*

Démonstration. Soit A un anneau factoriel ; A est donc un D.I. ([13], Déf. 7.87). Soit $K := FrA$ et A' la clôture intégrale de A dans K (Déf. 8.33). Etant donné $\alpha \in A' \setminus A$, il existe, dans A, des éléments non tous nuls c_i, $(1 \leq i \leq n-1), n \in \mathbb{N}^*$,
tels que

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0. \tag{8.9}$$

$$\alpha \in A' \setminus A \Longrightarrow \alpha = \frac{a}{b},\ (a,b) \in A \times A^*,\ b \notin U_A,\ a \wedge b = 1$$

$$\text{alors}\quad (8.9) \iff a^n + b(c_{n-1}a^{n-1} + \cdots + c_1 ab^{n-2} + c_0 b^{n-1}) = 0.$$

On en déduit que $b \mid a^n$ dans l'anneau factoriel A, ce qui contredit les hypothèses $a \wedge b = 1$ et $b \notin U_A$, donc $\alpha \in A$.
La réciproque de ce théorème est fausse (Ex. **4.**, Ch. 8). □

Corollaire 8.37. *Tout domaine principal, donc tout anneau euclidien, est intégralement clos.*

Démonstration. Cette propriété résulte directement de la Prop. 8.36, puisque tout anneau euclidien est un D.P. et tout D.P. est anneau factoriel ([13], Ch. 5). □

C. Anneaux de Dedekind

Définition 8.38. On dit qu'un domaine d'intégrité A est un **anneau de Dedekind** , si
i) A est noethérien et intégralement clos.
ii) Tout idéal premier non nul de A est maximal.

Exemple 8.39. 1) $\mathbb{Z}$ est un anneau de Dedekind.
En effet, $\mathbb{Z}$ est un D.I. noethérien (car principal, [13], p.54) dans lequel tout idéal premier non nul est maximal ([13], Th. 2.66). De plus $\mathbb{Z}$ est intégralement clos (Exemple 8.34.)
2) L'anneau $\mathcal{D}$ des entiers d'un corps de nombres K, est un anneau de Dedekind (Th. 8.30 et 8.35).

Remarque 8.40. a) La condition « tout idéal premier non nul est maximal » est vraie dans tout D.P. ([13], Th. 2.66), mais il existe des anneaux de Dedekind non principaux, car non factoriels (Ex. **4.**, Ch. 8).
b) La condition ii) de la Déf. 8.38 montre qu'un corps n'est pas un anneau de Dedekind.

D. Idéaux fractionnaires d'un D.I.

1/ Monoïde des idéaux d'un D.I.

Définition 8.41. On appelle **monoïde**, tout ensemble muni d'une loi de composition interne associative, pour laquelle il existe un élément neutre ([12], Déf. 1.1).
Si, de plus, la loi de composition est commutative, alors le monoïde est dit commutatif.

On rappelle ([13], Prop. 2.20) que, l'ensemble $\mathcal{I}$ des idéaux d'un anneau unitaire, commutatif, est muni d'un produit, tel que

$$\forall (I_1, I_2) \in \mathcal{I} \times \mathcal{I}, \quad I_1 I_2 = \Big\{ \sum_{finie} x_{i_1} x_{i_2} \, ; \, x_{i_1} \in I_1, \, x_{i_2} \in I_2 \Big\}.$$

Le produit des idéaux d'un anneau unitaire, commutatif A est associatif et commutatif ([13], Déf. 2.19, Prop. 2.22, Rem. 2.23) ; de plus, pour tout idéal I de A, on a

$$IA = AI = I.$$

On en conclut que *l'ensemble des idéaux d'un anneau unitaire, commutatif, muni du produit des idéaux, est un monoïde commutatif.*

Lemme 8.42. *Tout idéal propre, non nul d'un D.I. noethérien A (qui n'est pas un corps) contient un produit d'idéaux premiers non nuls de A.*

Démonstration. En vue d'un raisonnement par l'absurde, on suppose que la famille $\mathcal{T}$ des idéaux propres, non nuls de A, *ne contenant pas un produit d'idéaux premiers non nuls*, est non vide ; ceci implique, en particulier, qu'un idéal quelconque $I \in \mathcal{T}$ n'est pas premier.
L'anneau A est noethérien, donc la famille $\mathcal{T}$, ordonnée par l'inclusion, contient un élément maximal, I_0 ([13], Déf. 2.79).
L'idéal I_0 n'est pas premier, par suite, il existe x, y dans $A \setminus I_0$, tels que $xy \in I_0$.

I_0 étant maximal dans $\mathcal{T}$, les idéaux $Ax+I_0$ et $Ay+I_0$ n'appartiennent pas à la famille $\mathcal{T}$; par suite, chacun d'eux contient un produit d'idéaux premiers non nuls, soit :

$$P_1P_2\dots P_r \subseteq Ax+I_0, \quad Q_1Q_2\dots Q_s \subseteq Ay+I_0.$$
$$xy \in I_0 \Longrightarrow (Ax+I_0)(Ay+I_0) \subseteq I_0 \Longrightarrow P_1P_2\dots P_rQ_1Q_2\dots Q_s \subseteq I_0,$$

ce qui est en contradiction avec la condition $I_0 \in \mathcal{T}$, d'où le lemme. □

2/ Monoïde des idéaux fractionnaires d'un D.I.

Définition 8.43. Soit A un D.I. et $K := FrA$. On appelle **idéal fractionnaire** de A, tout sous-A-module J de K, tel qu'il existe $c \in A^* = A \setminus \{0\}$ vérifiant $J \subseteq c^{-1}A$.

Remarque 8.44. a) Dans les conditions de la Déf. 8.43,

$$J \subseteq c^{-1}A \iff cJ \subseteq A,$$

ce que l'on peut exprimer, en disant que les éléments de l'idéal fractionnaire $J \subseteq K$ ont un *dénominateur commun*, c.

$$I := cJ \text{ est alors un idéal de } A.$$

b) Tout idéal de A est un idéal fractionnaire de A.

c) Pour un idéal fractionnaire J de A, l'élément $c \in A^*$ vérifiant $cJ \subseteq A$, n'est pas unique, car

$$cJ \subseteq A \Longrightarrow acJ \subseteq A, \forall a \in A^*.$$

Exemple 8.45. Les idéaux fractionnaires de l'anneau $\mathbb{Z}$ sont les $q\mathbb{Z}$, pour $q \in \mathbb{Q}$.

$\mathcal{I}$ désignant l'ensemble des idéaux d'un domaine d'intégrité A, on notera $\mathcal{F}$ l'ensemble des idéaux fractionnaires de A. On a $\mathcal{I} \subseteq \mathcal{F}$.

Pour J_1, J_2 dans $\mathcal{F}$, il existe c_1, c_2 dans A^* et I_1, I_2 dans $\mathcal{I}$ tels que

$$J_1 = c_1^{-1}I_1 \quad \text{et} \quad J_2 = c_2^{-1}I_2.$$

On définit alors le produit des idéaux fractionnaires J_1, J_2, par

$$J_1J_2 := (c_1c_2)^{-1}I_1I_2.$$

On vérifie facilement que, relativement à ce produit, l'ensemble $\mathcal{F}$ est muni d'une *structure de monoïde commutatif* induite par celle de l'ensemble $\mathcal{I}$ (voir par. **1.**).

Proposition 8.46. *Soit A un D.I. et $K := FrA$.*

1) *Tout sous-A-module de* type fini *de K est un idéal fractionnaire de A.*

2) *Si A est* noethérien, *alors, tout idéal fractionnaire de A est un sous-A-module de type fini de K.*

Démonstration. 1) Soit J un sous-A-module de type fini de K et $\{x_1, \dots, x_n\}$ une partie génératrice finie de J ; alors, $J = \sum_{1 \le i \le n} Ax_i$.

$$\forall i (1 \le i \le n), x_i \in K \Longrightarrow x_i = \frac{a_i}{b_i}, (a_i, b_i) \in A \times A^*, a_i \wedge b_i = 1.$$
$$c := \prod_{1 \le i \le n} b_i \Longrightarrow c \neq 0 \text{ et } cx_i \in A, \forall i (1 \le i \le n),$$
$$\Longrightarrow c \neq 0 \text{ et } cJ \subseteq A,$$

donc J est un idéal fractionnaire de A. On a $cJ = I$, où I est l'idéal de type fini de A, engendré par les $x_i' := cx_i$, $1 \le i \le n$.

2) On suppose A noethérien. Soit J un idéal fractionnaire de A ; montrons que J est un sous-A-module de type fini de K.
En effet, il existe $c \in A^*$ tel que $J \subseteq c^{-1}A$; $c^{-1}A$ est un sous-A-module de K, isomorphe à A, donc de type fini, par suite $c^{-1}A$ est un A-module noethérien ([13], Cor. 3.80), ce qui entraîne que J, sous-A-module de $c^{-1}A$, est de type fini ([13], Th. 3.76). □

E. Idéaux fractionnaires d'un anneau de Dedekind

Dans tout ce paragraphe, on désigne par D, un anneau de Dedekind et $K := FrD$.
Les lemmes suivants ont pour but la preuve des Th. 8.50 et 8.51
Etant donné un idéal I de D, on pose

$$I' = \{\alpha \in K \,;\, \alpha I \subseteq D\}. \tag{8.10}$$

On remarque que pour des idéaux I_1, I_2 de D,

$$I_1 \subseteq I_2 \Longrightarrow I_2' \subseteq I_1'. \tag{8.11}$$

Lemme 8.47. *a) Pour tout idéal I de D, I' est un* idéal fractionnaire *de D tel que*

$$D \subseteq I' \quad \textit{et} \quad II' \textit{ est un idéal de } D.$$

b) Si I est un idéal propre, non nul *de D, alors* $D \subsetneq I'$.

Démonstration. Le cas $I = (0)$ est trivial, on suppose $I \neq (0)$.
a) On vérifie que I', défini par la Rel. (8.10), est un sous-D-module de K, contenant D.
D'autre part, pour tout $c \neq 0$, dans I, on a $cI' \subseteq D$, donc I' est un idéal fractionnaire de D tel que $II' \subseteq D$ et II' est un idéal de D.
b) On suppose I non nul et $I \neq D$. Il existe alors un idéal maximal $\mathcal{M}$ de D, contenant I ([13], Cor. 2.71). Soit $\mathcal{M}'$, l'idéal fractionnaire de D associé à l'idéal $\mathcal{M}$ (Rel. 8.10). D'après le résultat a) et la Rel. (8.11), on a

$$I \subseteq \mathcal{M} \Longrightarrow D \subseteq \mathcal{M}' \subseteq I'.$$

Pour prouver que $I' \neq D$, il suffit de montrer, que pour l'idéal maximal $\mathcal{M}$, on a $\mathcal{M}' \neq D$.
Soit $a \neq 0$, dans $\mathcal{M}$; d'après le Lem. 8.42., l'idéal principal (a) contient un produit d'idéaux *premiers*, non nuls, P_i, $1 \leq i \leq r$ de D :

$$P_1 P_2 \ldots P_r \subseteq (a) \subseteq \mathcal{M}. \tag{8.12}$$

Or, l'idéal maximal $\mathcal{M}$ est premier ([13], Cor. 2.64), par suite ([13], Prop. 2.55),

$$P_1 P_2 \ldots P_r \subseteq \mathcal{M} \Longrightarrow \exists i (1 \leq i \leq r) \text{ tel que } P_i \subseteq \mathcal{M}.$$

Moyennant, éventuellement, une permutation des indices i, on peut supposer $P_1 \subseteq \mathcal{M}$.
Dans l'anneau de Dedekind D, tout idéal premier non nul est maximal (Déf. 8.38), donc

$$P_1 \subseteq \mathcal{M} \Longrightarrow P_1 = \mathcal{M}.$$

D'autre part, si l'on suppose que, dans la relation (8.12), l'entier $r \geq 1$ est minimal, c'est-à-dire que tout produit d'idéaux premiers, non nuls, inclus dans (a), comporte au moins r facteurs, alors on a

$$\mathcal{M} P_2 \ldots P_r \subseteq (a) \quad \text{et} \quad P_2 \ldots P_r \nsubseteq (a).$$

On en déduit qu'il existe $b \in D$, tel que

$$b \in P_2 \ldots P_r \quad \text{et} \quad b \notin (a).$$
$$b\mathcal{M} \subseteq (a) = aD \Longrightarrow a^{-1} b \mathcal{M} \subseteq D \Longrightarrow a^{-1} b \in \mathcal{M}'.$$
Mais, $b \notin aD \Longrightarrow a^{-1} b \notin D$, d'où $\mathcal{M}' \neq D$.

□

Lemme 8.48. *Soit I est un idéal non nul de D et T une partie non vide de K, alors*

$$TI \subseteq I \Longrightarrow T \subseteq D.$$

Démonstration. L'anneau de Dedekind D est noethérien (Déf. 8.38), par suite, l'idéal $I \neq (0)$ est de type fini ; supposons

$$I = (x_1, x_2, \ldots, x_n), \quad \text{avec, } \forall i (1 \leq i \leq n),\ x_i \neq 0 \text{ dans } D.$$

Soit $\alpha \in T$, l'hypothèse implique $\alpha I \subseteq I$; alors, pour i, $1 \leq i \leq n$, il existe des éléments $b_{ij} \in D \subseteq K$, $1 \leq j \leq n$, tels que

$$\alpha x_i = \sum_{1 \leq j \leq n} b_{ij} x_j. \tag{8.13}$$

Ainsi, $\{x_1, \ldots, x_n\}$ est une solution du système homogène de n équations linéaires sur $D \subseteq K$, à n inconnues, dont la $i^{ème}$ équation est

$$\sum_{1 \leq j \leq n} (\delta_{ij}\alpha - b_{ij}) X_j = 0.$$

On en déduit (par un raisonnement déjà utilisé dans la preuve du Th. 8.10) que α est racine d'un polynôme unitaire de $D[X]$; or, l'anneau de Dedekind D est intégralement clos (Déf. 8.38), donc $\alpha \in D$. □

Lemme 8.49. *Tout idéal maximal $\mathcal{M}$ de D est inversible dans le monoïde commutatif $\mathcal{F}$ des idéaux fractionnaires de D.*

Démonstration. Soit $\mathcal{M}$ un idéal maximal de D et $\mathcal{M}'$ l'idéal fractionnaire qui lui est associé (Rel. (8.10)). Démontrons que, dans le monoïde $\mathcal{F}$, dont l'élément unité est D, on a $\mathcal{M}\mathcal{M}' = D$.

D'après le Lem. 8.47, on a $D \subsetneq \mathcal{M}'$ et $\mathcal{M}\mathcal{M}'$ est un idéal de D, alors,

$$(D \subsetneq \mathcal{M}' \text{ et } \mathcal{M} = \mathcal{M}D) \Longrightarrow \mathcal{M} \subseteq \mathcal{M}\mathcal{M}' \subseteq D.$$

Or, $\mathcal{M}$ est un idéal maximal, d'où

$$\mathcal{M}\mathcal{M}' = \mathcal{M} \quad \text{ou} \quad \mathcal{M}\mathcal{M}' = D.$$

D'après le Lem. 8.48, l'égalité $\mathcal{M}\mathcal{M}' = \mathcal{M}'\mathcal{M} = \mathcal{M}$ entraîne $\mathcal{M}' \subseteq D$, ce qui contredit le Lem. 8.47. On en conclut que

$$\mathcal{M}\mathcal{M}' = D.$$

Ainsi, $\mathcal{M}'$ est l'inverse de l'idéal maximal $\mathcal{M}$ dans le monoïde commutatif $\mathcal{F}$. □

Théorème 8.50. *Le monoïde des idéaux fractionnaires non nuls d'un anneau de Dedekind est un groupe abélien.*

Démonstration. On conserve les notations précédentes.

1°) Démontrons que pour tout idéal $I \neq (0)$ de D on a $II' = D$, I' étant l'idéal fractionnaire défini par (8.10).

La propriété a été prouvée dans le cas où I est maximal (Lem. 8. 49).

Supposons que l'ensemble, noté E, des idéaux non nuls I de D, pour lesquels $II' \neq D$, soit non vide.

L'anneau de Dedekind D étant noethérien, l'ensemble E contient au moins un *élément maximal*, que l'on note I.

D'après le Lem. 8.47, I n'est pas un idéal maximal de D, donc il existe un *idéal maximal* $\mathcal{M}$ de D tel que

$$I \subsetneq \mathcal{M}.$$

Soit $\mathcal{M}'$ l'idéal fractionnaire associé à $\mathcal{M}$ par la Rel. (8.10). En appliquant les lemmes précédents on obtient

$$D \subsetneq \mathcal{M}' \subseteq I' \Longrightarrow I \subseteq I\mathcal{M}' \subseteq II' \subseteq D.$$

$I \subseteq I\mathcal{M}' \subseteq D$ montre que $I\mathcal{M}'$ est un idéal de D contenant I.
On ne peut avoir $I = I\mathcal{M}'$, car, d'après le Lem. 8.48, cette égalité entraînerait $\mathcal{M}' \subseteq D$, ce qui contredit le Lem. 8.47, d'où $I \subsetneq I\mathcal{M}'$.
La maximalité de I dans E implique $I\mathcal{M}' \notin E$, donc

$$I\mathcal{M}'(I\mathcal{M}')' = D, \tag{8.14}$$

où $(I\mathcal{M}')'$ est l'idéal fractionnaire associé à l'idéal $I\mathcal{M}'$, par la Rel. (8.10).
Compte tenu de la définition de I', la Rel. (8.14) entraîne

$$\mathcal{M}'(I\mathcal{M}')' \subseteq I',$$

d'où l'on déduit

$$D \subseteq II' \subseteq D \Longrightarrow II' = D,$$

ce qui est contraire à l'hypothèse $II' \neq D$.
On en conclut que $E = \emptyset$, donc tout idéal non nul I de D est inversible dans le monoïde $\mathcal{F}$ et son inverse est l'idéal fractionnaire I'.
Désormais, pour tout idéal I non nul de D, on utilisera la *notation I^{-1} à la place de I'*.
2°) Considérons le cas d'un idéal fractionnaire quelconque, non nul, J de D. Il existe $c \in D^*$ tel que

$$J = c^{-1}I, \quad \text{où} \quad I \text{ est un idéal de } D \text{ ; alors,}$$
$$(c^{-1}I)(cI^{-1}) = II^{-1} = D,$$

entraîne que $J = c^{-1}I$ est inversible dans le monoïde $\mathcal{F}$ et $J^{-1} = cI^{-1}$.
Ainsi, $\mathcal{F}$, muni du produit des idéaux fractionnaires, est un groupe abélien. □

Théorème 8.51. *Soit D un anneau de Dedekind, $\mathcal{F}$ le groupe de ses idéaux fractionnaires et $\mathcal{P}$ l'ensemble de ses idéaux premiers, non nuls ; alors, tout $J \neq (0)$ dans $\mathcal{F}$ s'écrit, de façon unique (à l'ordre près des facteurs)*

$$J = \prod_{P \in \mathcal{P}} P^{n_P(J)}, \tag{8.15}$$

où les $n_P(J)$ sont presque tous nuls dans $\mathbb{Z}$.

Démonstration. 1°) Montrons, que tout idéal non nul de D est un produit d'idéaux premiers de D. Supposons qu'il n'en soit pas ainsi ; alors, l'ensemble, désigné par Σ, des idéaux non nuls de D, qui ne sont pas produit d'idéaux premiers est non vide.
L'anneau de Dedekind D est noethérien (Déf. 8.38), donc Σ contient au moins un *élément maximal*, que nous notons I. La définition de Σ implique que l'idéal non nul I n'est pas premier, donc n'est pas maximal. Par suite, il existe un idéal maximal $\mathcal{M}$ de D, tel que $I \subsetneq \mathcal{M}$.
Moyennant le Lem. 8.47 et la définition de l'inverse d'un idéal non nul (Cf. la preuve du Th. 8.38) on a,

$$D \subsetneq \mathcal{M}^{-1} \subseteq I^{-1} \Longrightarrow I \subsetneq I\mathcal{M}^{-1} \subseteq D.$$

$I\mathcal{M}^{-1}$ est donc un idéal non nul de D contenant strictement I. La maximalité de I dans Σ, implique que $I\mathcal{M}^{-1} \notin \Sigma$; alors $I\mathcal{M}^{-1}$ est un produit d'idéaux premiers non nuls $P_1, \ldots P_r$, et

$$I\mathcal{M}^{-1} = P_1P_2 \ldots P_r \Longrightarrow I = P_1P_2 \ldots P_r\mathcal{M}.$$

L'idéal maximal $\mathcal{M}$ est premier, donc I est un produit d'idéaux premiers, ce qui contredit l'hypothèse, $I \in \Sigma$, d'où nécessairement, $\Sigma = \emptyset$.

On en conclut, qu'un idéal non nul, quelconque, I de D, peut s'écrire

$$I = P_1 P_2 \dots P_n, \tag{8.16}$$

où, pour tout i, $1 \leq i \leq n$, P_i est un idéal premier, non nul de D.
Vérifions *l'unicité* de la relation (8.16), à l'ordre près des facteurs.
Supposons que l'on ait une autre factorisation de I :

$$I = Q_1 Q_2 \dots Q_m,$$

où les Q_j, $1 \leq j \leq m$, sont des idéaux premiers, non nuls et $m \neq n$; par exemple, $m < n$.
On a l'égalité

$$P_1 P_2 \dots P_n = Q_1 Q_2 \dots Q_m.$$

Les propriétés des idéaux premiers ([13], Prop. 2.55), donnent alors

$$\begin{aligned} P_1 P_2 \dots P_n \subseteq P_1 &\Longrightarrow Q_1 Q_2 \dots Q_m \subseteq P_1 \\ &\Longrightarrow \exists j_1, 1 \leq j_1 \leq m, \text{ tel que, } Q_{j_1} \subseteq P_1. \end{aligned}$$

Mais dans l'anneau de Dedekind D, tout idéal premier, non nul, est maximal, par suite, $Q_{j_1} = P_1$; de plus, P_1 est inversible dans $\mathcal{F}$ (Th. 8.50), il en résulte que

$$P_1 P_2 \dots P_n = P_1 \Big(\prod_{1 \leq j \leq m, j \neq j_1} Q_j \Big) \Longrightarrow P_2 \dots P_n = \prod_{1 \leq j \leq m, j \neq j_1} Q_j.$$

En réitérant le raisonnement pour $i = 2, \dots, m$, on peut dire que, pour tout $i (1 \leq i \leq m)$, il existe $j_i \in \{1, 2, \dots, m\}$ tel que $Q_{j_i} = P_i$, d'où l'on déduit que

$$P_{m+1} P_{m+2} \dots P_n = D.$$

Cette égalité implique : $D \subseteq P_i$, $\forall i (m+1 \leq i \leq n)$, ce qui est impossible, puisque les P_i, sont, par définition, des idéaux propres de D. On en conclut que $m = n$.
L'application $i \longmapsto j_i$ définit alors une permutation σ de $\{1, 2, \dots n\}$ telle que, pour tout $i (1 \leq i \leq n), P_i = Q_{\sigma(i)}$.
2°) Soit J un idéal fractionnaire non nul de D ; il existe un idéal non nul I de D et $c \in D^*$ tels que $cJ = I$.
L'idéal cD, engendré par $c \neq 0$, est inversible dans le groupe $\mathcal{F}$ (Th. 8.50), ce qui permet d'écrire

$$J = (cD)^{-1} I.$$

D'après la première partie de la preuve, les idéaux cD et I sont, *de façon unique*, des produits d'idéaux premiers inversibles dans $\mathcal{F}$:

$$(cD = P_1 P_2 \dots P_r,\ I = Q_1 Q_2 \dots Q_s) \Longrightarrow J = P_1^{-1} P_2^{-1} \dots P_r^{-1} Q_1 Q_2 \dots Q_s,$$

d'où l'on déduit l'égalité (8.15) de l'énoncé. □

Proposition 8.52. *Soit I et J deux* idéaux, non nuls, *d'un anneau de Dedekind D, tels que*

$$I = \prod_{P \in \mathcal{P}} P^{n_P(I)}, \quad J = \prod_{P \in \mathcal{P}} P^{n_P(J)},$$

où les $n_P(I)$ et $n_P(J)$ sont presque tous nuls dans $\mathbb{N}$; alors,
1) $n_P(IJ) = n_P(I) + n_P(J)$.
2) $I \subseteq J \iff n_P(I) \geq n_P(J)$, $\forall P \in \mathcal{P}$.
3) $I + J = \prod_{P \in \mathcal{P}} P^{\nu_P}$, $I \cap J = \prod_{P \in \mathcal{P}} P^{\mu_P}$,
où, pour tout $P \in \mathcal{P}$,

$$\nu_P = min(n_P(I), n_P(J)) \quad et \quad \mu_P = max(n_P(I), n_P(J)).$$

Démonstration. 1) Compte tenu de l'unicité de la factorisation d'un idéal de D (Th. 8.51), les hypothèses impliquent immédiatement le résultat énoncé.
2) D'après le Th. 8.51, les idéaux I et J sont inversibles dans $\mathcal{F}$ et

$$\begin{aligned} I \subseteq J &\iff IJ^{-1} \subseteq D \\ &\iff \prod_{P\in\mathcal{P}} P^{n_P(I)-n_P(J)} \subseteq D, \\ &\iff n_P(I) - n_P(J) \geq 0,\ \forall P \in \mathcal{P}. \end{aligned}$$

3) $I+J$ est l'idéal de D engendré par $I \cup J$ ([13], Prop. 2.13.), c'est donc, relativement à l'inclusion, le plus petit idéal de D, contenant I et J, ce qui entraîne, moyennant le résultat 2) précédent,

$$\forall P \in \mathcal{P},\ n_P(I+J) = min(n_P(I), n_P(J)).$$

$I \cap J$ est, relativement à l'inclusion, le plus grand idéal de D contenu dans I et J ; alors, à l'aide du résultat 2), on obtient

$$\forall P \in \mathcal{P},\ n_P(I \cap J) = max(n_P(I), n_P(J)). \qquad \square$$

Les résultats du Th. 8.51 et de la Prop. 8.52 conduisent à définir une notion de *divisibilité* dans l'ensemble des idéaux non nuls de D.

Définition 8.53. Etant donné deux idéaux, non nuls, I et J d'un anneau de Dedekind D, on dira que J **divise** I (noté $J \mid I$), si $I \subseteq J$.
On a alors

$$J \mid I \iff I \subseteq J \iff n_P(I) \geq n_P(J),\ \forall P \in \mathcal{P}. \tag{8.17}$$

Remarque 8.54. Moyennant le Th. 8.51, la Prop. 8.52 et la Déf. 8.53, on peut considérer que deux idéaux non nuls I et J, de D, ont un *p.g.c.d.* et un *p.p.c.m.* En effet, en définissant ces notions, comme elles l'ont été dans un D.I. et en particulier, dans un anneau factoriel ([13], Ch. 5), on vérifie que

$$I \text{ et } J \text{ ont } I+J \text{ pour } p.g.c.d. \text{ et } I \cap J \text{ pour } p.p.c.m.$$

6. Norme d'un idéal d'un anneau d'entiers algébriques

A. Propriétés préliminaires

Rappels relatifs aux les groupes abéliens libres (ou $\mathbb{Z}$-modules libres) de type fini ([12], Ch. 8).
Soit G un groupe abélien libre de type fini, de rang $n \geq 1$. Par définition, une base de G est une base du $\mathbb{Z}$-module libre G.
1) Si b et b' désignent deux bases de G, alors le déterminant de la matrice de passage de b à b' est égal à ± 1.
2) Tout sous-groupe H non nul de G est abélien libre de rang $m \leq n$ et

$$G/H \text{ est fini } \iff m = n.$$

Si $rang(H) = m \leq n = rang(G)$, alors ([12], Th. 8.54), il existe une base $\{u_1, .., u_n\}$ de G et des entiers $h_1, .., h_m$, dans $\mathbb{N}^*$, tels que

$$\{h_1u_1, \ldots, h_mu_m\} \text{ est une base de } H \text{ et } h_i \mid h_{i+1},\ \forall i (1 \leq i \leq m-1).$$

Dans le cas où $m = n$, on a ([12], Th. 8.57),

$$G/H \simeq \prod_{1\leq i\leq n} \mathbb{Z}/h_i\mathbb{Z}, \quad \text{d'où} \quad card\,(G/H) = h_1h_2 \ldots h_n. \tag{8.18}$$

Proposition 8.55. *Soit G un groupe abélien de rang fini et H un sous-groupe de G, tel que $rang(H) = rang(G) = n \geq 1$.*
On suppose que $\{x_1,\ldots,x_n\}$ et $\{y_1,\ldots,y_n\}$ sont, respectivement, des bases de G et de H, telles que

$$\forall i(1 \leq i \leq n),\ y_i = \sum_{1\leq j\leq n} a_{ij}x_j,\ a_{ij} \in \mathbb{Z}, \forall i,j,$$

alors, pour la matrice $A = (a_{ij})_{n\times n} \in M_{n\times n}(\mathbb{Z})$, on a

$$|\det A| = card(G/H). \tag{8.19}$$

Démonstration. Compte tenu des hypothèses et du Rappel 2) ci-dessus, il existe une base $\{u_1,\ldots,u_n\}$ de G et des entiers $h_1,\ldots,h_n$, dans $\mathbb{N}^*$, tels que
$\{h_1u_1,\ldots,h_nu_n\}$ est une base de H et $h_i \mid h_{i+1}$, $\forall i(1 \leq i \leq n-1)$.
Pour tout i, $1 \leq i \leq n$, posons

$$v_i := h_iu_i, \quad u_i = \sum_{1\leq j\leq n} b_{ij}x_j, \quad y_i = \sum_{1\leq j\leq n} c_{ij}v_j,$$

où tous les coefficients b_{ij}, c_{ij} sont dans $\mathbb{Z}$. Soit

$$B := (b_{ij})_{n\times n}, \quad C := (c_{ij})_{n\times n}, \quad M := \begin{pmatrix} h_1 & 0 & 0 & \ldots & 0 \\ 0 & h_2 & 0 & \ldots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & 0 & h_n \end{pmatrix}.$$

Par hypothèse $A = (a_{ij})_{n\times n}$ est la matrice de passage de la base $\{x_1,\ldots,x_n\}$ de G, à la base $\{y_1,\ldots,y_n\}$ de H.
D'autre part, B est la matrice de passage de la base $\{x_1,\ldots,x_n\}$ à la base $\{u_1,\ldots,u_n\}$ de G et C est la matrice de passage de la base $\{v_1,\ldots,v_n\}$ à la base $\{y_1,\ldots,y_n\}$ de H, on en déduit que

$$A = CMB, \quad \text{d'où} \quad \det A = \det C \det M \det B.$$

Or, on a (Cf. Rappel 1), ci-dessus),

$$\det B = \pm 1 \quad \text{et} \quad \det C = \pm 1.$$

On en conclut (Rel. (8.18)) que

$$|\det A| = |\det M| = h_1h_2\ldots h_n = card(G/H).$$

□

Exemple 8.56. Soit G un groupe abélien libre de rang 3 ; $\{x,y,z\}$ étant une base de G, soit H le sous-groupe de G engendré par $\{u,v,w\}$, où

$$\left.\begin{array}{l} u = 2x+y-z \\ v = 3x-y+5z \\ w = x+4y \end{array}\right| \Longrightarrow \left|\begin{array}{ccc} 2 & 1 & -1 \\ 3 & -1 & 5 \\ 1 & 4 & 0 \end{array}\right| = 48.$$

On a $48 \neq \pm 1$, donc $\{u,v,w\}$ est une base de H, qui est un sous-groupe *propre* de G (voir Rappel 1) et Prop. 8.55) et

$$rang(H) = rang(G) \Longrightarrow G/H \text{ fini et } card\, G/H = 48.$$

B. Norme d'un idéal, non nul, d'un anneau $\mathcal{D}$

Dans tout ce paragraphe, $\mathcal{D}$ désigne *l'anneau des entiers algébriques d'un corps de nombres* K (Déf. 8.4). On suppose $[K:\mathbb{Q}] = n \geq 1$; alors $\mathcal{D}$ est un groupe (additif) abélien libre de rang fini, égal à n (Th. 8.25).

Proposition 8.57. *Dans l'anneau $\mathcal{D}$ des entiers d'un corps de nombres, pour tout idéal* non nul, I, $\mathcal{D}/I$ *est fini ; par suite $(I,+)$ est un sous-groupe abélien libre de $(\mathcal{D},+)$ tel que* $rang(I) = rang(\mathcal{D})$.

Démonstration. Par hypothèse $(I,+)$ est un sous-groupe du groupe abélien libre de rang fini $(\mathcal{D},+)$; on suppose $rang\,(\mathcal{D}) = n \geq 1$.
Considérons le cas où I est un idéal principal de $\mathcal{D}$, donc $I = \alpha\mathcal{D}$, $\alpha \neq 0$.
L'application $m_\alpha : \mathcal{D} \longrightarrow \alpha\mathcal{D}$ telle que, quel que soit $x \in \mathcal{D}$, $m_\alpha(x) = \alpha x$, est un $\mathbb{Z}$-isomorphisme, par suite, $\alpha\mathcal{D}$ est un sous-groupe abélien libre de $\mathcal{D}$, de rang n. On en déduit que $\mathcal{D}/\alpha\mathcal{D}$ est fini (Rappel 2), ci-dessus).
Dans le cas où I est un idéal, non nul, quelconque de $\mathcal{D}$, considérons un élément $\alpha \neq 0$ dans I. On a $\alpha\mathcal{D} \subseteq I \subseteq \mathcal{D}$, d'où ([13], Th. 2.41)

$$\mathcal{D}/I \simeq (\mathcal{D}/\alpha\mathcal{D})/(I/\alpha\mathcal{D})$$
$$\text{et} \qquad (\mathcal{D}/\alpha\mathcal{D} \text{ fini}) \Longrightarrow (I/\alpha\mathcal{D}) \text{ fini}) \Longrightarrow \mathcal{D}/I \text{ fini}.$$

$(I,+)$ est alors un sous-groupe abélien libre de $(\mathcal{D},+)$, de rang n. □

Corollaire 8.58. *Les hypothèses sont celles de la* Prop. 8.57.
a) Pour tout idéal premier, *non nul, P de $\mathcal{D}$, $\mathcal{D}/P$ est un corps fini.*
b) Si $K = \mathbb{Q}(\alpha)$, où $\alpha \in \mathcal{D}$ (Th. 8.20), *alors*

$$card\,(\mathcal{D}/\alpha\mathcal{D}) = \mid N_{K:\mathbb{Q}}(\alpha) \mid .$$

Démonstration. a) $\mathcal{D}$ est un anneau de Dedekind (Exem. 8.39.), alors tout idéal premier, non nul, P de $\mathcal{D}$ est maximal (Déf. 8.38), donc $\mathcal{D}/P$ est un corps fini (Prop. 8.57.).
b) $\alpha \in \mathcal{D} = \mathcal{A} \cap \mathbb{Q}$, donc $p_\alpha(X) := Irr_K(\alpha, X)$ appartient à $\mathbb{Z}[X]$ (Th. 8.13.).
Si $[K:\mathbb{Q}] = n$ et

$$p_\alpha(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0,$$

alors, $N_{K:\mathbb{Q}}(\alpha)$ étant le produit des conjugués de α, donc des racines de $p_\alpha(X)$,

$$N_{K:\mathbb{Q}}(\alpha) = (-1)^n a_0 \in \mathbb{Z}.$$

D'autre part, les hypothèses entraînent que $b := \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ est une base de K sur $\mathbb{Q}$, mais le polynôme $p_\alpha(X)$ étant de degré n dans $\mathbb{Z}[X]$, on en déduit que b est une *base entière* (Déf. 8.26.) de K, c'est-à-dire une base du groupe libre $(\mathcal{D},+)$ et $b' := \{\alpha, \alpha^2, \ldots, \alpha^n\}$ est alors une base du sous-groupe $\alpha\mathcal{D}$ de $(\mathcal{D},+)$.
Soit $M_{bb'}$ la matrice de passage de la base b de $\mathcal{D}$ à la base b' de $\alpha\mathcal{D}$; d'après la Prop. 8.55, on a

$$card\,(\mathcal{D}/\alpha\mathcal{D}) = \mid det\,(M_{bb'}) \mid .$$

$$det\,M_{bb'} = \begin{vmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & -a_{n-1} \end{vmatrix} = (-1)^n a_0,$$

d'où $card\,(\mathcal{D}/\alpha\mathcal{D}) = \mid N_{K:\mathbb{Q}}(\alpha) \mid$. □

Définition 8.59. Soit $\mathcal{D}$ l'anneau des entiers d'un corps de nombres et I un idéal, non nul, de $\mathcal{D}$; on appelle **norme** de I, l'entier positif, noté $N(I)$, défini par

$$N(I) := card\,(\mathcal{D}/I).$$

Remarque 8.60. L'appellation « norme d'un idéal », utilisée dans la Déf. 8.59, se justifie par le résultat b) du Cor. 8.58., qui correspond au cas où l'idéal I est principal.

Théorème 8.61. *Soit $\mathcal{D}$ l'anneau des entiers algébriques d'un corps de nombres ; si I et J sont deux idéaux non nuls de $\mathcal{D}$, alors*

$$N(IJ) = N(I)N(J). \tag{8.20}$$

Démonstration. Compte tenu de la factorisation unique d'un idéal non nul de $\mathcal{D}$, en un produit d'idéaux premiers non nuls (Th. 8.51), il suffit de prouver la relation

$$N(IP) = N(I)N(P), \tag{8.21}$$

où P est un idéal premier non nul de $\mathcal{D}$.
Le $3^{ème}$ thèorème d'isomorphisme ([13], Th. 2.41) implique

$$\mathcal{D}/I \simeq (\mathcal{D}/IP)/(I/IP).$$

On en déduit que

$$card\,(\mathcal{D}/I) = card\,(\mathcal{D}/IP)\,card\,(I/IP). \tag{8.22}$$

Démontrons que $card\,(I/IP) = card\,(\mathcal{D}/P)$.
La factorisation unique (Th. 8.51) implique $I \neq IP$, donc $IP \subsetneq I$.
Vérifions qu'il n'existe aucun idéal J de $\mathcal{D}$, strictement compris entre IP et I. En effet, supposons

$$IP \subseteq J \subseteq I.$$

L'idéal non nul I étant inversible (Th. 8.50), on a

$$I^{-1}IP \subseteq I^{-1}J \subseteq I^{-1}I, \text{ donc } P \subseteq I^{-1}J \subseteq \mathcal{D}.$$

Or, dans ($\mathcal{D}$,P est un idéal maximal (Th. 8.30), d'où,

$$I^{-1}J = P \text{ ou } I^{-1}J = \mathcal{D} \text{ et par suite, } J = I \text{ ou } J = IP.$$

Il en résulte que, pour tout $a \in I \setminus IP$, on a

$$IP + < a >= I,$$

$< a >$ désignant l'idéal de $\mathcal{D}$ engendré par a.
Soit $\theta : \mathcal{D} \longrightarrow I/IP$ tel que $\theta(x) = \overline{xa} := IP + xa, \forall x \in \mathcal{D}$.
θ est un morphisme de $\mathcal{D}$-modules, qui est surjectif, puisque $I = IP + < a >$. On vérifie que $Ker\,\theta = P$, par suite,

$$\mathcal{D}/P \simeq I/IP.$$

La relation (8.22) implique alors

$$N(IP) = N(I)N(P),$$

entraînant la relation (8.20). □

Nous terminerons ce chapitre par un exemple de factorisation d'un idéal, dans un anneau d'entiers algébriques (Cf. Th. 8.51).

Exemple 8.62. Soit $\mathcal{D}$ l'anneau des entiers algébriques de $\mathbb{Q}(\sqrt{-17})$; on vérifie que (voir Ex. **2.**, Ch.8)

$$\mathcal{D} = \mathbb{Z}[\sqrt{-17}] = \{a+b\sqrt{-17}\,;\, a,b \text{ dans } \mathbb{Z}\}.$$

Soit $< 18 >$ l'idéal de l'anneau $\mathcal{D}$, engengré par 18.
On remarque que, dans $\mathcal{D}$, on a

$$18 = 2.3.3 = (1+\sqrt{-17})(1-\sqrt{-17}).$$

Soit $P_1 :=< 2, 1+\sqrt{-17} >$ l'idéal de $\mathcal{D}$ engendré par 2 et $1+\sqrt{-17}$;

$$1-\sqrt{-17} = 2-1+\sqrt{-17} \Longrightarrow (1-\sqrt{-17}) \in P_1,$$
$$\text{alors,} \quad 18 = (1+\sqrt{-17})(1-\sqrt{-17}) \Longrightarrow 18 \in P_1^2\,;$$
$$\text{d'où,} \quad < 18 > \subseteq P_1^2 \iff P_1^2 \mid < 18 > \text{ (Déf 8.53).}$$

Démontrons que P_1 est un idéal *premier* de $\mathcal{D}$, donc *maximal*, car $\mathcal{D}$ est un anneau de Dedekind (Exemple 8.3).
Un élément $x \in P_1$ s'écrit,

$$x = 2(a+b\sqrt{-17}) + (1+\sqrt{-17})(c+d\sqrt{-17}),$$

où, a,b,c,d sont dans $\mathbb{Z}$; d'où

$$x = (2a+c-17d) + (2b+c+d)\sqrt{-17}.$$

En posant $r := 2a+c-17d$ et $s := 2b+c+d$, on a

$$r-s = 2(a-b-9d) \in 2\mathbb{Z}.$$

On en déduit (à vérifier par le lecteur) que, pour r et s dans $\mathbb{Z}$,

$$x = r+s\sqrt{-17} \in P_1 \iff r-s \in 2\mathbb{Z}.$$

On en déduit que $P_1 \neq \mathcal{D}$ et pour prouver que P_1 est un idéal maximal, montrons que le quotient $\mathcal{D}/P_1$ est un corps ([13], Th. 2.62). Considérons le diagramme :

$$\begin{array}{ccc} \mathcal{D} & \xrightarrow{\quad f_1 \quad} & \mathbb{Z} \\ \Big\downarrow{\scriptstyle \pi_1} & & \Big\downarrow{\scriptstyle \sigma_1} \\ \mathcal{D}/P_1 & \overset{\exists!\overline{f_1}}{\dashrightarrow} & \mathbb{Z}/2\mathbb{Z} \end{array}$$

où, π_1 et σ_1 sont les morphismes canoniques et quel que soit $r+s\sqrt{-17}$ dans $\mathcal{D}$, $f_1(r+s\sqrt{-17}) = r-s$. On a

$$Ker(\sigma_1 \circ f_1) = P_1 \text{ et } \sigma_1 \circ f_1 \text{ surjectif,}$$

ce qui entraine l'existence de l'unique isomorphisme $\overline{f_1}$ ([13], Lem. 2.37) tel que

$$\overline{f_1} \circ \pi_1 = \sigma_1 \circ f_1.$$

Ainsi $\mathcal{D}/P_1$ est un corps isomorphe $\mathbb{Z}/2\mathbb{Z}$, d'où P_1 idéal maximal, donc premier dans $\mathcal{D}$.
On considère de même les idéaux

$$P_2 :=< 3, 1+\sqrt{-17} > \quad \text{et} \quad P_3 =< 3, 1-\sqrt{-17} >.$$

On a $18 \in P_2^2$ et $18 \in P_3^2$, d'où

$$< 18 > \subseteq P_i^2 \iff P_i^2 \mid < 18 >,\ i = 2,3.$$

Comme dans le cas de l'idéal P_1, on vérifiera que, pour $x = r+s\sqrt{-17}$ dans $\mathcal{D}$, on a

$$x \in P_2 \iff r-s \in 3\mathbb{Z} \quad \text{et} \quad x \in P_3 \iff r+s \in 3\mathbb{Z}.$$

Pour $i = 2,3$, on définit alors, les applications $f_i : \mathcal{D} \longrightarrow \mathbb{Z}$ telles que,

$$f_2(r+s\sqrt{-17}) = r-s \quad \text{et} \quad f_3(r+s\sqrt{-17}) = r+s.$$

Les diagrammes semblables à celui utilisé pour P_1, conduisent à l'exitence d'isomorphismes $\overline{f_i}$ de $\mathcal{D}/P_i$ sur le corps $\mathbb{Z}/3\mathbb{Z}$; par suite, P_2 et P_3 sont des idéaux maximaux, donc premiers dans $\mathcal{D}$.
Les résultats précédents entrainent que $P_1^2P_2^2P_3^2 \mid < 18 >$.
Si l'on suppose $< 18 > \neq P_1^2P_2^2P_3^2$, alors il existe un idéal non nul I de $\mathcal{D}$ tel que

$$< 18 >= P_1^2 P_2^2 P_3^2 I.$$

Calculons la norme des idéaux constituant chacun des deux membres de l'égalité précédente. On doit avoir (Th. 8.61)

$$N(< 18 >) = N(P_1^2)N(P_2^2)N(P_3^2)N(I).$$

Pour $x = a + b\sqrt{-17}$ dans $\mathcal{D}$, on a

$$x \in < 18 > \iff (a,b) \in 18\mathbb{Z} \times 18\mathbb{Z},$$

d'où

$$N(< 18 >) = card\,(\mathcal{D}/ < 18 >) = 18^2.$$

D'autre part,

$$\mathcal{D}/P_1 \simeq \mathbb{Z}/2\mathbb{Z} \Longrightarrow N(P_1) = 2,$$

$$\text{et pour} \quad i = 2,3, \quad \mathcal{D}/P_i \simeq \mathbb{Z}/3\mathbb{Z} \Longrightarrow N(P_i) = 3.$$

Il en résulte que

$$N(P_1^2)N(P_2^2)N(P_3^2) = 2^2 3^2 3^2 = 18^2.$$

Par suite, $N(I) = 1$ implique $I = \mathcal{D}$, d'où la conclusion :

$$< 18 >= P_1^2 P_2^2 P_3^2.$$

7. Exercices

1. On considère le corps quadratique $\mathbb{Q}(i)$, où $i^2 = -1$ dans $\mathbb{C}$.

1°) Vérifier que tout $\alpha \in \mathbb{Q}(i)$ s'écrit, de façon unique,

$$\alpha = a + bi; \quad a,b \text{ dans } \mathbb{Q}.$$

Pour $\alpha = a + bi$ dans $\mathbb{Q}(i)$, déterminer $p_\alpha(X) := Irr_{\mathbb{Q}}(\alpha, X)$.

2°) Soit $\mathcal{D}$ l'anneau des entiers algébriques de $\mathbb{Q}(i)$.

A tout $\alpha = a + bi$ dans $\mathbb{Q}(i)$, on associe $\overline{\alpha} := a - bi$. Justifier l'implication :

$$\alpha \in \mathcal{D} \Longrightarrow \overline{\alpha},\ \alpha + \overline{\alpha},\ \alpha - \overline{\alpha} \text{ et } \alpha\overline{\alpha} \text{ dans } \mathcal{D}.$$

Etant donné $\alpha = a + bi$ dans $\mathbb{Q}(i)$, on pose $u := 2a$, $v := 2b$; montrer que $\alpha \in \mathcal{D}$ si et seulement si

$$u \in \mathbb{Z},\ v \in \mathbb{Z} \text{ et } u^2 + v^2 \equiv 0 \pmod 4.$$

En déduire que

$$\mathcal{D} = \{a + bi\,;\ a,b, \text{ dans } \mathbb{Z}\} = \mathbb{Z}[i].$$

2. Soit $K := \mathbb{Q}(\sqrt{d})$ une extension quadratique de $\mathbb{Q}$; on suppose $d \leq -1$ ou $d > 1$ dans $\mathbb{Z}$ et d non divisible par un carré.

Selon la convention habituelle,

si $d > 0$, $\sqrt{d}$ désigne la racine carrée réelle positive de d ;

si $d < 0$, $\sqrt{d} = i\sqrt{-d}$, où $i^2 = -1$ dans $\mathbb{C}$.

1°) Vérifier que tout $\alpha \in K$, s'écrit de façon unique,

$$\alpha = a + b\sqrt{d};\ a,b \text{ dans } \mathbb{Q}.$$

2°) Etant donné $\alpha = a + b\sqrt{d}$ dans K, on pose $\alpha' := a - b\sqrt{d}$ et $N(\alpha) := N_{K:\mathbb{Q}}(\alpha)$.

On note $\mathcal{D}$ l'anneau des entiers algébriques de K.

a) Vérifier que $\alpha \in \mathcal{D}$ implique

$$\alpha',\ \alpha + \alpha',\ \alpha - \alpha' \text{ dans } \mathcal{D} \text{ et } N(\alpha) \text{ dans } \mathbb{Z}.$$

b) Pour $\alpha = a + b\sqrt{d}$ dans K, on pose $u := 2a$, $v := 2b$.

Démontrer que $\alpha \in \mathcal{D}$ si et seulement si

$$u \in \mathbb{Z},\ v \in \mathbb{Z} \text{ et } u^2 - dv^2 \equiv 0 \pmod 4.$$

3°) Vérifier que les hypothèses impliquent $d \not\equiv 0 \pmod 4$ et prouver que

$$d \not\equiv 1 \pmod 4 \Longrightarrow \mathcal{D} = \mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d}\,;\, a, b \text{ dans } \mathbb{Z}\}.$$
$$d \equiv 1 \pmod 4 \Longrightarrow \mathcal{D} = \{\frac{u}{2} + \frac{v}{2}\sqrt{d}\,;\, u, v \text{ de même parité dans } \mathbb{Z}\}.$$

(Indication : Pour $d \equiv 2$, ou 3, ou 1, modulo 4, considérer $u^2 - dv^2$ dans les quatre cas suivants : u et v pairs ; u pair, v impair ; u impair, v pair ; u et v impairs.)

3. Soit K un corps de nombres et $\mathcal{D}$ l'anneau des entiers algébriques de K. On note $U_{\mathcal{D}}$ le groupe des unités de l'anneau $\mathcal{D}$ ([13], prop. 1.9.). Pour tout $\alpha \in K$, on pose $N(\alpha) := N_{K:\mathbb{Q}}(\alpha)$.

1°) Pour $\alpha \in \mathcal{D}$, prouver que

$$\alpha \in U_{\mathcal{D}} \iff N(\alpha) = \pm 1.$$

En déduire que, pour α et β dans $\mathcal{D}$,

$$\alpha \sim \beta \Longrightarrow N(\alpha) = \pm N(\beta).$$

[$\alpha \sim \beta$ signifie : α *associé* à β ([13], Déf. 5.11.)]

2°) On suppose $K = \mathbb{Q}(\sqrt{d})$, $d \leq -1$, dans $\mathbb{Z}$ et d non divisible par un carré.

Les résultats de l'Ex. **2.** précédent sont supposés connus.

a) Prouver que

$d = -1 \Longrightarrow U_{\mathcal{D}} = \{\pm 1, \pm i\}$, où $i^2 = -1$ dans $\mathbb{C}$;

$d = -2 \Longrightarrow U_{\mathcal{D}} = \{\pm 1\}$;

$d = -3 \Longrightarrow U_{\mathcal{D}} = \{\pm 1, \pm j, \pm j^2\}$, où j et j^2 sont les racines cubiques non réelles de l'unité, dans $\mathbb{C}$;

$d < -3 \Longrightarrow U_{\mathcal{D}} = \{\pm 1\}$.

b) Démontrer que, pour $\alpha \in \mathcal{D}$,

$$N(\alpha) \text{ premier dans } \mathbb{Z} \Longrightarrow \alpha \text{ irréductible dans } \mathcal{D}.$$

3°) Dans le cas où $K = \mathbb{Q}(\sqrt{-7})$, vérifier que $\dfrac{1+\sqrt{-7}}{2}$ et $\dfrac{1-\sqrt{-7}}{2}$ sont des éléménts irréductibles de l'anneau $\mathcal{D}$.

En déduire que 2 n'est pas irréductible dans $\mathcal{D}$.

4. Soit $K = \mathbb{Q}(\sqrt{d})$ une extension quadratique de $\mathbb{Q}$, où l'on suppose $d \leq -1$ dans $\mathbb{Z}$, et d non divisible par un carré.

Les résultats de l'Ex. **2.** précédent sont supposés connus.

On note $\mathcal{D}$ l'anneau des entiers algébriques de K et $U_{\mathcal{D}}$ le groupe des unités de $\mathcal{D}$.

1°) Pour tout $\alpha \in K$, on pose $N(\alpha) := N_{K:\mathbb{Q}}(\alpha)$.

Vérifier que $\alpha \in \mathcal{D}^* := \mathcal{D} \setminus \{0\} \Longrightarrow N(\alpha) \in \mathbb{N}^*$.

2°) On suppose $d \in \{-1, -2, -3, -7, -11\}$ et soit

$$N : \mathcal{D} \longrightarrow \mathbb{N}$$
$$\alpha \longmapsto N(\alpha).$$

a) Montrer que $\alpha \mid \beta$ dans $\mathcal{D}^* \Longrightarrow N(\alpha) \leq N(\beta)$ dans $\mathbb{N}^*$.

b) Soit $\alpha = a + b\sqrt{d}$ et $\beta = r + s\sqrt{d}$ dans $\mathcal{D}^*$.

Démontrer qu'il existe γ et ρ dans $\mathcal{D}$ tels que

$$\alpha = \beta\gamma + \rho, \text{ avec } \rho = 0 \text{ ou } N(\rho) < N(\beta) \text{ dans } \mathbb{N}^*.$$

En déduire que, quelque soit $d \in \{-1, -2, -3, -7, -11\}$, l'anneau $\mathcal{D}$ est euclidien.

(Indications : utiliser la même méthode que celle qui a permis de montrer que l'anneau de Gauss est euclidien ([13], Exemple 5.75), en distinguant les cas où $d \not\equiv 1 \mod 4$ et $d \equiv 1 \mod 4$).

Remarque : on a $-5 \not\equiv 1 \mod 4$, donc l'anneau des entiers algébriques de $\mathbb{Q}(\sqrt{-5})$ est $\mathbb{Z}[\sqrt{-5}]$, qui est un D.I. non factoriel ([13], p.145), donc non euclidien.

3°) Le but de cette question est de prouver que pour $d < -11$, l'anneau $\mathcal{D}$ n'est pas euclidien.

En vue d'un raisonnement par l'absurde, on suppose que pour $d < -11$, l'anneau $\mathcal{D}$ est euclidien relativement à un stathme $\delta : \mathcal{D}^* \longrightarrow \mathbb{N}$.

On note $\mathcal{U}_{\mathcal{D}}$ le groupe des unités de $\mathcal{D}$.

Soit $\alpha \in \mathcal{D}^*$ tel que $\alpha \notin \mathcal{U}_{\mathcal{D}}$ et $\delta(\alpha)$ *minimal* dans $\mathbb{N}$.

a) Etant donné $\beta \in \mathcal{D}^*$, par hypothèse, il existe γ et ρ dans $\mathcal{D}$ tels que

$$\beta = \alpha\gamma + \rho, \quad \text{avec } \rho = 0 \text{ ou } \delta(\rho) < \delta(\alpha).$$

Montrer que la minimalité de $\delta(\alpha)$ implique

$$\rho = 0 \quad \text{ou} \quad \rho = \pm 1.$$

En déduire que $card(\mathcal{D}/\alpha\mathcal{D}) \leq 3$ et que par suite, $N(\alpha) \leq 3$.

b) Démontrer que les conditions $N(\alpha) \leq 3$ et $d < -11$ entraînent une contradiction avec l'hypothèse $\alpha \notin \mathcal{U}_{\mathcal{D}}$ et conclure.

(Distinguer les cas où $d \not\equiv 1 \pmod 4$ et $d \equiv 1 \pmod 4$).

5. Soit B un domaine d'intégrité (D.I.) et A un sous-anneau de B tel que B soit *entier* sur A (Déf. 8.31).

Le but de l'exercice est de prouver que B est un corps si et seulement si A est un corps.

1°) On suppose que A est un corps. Soit $b \in B \setminus \{0\}$.

a) Vérifier que $A[b] := \{f(b)\,;\, f(X) \in A[X]\}$ est A-espace vectoriel de dimension finie.

b) Prouver que l'application

$$\begin{aligned} A[X] &\longrightarrow A[b] \\ \alpha &\longmapsto b\alpha \end{aligned}$$

est A-linéaire et bijective. En déduire que B est un corps.

2°) Réciproquement, on suppose que B est un corps.

Soit $a \in A \setminus \{0\}$ et a^{-1} l'inverse de a dans B. Prouver que $a^{-1} \in A$ et conclure.

6. Soit p un nombre premier et $\omega \in \overline{\mathbb{Q}}$, une racine $p^{ème}$ *primitive* de l'unité. Pour tout $\alpha \in \mathbb{Q}(\omega)$, on pose

$$T(\alpha) = T_{\mathbb{Q}(\omega):\mathbb{Q}}(\alpha) \quad \text{et} \quad N(\alpha) = N_{\mathbb{Q}(\omega):\mathbb{Q}}(\alpha).$$

1°) a) Rappeler quel est le polynôme $Irr_{\mathbb{Q}}(\omega, X)$ et préciser sa factorisation dans $\overline{\mathbb{Q}}[X]$.

b) Montrer que $T(\omega) = -1$, $T(1) = p - 1$, et $T(\omega^j) = -1$, quel que soit $j (1 \leq j \leq p-1)$.

En déduire que

$$T(1-\omega) = p = T(1-\omega^j),\ \forall j (1 \leq j \leq p-1).$$

c) Montrer que $N(\omega) = (-1)^{p-1}$ et $N(\omega - 1) = (-1)^{p-1} p$.

En déduire que $(1-\omega)(1-\omega^2)\ldots(1-\omega^{p-1}) = p$.

2°) Soit $\mathcal{D}$ l'anneau des entiers algébriques de $\mathbb{Q}(\omega)$.

a) Vérifier que $\omega \in \mathcal{D}$; en déduire que $p \in (1-\omega)\mathcal{D}$.

b) Prouver que $(1-\omega)\mathcal{D} \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ et que

$$(1-\omega)\mathcal{D} \cap \mathbb{Z} = p\mathbb{Z}.$$

(Indication : montrer que $(1-\omega)\mathcal{D} \cap \mathbb{Z} \neq p\mathbb{Z}$ conduit à une contradiction.)

3°) Démontrer que pour tout $\alpha \in \mathcal{D}$, on a

$$T(\alpha(1-\omega)) \in p\mathbb{Z}.$$

4°) Soit $\alpha \in \mathcal{D}$.

a) Vérifier que α s'écrit de façon unique

$$\alpha = \sum_{0 \le j \le p-1} a_j \omega^j,$$

où $a_j \in \mathbb{Q}, \forall j (0 \le j \le p-1)$.

Démontrer que $T(\alpha(1-\omega)) = a_0 p$; en déduire que $a_0 \in \mathbb{Z}$.

b) Vérifier que $\omega^{-1} \in \mathcal{D}$; en déduire que $(\alpha - a_0)\omega^{-1} \in \mathcal{D}$.

On pose $\alpha_1 := (\alpha - a_0)\omega^{-1}$; démontrer que $a_1 \in \mathbb{Z}$, en utilisant la méthode qui a permis de prouver que $a_0 \in \mathbb{Z}$.

c) Montrer que pour tout $j (0 \le j \le p-1)$, on a $a_j \in \mathbb{Z}$; en déduire que

$$\mathcal{D} = \mathbb{Z}[\omega] := \{ \sum_{0 \le j \le p-1} a_j \omega^j \, ; \, a_j \in \mathbb{Z}, \forall j (0 \le j \le p-1) \}.$$

En conclure que $\{1, \omega, \ldots, \omega^{p-1}\}$ est une base entière de $\mathbb{Q}(\omega)$ et que, quel que soit le nombre premier p, $\mathbb{Z}[\omega]$ est un anneau de Dedekind.

7. Soit R un domaine d'intégrité (D.I.), A un sous-anneau de R et S une partie multiplicative de A ([13], Déf. 6.1.).On note B la fermeture intégrale de A dans R.

1°) Démontrer que la fermeture intégrale de $S^{-1}A$ dans $S^{-1}R$ est $S^{-1}B$ ([13], Ch. 6).

2°) Montrer que si A est un anneau intégralement clos (Déf. 8.33) alors, pour toute partie multiplicative S de A, l'anneau localisé $S^{-1}A$ est intégralement clos.

3°) Démontrer que tout localisé $S^{-1}A$ d'un anneau de Dedekind A est un anneau de Dedekind (voir [13], Prop. 6.16, 6.19 et Th. 6.21).

8. Le but est de prouver (Th. de Ramanujan-Nagell) que les seuls couples $(x,n) \in \mathbb{Z} \times \mathbb{N}$ satisfaisant à l'équation

$$x^2 + 7 = 2^n \tag{8.23}$$

sont $(\pm 1, 3), (\pm 3, 4), (\pm 5, 5), (\pm 11, 7), (\pm 181, 15)$.

On considère le corps quadratique $K = \mathbb{Q}(\sqrt{-7})$; $\mathcal{D}$ étant l'anneau des entiers algébriques de K, les résultats (supposés connus) des Ex. **2.**, **3.**, **4.**, ci-dessus, impliquent

$$\mathcal{D} = \{ \frac{u + v\sqrt{-7}}{2} \, ; \, u, v \text{ de même parité dans } \mathbb{Z} \}$$

et $\mathcal{D}$ euclidien.

1°) Montrer que les seules solutions de l'équation (8.23) pour lesquelles n est *pair* sont $(\pm 3, 4)$.

2°) On recherche désormais les solutions de (8.23), pour lesquelles n est *impair*.

a) On remarque que l'équation (8.23) n'a pas de solution pour $n = 1$ et que, pour $n = 3$, on obtient $x = \pm 1$.

On considère dans la suite, $n > 3$ et *impair* ; on pose alors

$$m := n - 2 > 1.$$

On écrit l'équation (8.23) sous la forme

$$\frac{x^2 + 7}{4} = 2^m. \tag{8.24}$$

On note que dans toute solution de l'équation (8.24), x est nécessairement *impair*.

Montrer que (8.24) peut s'écrire

$$\left(\frac{x + \sqrt{-7}}{2}\right)\left(\frac{x - \sqrt{-7}}{2}\right) = \left(\frac{1 + \sqrt{-7}}{2}\right)^m \left(\frac{1 - \sqrt{-7}}{2}\right)^m. \tag{8.25}$$

Prouver que

$$(8.25) \Longrightarrow \frac{x \pm \sqrt{-7}}{2} = \pm\left(\frac{1 \pm \sqrt{-7}}{2}\right)^m ; \tag{8.26}$$

$$(8.26) \Longrightarrow \pm\sqrt{-7} = \left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m . \tag{8.27}$$

b) On pose $a := \dfrac{1+\sqrt{-7}}{2}$ et $b := \dfrac{1-\sqrt{-7}}{2}$.

On considère le cas où le signe du premier membre de l'équation (8.27) est + ; on a donc

$$\sqrt{-7} = a^m - b^m . \tag{8.28}$$

En utilisant les relations $a+b=1$, $a-b=\sqrt{-7}$, $ab=2$, démontrer que, dans l'anneau euclidien $\mathcal{D}$,

$$(8.28) \Longrightarrow a \equiv a-b \pmod{b^2}.$$

En conclure que, dans le premier membre de l'équation (8.27), le signe + est impossible.

3°) Pour $m > 1$, dans $\mathbb{N}$, on considère l'équation

$$-\sqrt{-7} = \left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m . \tag{8.29}$$

a) En utilisant la formule du binôme, prouver que

$$(8.29) \Longrightarrow -2^{m-1} \equiv m \pmod 7. \tag{8.30}$$

b) Etant donné que $2^3 \equiv 1 \pmod 7$, montrer que si m vérifie (8.30), alors, pour $m' > 1$ dans $\mathbb{N}$,

$$m' \equiv m \pmod{21} \Longrightarrow -2^{m'-1} \equiv m' \pmod 7.$$

c) Prouver que les seuls entiers impairs m, vérifiant (8.30) et pour lesquels $1 < m \leq 21$, sont 3, 5 et 13.

4°) a) Montrer que, pour $m \in \{3,5,13\}$, l'équation (8.24) a des solutions, que l'on déterminera.

En déduire les solutions correspondantes de l'équation (8.23).

b) Vérifier que pour $m \in \{3,5,13\}$ et $m' \in \mathbb{N}$,

$$(m' \equiv m \pmod{21} \text{ et } m' \text{ impair}) \Longrightarrow m' \equiv m \pmod{42}.$$

c) On suppose $m \in \{3,5,13\}$, $m' \neq m$, dans $\mathbb{N}$ et $m' \equiv m \pmod{42}$; le but de ce qui suit est de prouver que l'équation

$$\frac{x^2+7}{4} = 2^{m'} \tag{8.31}$$

n'a aucune solution.

On suppose que $7^k, k \in \mathbb{N}^*$, est la *plus grande puissance* de 7 divisant $m'-m$.

Les notations étant celles de la question 2°, b), vérifier les relations suivantes, dans l'anneau euclidien $\mathcal{D}$.

$$a^{m'} = a^m \left(\frac{1}{2}\right)^{m'-m} (1+\sqrt{-7})^{m'-m} ; \tag{8.32}$$

$$\left(\frac{1}{2}\right)^{m'-m} - 1 \equiv 0 \pmod{7^{k+1}} ; \tag{8.33}$$

$$(1+\sqrt{-7})^{m'-m} - 1 \equiv (m'-m)\sqrt{-7} \pmod{7^{k+1}} ; \tag{8.34}$$

$$a^m \equiv \frac{1+m\sqrt{-7}}{2} \pmod 7. \tag{8.35}$$

En déduire, en utilisant la relation (8.32), que

$$a^{m'} \equiv a^m + \frac{m'-m}{2^m}\sqrt{-7} \pmod{7^{k+1}}, \tag{8.36}$$

$$b^{m'} \equiv b^m - \frac{m'-m}{2^m}\sqrt{-7} \pmod{7^{k+1}}. \tag{8.37}$$

Démontrer qu'on a alors, $m' \equiv m \pmod{7^{k+1}}$; en déduire une contradiction avec l'hypothèse consernant 7^k et conclure.

Chapitre 9
Résolution des équations par radicaux

Historique du problème ([10], [45])

Les équations polynômiales ont une longue histoire.
Des tables babyloniennes, datant de 1600 av. J.C., posent déjà des problèmes amenant à la résolution d'équations du second degré ; il est clair, d'après les tablettes, que les Babyloniens avaient des méthodes pour les résoudre, bien qu'ils n'aient pas de notations algébriques pour exprimer leurs solutions.
Les Grecs de l'antiquité résolvaient les équations du second degré par des constructions géométriques, mais il n'y a aucun signe de formulation algébrique, avant 100 ap. J.C.
Toujours grâce à la géométrie, les Grecs avaient aussi des méthodes de résolution des équations polynômiales du $3^{ème}$ degré ; mais la résolution algébrique de celles-ci restent longtemps inconnue, puisqu' en 1494, Pacioli publie un traité arithmétique, dans lequel il écrit que la résolution des équations

$$x^3+mx=n\,;\ x^3+n=mx \quad (m \text{ et } n \text{ entiers positifs}),$$

est aussi impossible, compte tenu des connaissances « actuelles », que la quadrature du cercle !
Cependant, *les mathématiciens italiens de la Renaissance,* principalement ceux de Bologne, arrivent à résoudre algébriquement les équations du $3^{ème}$ degré, à coefficients entiers positifs (car les nombres négatifs n'étaient pas encore utilisés), en les ramenant aux trois types suivants :

$$x^3+px=q,\quad x^3=px+q,\quad x^3+q=px.$$

Plusieurs mathématiciens italiens se disputent alors la primauté de la résolution de ces équations, que certains gardent farouchement secrète.
Finalement, en 1545, le physicien Girolamo *Cardano* publie, dans *Ars Magna*, la résolution complète de ces équations, découverte, au moins une dizaine d'années auparavant, par des mathématiciens de l'époque, dont Niccolo *Fontana.*
Dans *Ars Magna*, Cardano donne les fameuses formules exprimant les solutions des équations du $3^{ème}$ degré, citées plus haut ; par exemple, celle (attribuée à Fontana) qui donne une solution de l'équation,

$$x^3+px=q, \quad \text{où} \quad p \text{ et } q \text{ sont des entiers positifs :}$$

$$x=\sqrt[3]{\frac{q}{2}+\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}+\sqrt[3]{\frac{q}{2}-\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}. \tag{9.1}$$

Ce sont des formules de ce type (qu' on a pris l'habitude d'appeler *Formules de Cardan*) qui permettent d'écrire les solutions d'une équation du genre $X^3+pX+q=0$, à coefficients dans $\mathbb{C}$ ([13], Ex. 7, Ch. 8) et on sait, d'autre part, que toute équation polynômiale de degré 3, peut se ramener à cette forme *canonique* ([13], p. 277).
Ces formules nous amènent à préciser le sens du Titre de ce Chapitre.

Etant donné une équation polynômiale à coefficients dans $\mathbb{Q}$, par définition, *résoudre cette équation par radicaux*, c'est pouvoir exprimer ses solutions, à l'aide des seules opérations suivantes : addition, multiplication, soustraction, division et extraction de racine.
Une **expression** algébrique, ainsi obtenue, sera dite **radicale**.
La publication de Cardano, *Ars Magna*, contenait aussi une méthode (due à Ludovico Ferrari) de résolution par radicaux, d'équations de degré 4, obtenue en se ramenant à la résolution d'équations de degré 3.
Dès 1545, il devient naturel de s'attaquer au problème de la résolution des équations de degré supérieur à 4, en particulier, de degré 5.
Plusieurs mathématiciens s'intéressent au problème. Mais ce n'est qu'en 1770, que *Lagrange* (Louis Joseph de) franchit une étape importante, en montrant que les méthodes, utilisées pour les équations de degré inférieur ou égal à 4, tombaient en défaut pour celles de degré 5.
Dès ce moment-là, l'idée, que toutes les équations du $5^{ème}$ degré n'étaient pas résolubles par radicaux, était dans l'air.
C'est *Abel* (Niels Henrik) qui, en 1824, trancha la question, en démontrant, rigoureusement, que l'équation polynômiale, dite *générale* (Déf. 9.26), du $5^{ème}$ degré, n'est pas résoluble par radicaux.
Le nouveau problème était alors, de savoir à quelle condition, une équation polynômiale de degré quelconque $n \geq 4$, est, ou non, résoluble par radicaux.
C'est Evariste *Galois*, qui, avant de mourir, en 1832, donna une réponse définitive à cette question ; mais, comme nous l'avons signalé dans la Préface, ses travaux ne furent publiés, qu'en 1843, par Joseph *Liouville*.

1. Extensions radicales

La notion d'*extension radicale* va permettre de formaliser algébriquement la notion de *polynôme résoluble par radicaux.*

Définition 9.1. Une extension de corps $L : K$ est dite **radicale** , si

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_m), \quad m \in \mathbb{N}^*, \quad \text{et}$$

$$\forall i (1 \leq i \leq m), \exists n_i \in \mathbb{N}^* ; \quad \alpha_1^{n_1} \in K, \quad \alpha_i^{n_i} \in K(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}). \tag{9.2}$$

On dit que les éléments α_i, $1 \leq i \leq m$, forment une **suite radicale** pour l'extension $L : K$.
Une extension $K(\alpha) : K$ sera dite **simple radicale** , s'il existe un entier $n \geq 1$ tel que $\alpha^n \in K$.

Remarque 9.2. a) Une extension radicale est de degré fini.
En effet, dans le contexte de la Déf. 9.1, pour tout $i (1 \leq i \leq m)$, posons
$L_i = K(\alpha_1, \alpha_2, \ldots, \alpha_i)$ et $L_0 = K$.

$$([L_i : L_{i-1}] = [L_{i-1}(\alpha_i) : L_{i-1}] \text{ et } \alpha_i^{n_i} \in L_{i-1}) \Longrightarrow [L_i : L_{i-1}] < \infty.$$

$$\text{Par suite,} \qquad [L : K] = \prod_{1 \leq i \leq m} [L_i : L_{i-1}] \Longrightarrow [L : K] < \infty.$$

$L : K$ est de degré fini, donc algébrique (Th. 2.26).

b) Avec les notations précédentes, on a

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{m-1} \subseteq L_m, \tag{9.3}$$

$$\forall i(1 \leq i \leq m), \quad L_i = L_{i-1}(\alpha_i) \quad \text{et} \quad \alpha_i^{n_i} \in L_{i-1},\ n_i \in \mathbb{N}^*. \tag{9.4}$$

On en déduit l'énoncé suivant.
Une extension $L : K$ est radicale si et seulement s'il existe une chaîne de corps intermédiaires telle que (9.3), *dans laquelle chaque extension $L_i : L_{i-1}$ est simple radicale.*

c) On suppose que, dans la relation (9.3), pour tout $i(1 \leq i \leq m)$, n_i est *minimal*, c'est-à-dire, est le plus petit entier non nul et positif vérifiant (9.2).
Par suite, si pour $1 \leq i \leq m$, l'entier n_i n'est pas premier et $n_i > 1$, alors il existe un nombre premier p_i qui divise n_i et

$$H_{i-1} := L_{i-1}(\alpha_i^{p_i}) \implies L_{i-1} \subset H_{i-1} \subset L_i.$$

On peut, dans ce cas, intercaler H_{i-1} dans la chaîne (9.3).
En réitérant ce processus, autant de fois qu'il est nécessaire, on aboutit à une chaîne du type (9.3), dans laquelle (moyennant une adaptation des notations), pour tout $i(1 \leq i \leq m)$, il existe une puissance première p_i de α_i qui appartient à L_{i-1}.

d) Toute *expression radicale*, telle qu'on l'a définie dans l'introduction historique, appartient à une extension radicale de $\mathbb{Q}$; par exemple

$$x = \sqrt{7}\sqrt[4]{3+\sqrt[3]{23}} + \sqrt[5]{\frac{1+\sqrt{5}}{2}} \implies x \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5), \text{ où,}$$

$$\alpha_1^2 = 7, \quad \alpha_2^3 = 23, \quad \alpha_3^4 = 3 + \alpha_2, \quad \alpha_4^2 = 5, \quad \alpha_5^5 = \frac{1+\alpha_4}{2}.$$

Cette remarque nous conduit à généraliser la notion d'équation polynômiale résoluble par radicaux, aux polynômes à coefficients dans un corps K quelconque.
Dans l'étude qui suit, nous supposerons $car K = 0$.

Définition 9.3. Etant donné un corps K de caractéristique 0 et un polynôme $f(X)$, non constant dans $K(X)$, on désigne par E, un corps de décomposition de $f(X)$ sur K. On dira que le **polynôme** $f(X)$ est **résoluble par radicaux** , s'il existe une extension R de E radicale sur K.

Remarque 9.4. a) Dans la Déf. 9.3, on a $K \subseteq E \subseteq R$ et il n'est pas nécessaire que E soit radicale sur K.
b) La définition 9.3 implique que toutes les racines du polynôme $f(X)$ sont exprimables par radicaux ; mais il est possible qu'un polynôme soit tel que seulement certaines de ses racines le soient. En effet, il suffit de prendre un produit de deux polynômes, dont l'un seulement est résoluble par radicaux.
Cependant, si $f(X)$ est *irréductible* sur K et si l'une de ses racines est exprimable par radicaux, les autres le sont aussi (Cf. Th. 2.16).

Définition 9.5. Etant donné $f(X)$, non constant dans $K(X)$ et E un corps de décomposition de $f(X)$ sur K, le groupe de Galois $G(E : K)$ est appelé **groupe de Galois du polynôme** $f(X)$ sur K.

Remarque 9.6. a) Dans la Déf. 9.5, le corps de décomposition E de $f(X)$ sur K est défini à un K-isomorphisme près (Cor. 3.9) ; on admettra que le groupe $G(E : K)$ est alors défini à un isomorphisme près.
b) Si $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ sont les racines *distinctes* de $f(X)$ dans E, alors tout $\sigma \in G(E : K)$, est une permutation des α_i, $1 \leq i \leq r$ (Rem. 7.11, d)). Par suite, $G(E : K)$ est un sous-groupe du groupe symétrique S_r ([12], Ch. III).

2. Polynômes résolubles par radicaux

A. Rappels concernant les groupes résolubles

La caractérisation des polynômes *résolubles par radicaux* est liée à la notion de groupe *résoluble* ([12], Ch. VII). C'est d'ailleurs cette question qui est à l'origine du qualificatif « résoluble » donné à de tels groupes.

Rappelons qu'on appelle *suite de composition* d'un groupe G ([12], Déf. 7.1), toute chaîne finie de sous-groupes de G du type :

$$(1) = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_1 \subseteq G_0 = G,$$

dans laquelle, pour tout $i\,(1 \leq i \leq n)$, on a $G_i \lhd G_{i-1}$.
Les groupes G_{i-1}/G_i sont appelés les *quotients* de la suite.

On utilisera, essentiellement, les propriétés suivantes :

(1) Les trois conditions suivantes sont équivalentes :

i) G est un groupe résoluble.

ii) G a une suite de composition telle que tous les quotients de la suite sont abéliens ([12], Th. 7.25).

iii) G contient un sous-groupe normal propre H tel que H et G/H sont résolubles ([12], Th. 7.29).

(2) Si G est un groupe résoluble, alors tout sous-groupe et tout quotient de G est résoluble ([12], Th. 7.23).

(3) Pour $n \geq 5$, le groupe symétrique S_n *n'est pas résoluble* ([12], Cor. 7.27).

B. Caractérisation des polynômes résolubles par radicaux

Le but de ce paragraphe est de prouver le résultat définitif obtenu par Galois :

Théorème 9.7. Théorème de Galois
Soit K un corps, de caractéristique 0, et $f(X) \in K[X] \setminus K$, alors $f(X)$ est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.

Cette assertion sera la conséquence directe du Th. 9.11 (Cond. necéssaire) et du Th. 9.12. Dans tout ce qui suit, K désigne un corps de caractéristique 0, ce qui entraîne que K est un corps parfait (Déf. 3.25.), donc une extension, de degré fini sur K, est galoisienne si et seulement si elle est normale sur K.

Lemme 9.8. *Si, pour un entier $n > 1$, le polynôme $X^n - 1$ de $K[X]$ est scindé sur K, alors, pour tout $a \neq 0$ dans K, le groupe de Galois du polynôme $X^n - a$ est abélien.*

Preuve : Voir Ex. **2.**, Ch 7.

Lemme 9.9. *Soit $F : K$ une extension galoisienne, de degré fini et $F(\gamma)$ une extension simple, radicale de F ; alors il existe une extension L de F telle que*
a) $L : F$ est radicale.

b) $L : F$ et $L : K$ sont galoisiennes.
c) Le groupe $G(L : F)$ est résoluble.
Si, de plus, on suppose $G(F : K)$ résoluble, alors $G(L : K)$ est résoluble.

Démonstration. On suppose $K \subset F \subset F(\gamma) \subset \overline{K}$, où $\overline{K}$ est une clôture algébrique de K.
a) Soit $n > 1$ le plus petit entier tel $\gamma^n \in F$. Posons

$$\alpha_1 := \gamma^n,\ p(X) := Irr_K(\alpha_1, X), \text{ et } k := deg\, p > 1.$$

La condition $car K = 0$ implique que $p(X)$ est un polynôme irréductible et séparable sur K (Cf. Ch. 3). D'autre part, $F : K$ est galoisienne, donc normale (Th. 7.27), alors $p(X)$ est scindé sur F. Soit

$$\alpha_i,\ (1 \leq i \leq n),\ \text{ les } k \text{ racines distinctes de } p(X) \text{ dans } F.$$

On a $\gamma^n = \alpha_1$ et, pour tout $i\,(2 \leq i \leq n)$, il existe $\gamma_i \in \overline{K}$, tel que $\gamma_i^n = \alpha_i$.
Soit $\omega \in \overline{K}$ une racine $n^{ème}$ primitive de l'unité de K. Posons $\gamma_1 := \gamma$ et

$$F_0 := F(\omega),\ F_i := F(\omega, \gamma_1, \gamma_2, \ldots, \gamma_i),\ \forall i (1 \leq i \leq k);\ L := F_k. \tag{9.5}$$

On a $F \subseteq F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = L$.
De plus, $\omega^n = 1$ implique que l'extension $F_0 : F$ est simple radicale et d'après la définition des γ_i, pour tout $i\,(1 \leq i \leq k)$, $F_i : F_{i-1}$ est simple radicale ; par suite, $L = F_k$ est radicale sur F (Rem. 9.2, b)).

b) Soit $q(X) := \prod_{1 \leq i \leq k} (X^n - \alpha_i)$; $q(X) \in F[X]$, puisque les α_i sont dans F. Les racines de ce polynôme sont les $\omega^j \gamma_i$, $1 \leq j \leq n$, $1 \leq i \leq k$.
Or, d'après ce qui précède, $L = F(\omega, \gamma_1, \gamma_2, \ldots, \gamma_k)$; par suite, L est corps de décomposition de $q(X)$ sur F, donc l'extension de degré fini $L : F$ est galoisienne (Cor. 7.28).
D'autre part,

$$p(X) = Irr_K(\alpha_1, X) = \prod_{1 \leq i \leq k} (X - \alpha_i) \Longrightarrow p(X^n) = q(X) \in K[X].$$

Soit $m := [F : K]$. Dans F, $\alpha_1 \neq 0$ entraîne l'existence d'une base B de F sur K telle que

$$B := \{\alpha_1, x_2, \ldots, x_m\}.$$

On a alors (Rem. 1.25), $F = K(\alpha_1, x_2, \ldots, x_m)$. Posons

$$p_s(X) := Irr_K(x_s, X), \forall s (2 \leq s \leq m) \quad \text{et} \quad f(X) := p(X) p_2(X) \ldots p_m(X).$$

Par hypothèse, $F : K$ est normale, de degré fini ; on en déduit que F est corps de décomposition de $f(X)$ sur K (Déf. 3.13, Th. 3.15), d'où

$$L = K(\omega, x_2, \ldots, x_m, \gamma_1, \gamma_2, \ldots, \gamma_k), \quad \text{car} \quad \alpha_1 = \gamma_1^n.$$

Ainsi, L est corps de décomposition, sur K, du polynôme séparable $q(X) p_2(X) \ldots p_m(X)$, donc $L : K$ est galoisienne, de degré fini.

c) Par hypothèse, $F : K$ est galoisienne, de degré fini. D'autre part, avec les notations utilisées précédemment, on a
$F_0 = F(\omega)$; or $F(\omega)$ est corps de décomposition de $X^n - 1$ sur F, donc $F_0 : F$ est galoisienne, de degré fini.
Quel que soit $i\,(1 \leq i \leq k)$, F_i est corps de décomposition de $X^n - \alpha_i$ sur F_{i-1}, par suite, $F_i : F_{i-1}$ est galoisienne, de degré fini.
Enfin, quel que soit $i\,(1 \leq i \leq k)$, $L = F_i(\gamma_{i+1}, \ldots, \gamma_k)$ implique que L est corps de décomposition, sur F_i, du polynôme

$$h_i(X) := (X^n - \alpha_{i+1})(X^n - \alpha_{i+2})\dots(X^n - \alpha_k);$$

donc $L : F_i$ est galoisienne, de degré fini.
On peut alors associer, à la chaîne d'extensions de corps

$$K \subseteq F \subseteq F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = L, \tag{9.6}$$

la chaîne de sous-groupes de $G(L : K)$:

$$(id_L) \subseteq G(L : F_{k-1}) \cdots \subseteq G(L : F_0) \subseteq G(L : F) \subseteq G(L : K). \tag{9.7}$$

La chaîne (9.7) est une *suite de composition* du groupe $G(L : K)$ (Cf. Rappels, Par. **A.** ci-dessus), car, compte tenu des hypothèses et des résultats précédents, on a, d'après le Théorème fondamental de Galois,

$$G(L : F) \lhd G(L : K), \quad G(L : F_0) \lhd G(L : F), \tag{9.8}$$

$$G(F_0 : F) \simeq G(L : F)/G(L : F_0), \tag{9.9}$$

$$\forall i (1 \leq i \leq k), \quad G(L : F_i) \lhd G(L : F_{i-1}), \tag{9.10}$$

$$G(F_i : F_{i-1}) \simeq G(L : F_{i-1})/G(L : F_i). \tag{9.11}$$

On a supposé $car K = 0$, on a donc aussi $car F = 0$ et par définition, $F_0 = F(\omega)$, où ω est une racine $n^{ème}$ primitive de l'unité ; alors le groupe de Galois
$G(F_0 : F) = G(F(\omega) : F)$ est abélien (même preuve que dans le cas où $F = \mathbb{Q}$, (Cf. Exemple 7.29, 2)).
D'autre part, la définition des F_i (Rel. (9.5)) montre que, pour tout $i (1 \leq i \leq k)$, F_i est corps de décomposition de $X^n - \alpha_i$ sur F_{i-1} et que le polynôme $X^n - 1$ est scindé sur F_{i-1}. De plus, d'après le Lem. 9.8, le groupe $G(F_i : F_{i-1})$ est abélien.
Alors, des Rel. (9.9) et (9.11), on déduit que tous les quotients de la suite de composition (9.7) sont abéliens, donc $G(L : F)$ est un groupe *résoluble* (Rappels, Par. **A.**).
Si on suppose, de plus, $G(F : K)$ résoluble, alors (Rappels, Par. **A.**, *i*) $\Longleftrightarrow$ *iii*)),

$$G(F : K) \simeq G(L : K)/G(L : F) \Longrightarrow G(L : K) \text{ résoluble.} \qquad \square$$

Lemme 9.10. *Si $M : K$ est une extension radicale, il existe, alors, une extension L de K, contenant M, telle que*

$$L : K \text{ est galoisienne, de degré fini, et } G(L : K) \text{ est résoluble.}$$

Démonstration. Par hypothèse, $M = K(\lambda_1, \lambda_2, \dots \lambda_s)$, $s \geq 1$, et

$$\forall i (1 \leq i \leq s), \exists n_i \in \mathbb{N}^* \text{ tel que } \lambda_1^{n_1} \in K, \quad \lambda_i^{n_i} \in K(\lambda_1, \lambda_2, \dots, \lambda_{i-1}).$$

Pour tout i, $1 \leq i \leq s$, on suppose l'entier n_i minimal (Rem. 9.2, b)).
Soit ω_1 une racine $n_1^{ème}$ primitive de l'unité de K. On pose $F = K(\omega_1)$; alors F est corps de décomposition de $X^{n_1} - 1$ sur K, de plus il existe $n_1 \in \mathbb{N}^*$ tel que $\lambda_1^{n_1} \in K \subseteq F$; par suite,

$$F : K \text{ est galoisienne, de degré fini et } F(\lambda_1) : F \text{ est simple radicale.}$$

D'après le Lem. 9.9., il existe une extension L_1 de F telle que

$$L_1 : F \text{ est radicale et galoisienne,}$$

$$L_1 : K \text{ est galoisienne et le groupe } G(L_1 : F) \text{ est résoluble.}$$

Or le groupe $G(F : K) = G(K(\omega_1) : K)$ est abélien, donc trivialement résoluble, par suite (Lem. 9.9.), $G(L_1 : K)$ est résoluble.
D'après la construction de L_1 (Voir L dans la preuve du Lem. 9.9), on a

$$K(\lambda_1) \subseteq L_1.$$

Considérons maintenant, les extensions $K \subseteq L_1 \subseteq L_1(\lambda_2)$;

$L_1 : K$ est galoisienne de degré fini et $L_1(\lambda_2)$ est simple radicale,

il existe alors (Lem. 9.9), une extension L_2 de L_1 telle que

$L_2 : L_1$ est radicale et galoisienne,

$L_2 : K$ est galoisienne et le groupe $G(L_2 : L_1)$ est résoluble.

Mais, d'après ce qui précède, le groupe $G(L_1 : K)$ est résoluble, ce qui entraîne (Lem. 9.9) $G(L_2 : K)$ résoluble.

D'après la construction de L_2 (Preuve du Lem. 9.9), on a

$$K(\lambda_1, \lambda_2) \subseteq L_2.$$

Ainsi, de proche en proche, on arrive à une extension L_s de degré fini sur K telle que

$$K(\lambda_1, \lambda_2, \ldots, \lambda_s) = M \subseteq L_s,$$

$L_s : K$ est galoisienne et le groupe $G(L_s : K)$ est résoluble.

On obtient l'énoncé du Lem. 9.11, en posant $L := L_s$. □

Théorème 9.11. *Si $f(X) \in K(X) \setminus K$ est un polynôme résoluble par radicaux, alors son groupe de Galois est résoluble.*

Démonstration. On suppose que $f(X) \in K[X] \setminus K$, est résoluble par radicaux (Déf. 9.3), donc Il existe une extension radicale $M : K$ telle que $K \subseteq E \subseteq M$, où E désigne un corps de décomposition de $f(X)$ sur K. Le Lem. 9.10. implique alors l'existence d'une extension L de M telle que

$L : K$ est galoisienne, de degré fini et $G(L : K)$ est résoluble.

L'application du Théorème fondamental de Galois (Th. 7.32.) aux extensions $K \subseteq E \subseteq L$ donne

$$G(E : K) \simeq G(L : K)/G(L : E).$$

Le groupe $G(E : K)$ est alors résoluble, en tant que quotient d'un groupe résoluble (Cf. Rappel (2), Par. **A.**). □

Théorème 9.12. *Etant donné un corps K de caractéristique 0, soit L une extension de degré fini, normale sur K telle que $G(L : K)$ est résoluble ; alors, il existe une extension $R : L$ telle $R : K$ est radicale.*

Démonstration. L'hypothèse $car K = 0$ entraîne que $L : K$ est séparable, par suite, $L : K$ est galoisienne de degré fini.

On démontre le théorème, par récurrence sur $n := [L : K]$. On pose $G := G(L : K)$ et $o(G)$ désigne l'ordre du groupe G.

Si $[L : K] = 1$, alors $L = K$ et K est trivialement radicale sur K.

Pour $[L : K] = n > 1$, on a $o(G) = n$. Soit H un sous-groupe propre, normal maximal de G; H existe, car G est un groupe fini d'ordre $n > 1$ ([12], Rem. 4.49). G/H est alors un groupe simple ([12], Prop. 4.52) et G/H est un groupe résoluble, car, par hypothèse, G est résoluble (Rappel (2), Par. **A.**). On en déduit que G/H est cyclique d'ordre premier ([12], Cor. 7.26). Soit $p := o(G/H)$ et E un corps de décomposition, sur L, du polynôme $X^p - 1$.

L'extension $L : K$ étant galoisienne, de degré fini, L est corps de décomposition, sur K, d'un polynôme (séparable) $f(X) \in K[X]$ (Cor. 7.28), donc E est corps de décomposition, sur K, de $(X^p - 1)f(X)$, par suite, E est galoisienne, de degré fini sur K.

Dans E, une racine $\omega \neq 1$, du polynôme $X^p - 1$ est une racine $p^{ème}$ primitive de l'unité, puisque p est un nombre premier, d'où $E = L(\omega)$.

Posons $M := K(\omega)$, alors, $\omega^p = 1$ implique que les extensions $E : L$ et $M : K$ sont simples radicales. Soit $\alpha_1, \alpha_2, \ldots, \alpha_r$, les racines distinctes de $f(X)$, dans $L \subseteq E$, alors,

$$\big(E = K(\omega, \alpha_1, \alpha_2, \ldots, \alpha_r) \text{ et } M = K(\omega)\big) \Longrightarrow E = M(\alpha_1, \alpha_2, \ldots, \alpha_r).$$

Ainsi, E est corps de décomposition de $f(X)$ sur M, on en déduit que est E galoisienne, de degré fini sur M.

D'autre part, on sait que le groupe $G(E:L) = G(L(\omega):L)$ est abélien (Ex. **19**, Ch. 7), donc résoluble et l'application du Théorème fondamental de Galois (Th. 7.32) aux extensions $K \subseteq L \subseteq E$, donne

$$G(L:K) \simeq G(E:K)/G(E:L).$$

Les groupes $G(L:K)$ et $G(E:L)$ étant résolubles, on en déduit que le groupe G(E : K) est résoluble (Rappels, **(1)**, $i) \Longleftrightarrow iii)$, Par. **A.**).

Montrons que $G(E:M)$ est isomorphe à un sous-groupe de $G(L:K)$.

Pour $\sigma \in G(E:M)$, on a

$$\sigma_{/M} = id_M \Longrightarrow \sigma_{/K} = id_K \Longrightarrow \sigma_{/L} \in G(L:K).$$

On peut alors considérer l'application

$$\begin{aligned} \rho : G(E:M) &\longrightarrow G(L:K) \\ \sigma &\longmapsto \sigma_{/L}. \end{aligned}$$

ρ est un morphisme de groupes ; vérifions que ρ est injectif.

$$\sigma \in Ker\rho \Longleftrightarrow \sigma_{/L} = id_L;$$

$$\sigma_{/M} = id_M \Longleftrightarrow \sigma_{/K} = id_K \text{ et } \sigma(\omega) = \omega;$$

or, $E = L(\omega)$, d'où, $(\sigma \in G(E:M) \text{ et } \sigma_{/L} = id_L) \Longrightarrow \sigma_{/E} = id_E$.

On en déduit que $Ker\rho = \{id_E\}$; donc ρ est injectif et

$$J := Im\rho \Longrightarrow G(E:M) \simeq J.$$

J est sous-groupe du groupe résoluble $G(L:K)$, donc J est résoluble, par suite, le groupe $G(E:M)$ est résoluble.

$\underline{1^{er} \text{ cas}}$: $J \neq G(L:K)$; l'extension $E:M$ étant galoisienne, on a (Th. 7.27)

$$[E:M] = \mid G(E:M) \mid = o(J) < n.$$

L'hypothèse de récurrence, appliquée à l'extension $E:M$, entraîne l'existence d'une extension R de E telle que $R:M$ est radicale et $K \subset L \subset E \subseteq R$.

Par définition, $M = K(\omega)$, où $\omega^p = 1$ et $\omega \neq 1$; alors si $\beta_1, \ldots, \beta_m$ est une suite radicale (Déf. 9.1) pour l'extension $R:M$,

$$R = M(\beta_1, \ldots, \beta_m) \Longrightarrow R = K(\omega, \beta_1, \ldots \beta_m)$$

et $\omega, \beta_1, \ldots, \beta_m$ est une suite radicale pour l'extension $R:K$, donc $R:K$ est radicale.

$\underline{2^{ème} \text{ cas}}$: $J = G(L:K)$; le morphisme ρ est alors, un isomorphisme de groupes. Soit $H' := \rho^{-1}(H)$, où H est le sous-groupe normal, d'indice p, de $G = G(L:K)$, considéré au début de la preuve.

Puisque ρ est un isomorphisme, H' est un sous-groupe normal, d'indice p, dans $G(E:M)$.

$$F := Inv_E(H') \Longrightarrow M \subseteq F \subseteq E.$$

L'extension $E:M$ est galoisienne, de degré fini, alors, d'après le Théorème fondamental de Galois (Th. 7.32), il en est de même de $E:F$ et de plus, puisque $H' = G(E:F)$, on a

$$H' \lhd G(E:M) \Longrightarrow F:M \text{ galoisienne, de degré fini}$$
$$\text{et} \qquad G(F:M) \simeq G(E:M)/H'.$$

D'autre part, le polynôme $X^p - 1$ est scindé sur M ; on en déduit (Th. 7.55) que $F = M(\alpha)$, où $\alpha^p = a \in M$, le polynôme $X^p - a$ étant irréductible sur M.

L'extension, de degré fini $E:F$ est galoisienne, donc normale ;

$$M \subsetneq F \subseteq E \Longrightarrow G(E:F) \subsetneq G(E:M);$$

on en déduit que $[E:F] = \mid G(E:F) \mid < \mid G(E:M) \mid = n$ et

$$G(E:M) \simeq G(L:K) \Longrightarrow G(E:F) \text{ résoluble.}$$

L'hypothèse de récurrence appliquée à l'extension $E : F$ entraîne l'existence d'une extension R de E telle que $R : F$ est radicale ; on a $L \subseteq E$, donc R est extension de L et

$$(R : F \text{ radicale}, \ F = M(\alpha), \ \alpha^p = a \in M) \Longrightarrow R : M \text{ radicale};$$
$$(R : M \text{ radicale}, \ M = K(\omega), \ \omega^p = 1 \Longrightarrow R : K \text{ radicale.})$$

□

Preuve du Théorème de Galois (Th. 9.7)

Rappel de l'énoncé : Etant donné un corps $K\,(car K = 0)$, $f(X) \in K(X) \setminus K$ *est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Démonstration. D'après le Th. 9.11, si $f(X)$ est résoluble, son groupe de Galois est résoluble. Montrons que le Th. 9.12 entraîne la réciproque de ce résultat.
Soit E un corps de décomposition, sur K, d'un polynôme $f(X)$ non constant de $K[X]$; si le groupe $G(E : K)$ est résoluble, alors, d'après le Th. 9.12, il existe une extension R de E telle que $R : K$ est radicale, donc $f(X)$ est résoluble par radicaux (Déf. 9.3). □

Remarque 9.13. a) Un polynôme $f(X) \in K[X] \setminus K$ $(car K = 0)$, dont le groupe de Galois est *abélien* est résoluble par radicaux ; en particulier, quel que soit
$n > 1$, $X^n - 1 \in \mathbb{Q}[X]$, est résoluble par radicaux.
b) Pour tout $n \geq 5$, le groupe symétrique S_n étant non résoluble (Rappel, **(3)**, Par. **A.**), tout polynôme de $K[X]$, dont le groupe de Galois est isomorphe à un groupe symétrique S_n $n \geq 5$, est non résoluble par radicaux.
L'étude de certains de ces polynômes fait l'objet du paragraphe suivant.

3. Exemples de polynômes non résolubles par radicaux

A. Polynômes de degré premier impair

Proposition 9.14. *Soit p un nombre premier impair et, dans $\mathbb{Q}[X]$, un polynôme $f(X)$, irréductible, de degré p, ayant exactement deux racines complexes, non réelles, alors le groupe de Galois de $f(X)$ sur $\mathbb{Q}$ est le groupe symétrique S_p.*

Démonstration. Soit $E \subset \overline{\mathbb{Q}}$, un corps de décomposition de $f(X)$ sur $\mathbb{Q}$. L'extension $E : \mathbb{Q}$ est galoisienne, de degré fini ; posons $G := G(E : \mathbb{Q})$.
Le polynôme irréductible $f(X)$ est séparable (Th. 3.24), donc G est un groupe de permutations des p racines distinctes de $f(X)$ dans E ; G peut alors être considéré comme un sous-groupe de S_p.
Soit $\alpha \in E$ tel que $f(\alpha) = 0$; alors, $f(X) = Irr_{\mathbb{Q}}(\alpha, X)$, d'où

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = p \Longrightarrow p \mid [E : \mathbb{Q}].$$

Par suite, $p \mid o(G)$; or, p est premier, donc il existe au moins un élément, σ, d'ordre p dans G ([12], Cor. 6.4). Mais les seuls éléments d'ordre p, dans S_p, sont les p-cycles ([12], Ch. III) donc σ est un p-cycle.
D'autre part, notons ici, Γ, la conjugaison complexe :

$$\Gamma : \mathbb{C} \longrightarrow \mathbb{C} \text{ et } \Gamma(a + ib) = a - ib, \ \forall a + ib \in \mathbb{C}.$$

Γ est un $\mathbb{R}$-automorphisme de $\mathbb{C}$, donc $\Gamma_{/E} \in G$; de plus, $\Gamma_{/E}$ laisse fixes les $p-2$ racines réelles de $f(X)$ et permute ses deux racines non réelles. On en déduit que le groupe G contient un 2-cycle, c'est-à-dire, une transposition.
En changeant, au besoin, les notations, on peut supposer que G contient la transposition $(1,2)$ et le cycle $(1,2,\ldots,p-1,p)$; or ces deux permutations engendrent le groupe symétrique S_p ([12], Ex. **24.**, Ch. III), par suite, $G = S_p$. □

Remarque 9.15. Un polynôme de degré premier $p \geq 5$, satisfaisant aux hypothèses de la Prop. 9.14, est non résoluble par radicaux.

Exemple 9.16. Soit $f(X) = X^5 - 4X - 2$ dans $\mathbb{Q}[X]$.
Ce polynôme est unitaire et irréductible dans $\mathbb{Z}[X]$, d'après le Critère d'Eisenstein (appliqué avec $p = 2$) ([13], Prop. 5.112), c'est donc un polynôme irréductible de $\mathbb{Q}[X]$ ([13], Prop. 5.108.), de degré 5 (premier impair). Montrons que $f(X)$ a exactement trois racines réelles distinctes. On note que

$$f(-2) = -26,\ f(-1) = 1,\ f(0) = -2,\ f(1) = -5,\ f(2) = 22.$$

La fonction polynôme f, de $\mathbb{R}$ dans $\mathbb{R}$, étant une fonction continue, on en déduit qu'il existe $\alpha_1, \alpha_2, \alpha_3$, réels tels que

$$-2 < \alpha_1 < -1 < \alpha_2 < 0 < 1 < \alpha_3 < 2 \quad \text{et} \quad f(\alpha_i) = 0, \text{ pour } i = 1,2,3.$$

L'étude de la croissance de la fonction réelle f montre que le polynôme $f(X)$ n'a pas d'autre racine réelle. En effet,

$$f'(X) = 5x^4 - 4 = (\sqrt{5}X^2 - 2)(\sqrt{5}X^2 + 2);$$

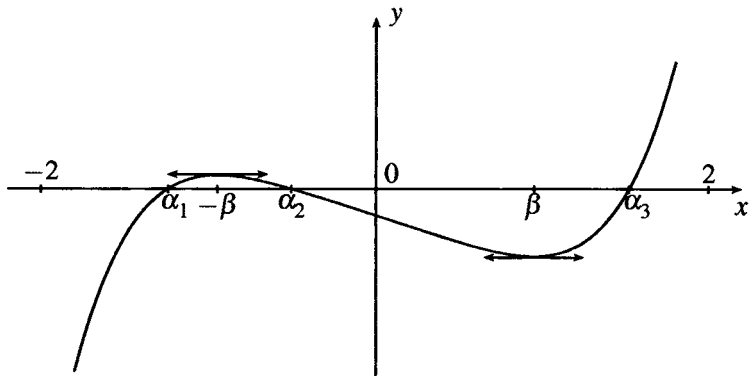
Le signe de $f'(x)$, pour x réel, est celui de $\sqrt{5}x^2 - 2$, qui s'annule pour $x = \pm\sqrt{\frac{2}{\sqrt{5}}}$. Posons $\beta := \sqrt{\frac{2}{\sqrt{5}}}$; on a $f'(-\beta) = f'(\beta) = 0$ et le tableau de variation de la fonction réelle f est le suivant

	$-\infty$		-1	$-\beta$		0	β	1		$+\infty$
$f'(x)$		$+$		0	$-$		0		$+$	
$f(x)$	$-\infty$	↗		M	↘		m	↗		$+\infty$

On a nécessairement

$$-2 < \alpha_1 < -1 < -\beta < \alpha_2 < 0 < \beta < 1 < \alpha_3 < 2$$

et $f(x)$ a un maximum positif $f(-\beta)$ et un minimum négatif $f(\beta)$.



On en conclut que $f(X)$ a exactement trois racines réelles distinctes, α_i, $1 \leq i \leq 3$, donc deux racines complexes, non réelles. Par suite (Prop. 9. 15), le groupe de Galois de $f(X)$ est le groupe symétrique S_5, non résoluble, d'où $f(X)$ non résoluble par radicaux.

B. Equation polynômiale générale

1 / Degré de transcendance d'une extension de type fini

Définition 9.17. On dira qu'une extension de corps $L : K$ est **de type fini** si L est obtenue par l'ajonction à K, d'un nombre fini d'éléments.

Remarque 9.18. Soit L est une extension d'un corps K, si $t_1, t_2, \ldots, t_n$, $n > 1$, sont des éléments de L, tous transcendants sur K, alors, ces éléments peuvent être algébriquement indépendants (Déf. 5.17) ou algébriquement dépendants sur K, comme le montrent les exemples suivants.
Soit t et u dans L ; supposons t transcendant sur K et u transcendant sur $K(t)$. Vérifions que t et u sont *algébriquement indépendants* sur K.
En effet,l'anneau de polynômes $K[X,Y]$ étant identifiable à l'anneau $K[X][Y]$, si u est transcendant sur $K(t)$ alors,

$$(f(u) \neq 0, \quad \forall f \in K(t)[Y]) \Longrightarrow g(t,u) \neq 0, \quad \forall g \in K[X,Y].$$

Par contre, soit $t \in L$ transcendant sur K et $u = t + 1$, alors u est un élément de L, transcendant sur K, mais

$$(f(X,Y) = X - Y + 1, \text{ dans } K[X,Y]) \Longrightarrow f(t,u) = 0,$$

donc, dans ce cas, t et u sont *algébriquement dépendants* sur K.

Proposition 9.19. *Soit $L : K$ une extension de corps* de type fini, *non algébrique ; il existe alors un corps intermédiaire F tel que*
i) $F = K(\alpha_1, \ldots, \alpha_r)$, $r \in \mathbb{N}^*$, où les α_i, $1 \leq i \leq r$, sont transcendants, algébriquement indépendants sur K ;
ii) $[L : F]$ est fini.
iii) Si M est un autre corps intermédiaire tel que $M = K(\beta_1, \ldots, \beta_s)$, où les β_j, $1 \leq j \leq s$, sont transcendants, algébriquement indépendants sur K et $[L : M]$ fini, alors, $s = r$.

Démonstration. On suppose $L = K(\alpha_1, \ldots, \alpha_n)$, non algébrique sur K, donc il existe au moins un $\alpha_i, 1 \leq i \leq n$, transcendant sur K ; de plus on a nécessairement $[L : K]$ infini (Prop. 2.36). Quitte à changer l'ordre des α_i, on peut supposer α_1 transcendant sur K.
Si $[L : K(\alpha_1)] < \infty$, alors $F := K(\alpha_1)$ vérifie les conditions i) et ii) de l'énoncé.
Si $[L : K(\alpha_1)]$ est infini, il existe nécessairement α_i, $2 \leq i \leq n$, transcendant sur $K(\alpha_1)$, donc sur K ; supposons α_2 transcendant sur $K(\alpha_1)$.
Si $[L : K(\alpha_1, \alpha_2)] < \infty$, alors $F := K(\alpha_1, \alpha_2)$ convient, sinon, on réitére le processus, jusqu'à ce que l'on obtienne, pour r, $1 \leq r \leq n$, $K(\alpha_1, \ldots, \alpha_r)$, tel que

$$[L : K(\alpha_1, \ldots, \alpha_r)] < \infty ; \text{ alors, } F = K(\alpha_1, \ldots, \alpha_r) \text{ vérifie i) et ii).}$$

Le procédé de construction de F montre que chaque α_i, $1 \leq i \leq r$, est transcendant sur $K_{i-1} = K(\alpha_1, \ldots, \alpha_{i-1})$, où $K_0 = K$. On en déduit que les α_i, $1 \leq i \leq r$, sont trancendants, algébriquement indépendants sur K.
Montrons que F satisfait à la condition iii) de l'énoncé.
Soit M un corps tel que $K \subseteq M \subseteq L$, $[L : M] < \infty$ et $M = K(\beta_1, \ldots, \beta_s)$, où les β_j, $1 \leq j \leq s$, sont transcendants, algébriquement indépendants sur K.

$$[L : F] < \infty \Longrightarrow L \text{ algébrique sur } F \Longrightarrow M \text{ algébrique sur } F ;$$

alors, β_1 est algébrique sur F, donc il existe $f \in F[X]$, tel que $f(\beta_1) = 0$; d'autre part, $F = K(\alpha_1, \ldots, \alpha_r)$ implique $f \in K(\alpha_1, \ldots, \alpha_r)[X]$. On en déduit qu'il existe g dans l'anneau des polynômes à $r + 1$ indéterminées sur K tel que

$$g(\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_r) = 0. \tag{9.12}$$

Si l'élément α_1 figure explicitement dans l'égalité (9.12), alors α_1 est algébrique sur $K(\beta_1, \alpha_2, \ldots, \alpha_r)$. On a

$$[L:F] < \infty \Longrightarrow [L : K(\beta_1, \alpha_1, \ldots, \alpha_r)][K(\beta_1, \alpha_1, \ldots, \alpha_r) : F] < \infty$$
$$\Longrightarrow [L : K(\beta_1, \alpha_1, \ldots, \alpha_r)] < \infty.$$

$$K(\beta_1, \alpha_2, \ldots, \alpha_r) \subset K(\beta_1, \alpha_1, \ldots, \alpha_r) \subseteq L \quad \text{implique}$$

$$[L : K(\beta_1, \alpha_1, \ldots, \alpha_r)][K(\beta_1, \alpha_1, \ldots, \alpha_r) : K(\beta_1, \alpha_2, \ldots, \alpha_r)] < \infty,$$
$$\text{d'où,} \qquad [L : K(\beta_1, \alpha_2, \ldots, \alpha_r)] < \infty.$$

Si $s > r$, avec le processus précédent, on remplace, de proche en proche les α_i, $1 \leq i \leq r$, respectivement, par les β_i, $1 \leq i \leq r$; on obtient alors,

$$[L : K(\beta_1, \beta_2, \ldots, \beta_r)] < \infty,$$

d'où, compte tenu des hypothèses, β_{r+1} transcendent sur $K(\beta_1, \beta_2, \ldots, \beta_r)$, ce qui contradit $L : K(\beta_1, \beta_2, \ldots, \beta_s)$ algébrique, d'où nécessairement, $s \leq r$.
Si l'on avait $s < r$, alors, le raisonnement précédent, appliqué en échangeant les rôles de F et M, conduirait à : $r \leq s$, donc, en conclusion $r = s$. □

Remarque 9.20. Les hypothèses étant celles de la Prop. 9.19, l'entier $r > 0$ caractérise l'extension $L : K$ de type fini, non algébrique.
Si une extension $L : K$ est de type fini et algébrique, alors L est obtenue par l'adjonction à K d'un nombre fini d'éléments, tous algébriques sur K, ce qui entraîne (Th. 2.29) :

$$[L : K] < \infty.$$

On peut, alors, considérer que le résultat de la Prop. 9.19 reste valable, en prenant

$$F = K \quad \text{et} \quad r = 0.$$

Définition 9.21. L'entier $r \geq 0$ qui, selon la Prop. 9.19 et la Rem. 9.20, caractérise une extension de corps de type fini $L : K$, est appelé le **degré de transcendance** de cette extension.

Remarque 9.22. Si $L = K(\alpha_1, \ldots, \alpha_n)$, $n \in \mathbb{N}^*$, on a $0 \leq r \leq n$ et

$r = 0 \iff [L : K] < \infty \iff L : K$ algébrique;
$r > 0 \iff [L : K]$ infini $\iff L : K$ non algébrique.
$r = n \iff \alpha_1, \ldots, \alpha_n$ transcendants, algébriquement indép. sur K.

Exemple 9.23. Supposons $L = K(t, u, v)$, où t est transcendant sur K, $u^2 = t$ et v transcendant sur $K(t, u)$.
Posons $F := K(t, v)$, alors t, v sont transcendants, algébriquement indépendants sur K et $[L : F] = [F(u) : F] = 2$, par suite, le degré de transcendance de L sur K est 2.

Remarque 9.24. On rappelle que toute extension simple, transcendante d'un corps K, est isomorphe à l'extension $K(X) : K$, où $K(X)$ est le corps des fractions rationnelles à une indéterminée sur K (Th. 2.5).
Par récurrence, on montre qu'une extension de type fini,

$$L = K(\alpha_1, \ldots, \alpha_n),\ n \in \mathbb{N}^*,$$

où les α_i, $1 \leq i \leq n$, sont *transcendants, algébriquement indépendants* sur K, est isomorphe à l'extension $K(X_1, \ldots, X_n) : K$, où $K(X_1, \ldots, X_n)$ est le corps des fractions rationnelles, à n indéterminées sur K ; cet isomorphisme est défini par

$$K(X_1, \ldots, X_n) \longrightarrow K(\alpha_1, \ldots, \alpha_n)$$
$$f(X_1, \ldots, X_n) \longmapsto f(\alpha_1, \ldots, \alpha_n),$$
$$\text{d'où,} \quad \forall u \in L, \exists! f \in K(X_1, \ldots, X_n)\ ;\ u = f(\alpha_1, \ldots, \alpha_n). \tag{9.13}$$

Proposition 9.25. *Soit $L = K(\alpha_1, \ldots, \alpha_n)$ une extension de type fini de K, $n \in \mathbb{N}^*$, où les α_i, $1 \leq i \leq n$, sont transcendants, algébriquement indépendants sur K ; alors,*
1) *Le groupe symétrique S_n s'identifie à un sous-groupe de $G(L : K)$.*
2) *$F := Inv_L(S_n) = K(s_1, \ldots, s_n)$, où les s_k, $1 \leq k \leq n$, sont les fonctions symétriques élémentaires des α_i, $1 \leq i \leq n$.*
$[L : F] = n!$, $G(L : F) = S_n$, d'où $L : F$ galoisienne de degré fini.
De plus, les s_k, $1 \leq k \leq n$, sont transcendants, algébriquement indépendants sur K.

Démonstration. 1) Soit $G := G(L : K)$ et S_n le groupe des permutations de $\{1, 2, \ldots, n\}$, que l'on identifie au groupe de permutations de l'ensemble $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, en posant ([12], Lem. 1.74) :

$$\forall \sigma \in S_n,\ \forall i (1 \leq i \leq n),\ \sigma(\alpha_i) = \alpha_{\sigma(i)}.$$

On peut alors considérer que tout $\sigma \in S_n$ détermine un élément du groupe G, que l'on appellera encore σ, tel que

$$\forall a \in K,\ \forall i (1 \leq i \leq n),\ \sigma(a) = a,\ \sigma(a\alpha_i) = a\alpha_{\sigma(i)}.$$

On identifie ainsi S_n, à un sous-groupe de $G = G(L : K)$.
2) Soit $F := Inv_L(S_n)$.
On rappelle qu'une fraction rationnelle $f \in K(X_1, \ldots, X_n)$ est dite *symétrique* ([13], p. 260) si

$$\forall \sigma \in S_n,\ f_\sigma = f,$$

où, dans $K(X_1, \ldots, X_n)$, $f_\sigma(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$.
Par suite, compte tenu de la relation (9.13), pour $f \in K(X_1, \ldots, X_n)$,

$$f(\alpha_1, \ldots, \alpha_n) \in F \iff f_\sigma = f,\ \forall \sigma \in S_n. \tag{9.14}$$

Ainsi, toute expression polynômiale sur K, symétrique en $\alpha_1, \alpha_2, \ldots, \alpha_n$, appartient à F ; en particulier, les fonctions symétriques élémentaires des α_i ([13], p. 250) sont des éléments de F. Compe tenu des notations de l'énoncé, pour tout k, $1 \leq k \leq n$,

$$s_k = \Sigma_k(\alpha_1, \ldots, \alpha_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_k}.$$

En particulier,
$$s_1 = \Sigma_1(\alpha_1, \ldots, \alpha_n) = \alpha_1 + \alpha_2 + \cdots + \alpha_n,$$
$$s_2 = \Sigma_2(\alpha_1, \ldots, \alpha_n) = \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j;$$
$$\ldots\ldots$$
$$s_n = \Sigma_n(\alpha_1, \ldots, \alpha_n) = \alpha_1 \alpha_2 \ldots \alpha_n.$$

D'après ce qui précède, on a $K(s_1, \ldots, s_n) \subseteq F$.
Mais, pour toute fraction rationnelle f *symétrique* dans $K(X_1, \ldots, X_n)$, il existe ([13], Th. 8.29) une fraction rationnelle ϕ, à n indéterminées sur K, telle que

$$f(\alpha_1, \ldots, \alpha_n) = \phi(s_1, \ldots, s_n). \tag{9.15}$$

La relation (9.14) implique alors,

$$F := Inv_L(S_n) = K(s_1, \ldots, s_n).$$

D'autre part, S_n étant un sous-groupe *fini* de $G(L : K) \subset Aut\, L$, d'après le Thèorème d'Artin (Th. 7.26), on a

$$[L : F] = |\, S_n \,| = n!, \quad G(L : F) = S_n, \quad \text{et} \quad F = Inv_L(G(L : F)),$$

donc l'extension $L : F$ est galoisienne de degré fini.
De plus, quel que soit k, $1 \leq k \leq n$, s_k est un polynôme symétrique en $\alpha_1, \ldots, \alpha_n$. Or, par hypothèse, les α_i, $1 \leq i \leq n$, sont transcendants, algébriquement indépendants sur K. On en déduit (en utilisant (9.15)) que $s_1, \ldots, s_n$ sont transcendants, algébriquement indépendants sur K.
Par suite, le degré de transcendance des extensions de type fini $L : K$ et $F : K$ est n. □

2 / Notion de polynôme général sur un corps

Définition 9.26. Soit $F = K(s_1, \ldots, s_n)$ une extension de type fini d'un corps K, où l'on suppose que les s_k, $1 \leq k \leq n$, sont transcendants, algébriquement indépendants sur K; alors, le polynôme

$$g(X) = X^n - s_1 X^{n-1} + \cdots + (-1)^k s_k X^{n-k} + \cdots + (-1)^n s_n, \tag{9.16}$$

appartenant à $F[X]$, est appelé le

polynôme général, de degré n, sur K.

L'équation $g(X) = 0$ est alors,

l'équation polynômiale générale , de degré n, sur K.

Théorème 9.27. *Les hypothèses et les notations étant celles de la* Déf. 9.26, *soit L un corps de décompositon, sur F, du polynôme « général », $g(X)$, de degré n sur K ; alors les zéros $\alpha_1, \ldots, \alpha_n$, de $g(X)$, dans L, sont transcendants, algébriquement indépendants sur K et le groupe de Galois de $g(X)$ est le groupe symétrique S_n.*

Démonstration. Les hypothèses impliquent que $L = F(\alpha_1, \ldots, \alpha_n)$ (Prop. 3.5) et que $L : F$ est de degré fini (Th. 3.15).
D'autre part, les Relations entre les Coefficients et les Racines du polynôme $g(X)$ ([13], p. 259) montrent que les s_k, $1 \leq k \leq n$, sont, respectivement, égaux aux n fonctions symétriques élémentaires des α_i, $1 \leq i \leq n$; alors,

$$F = K(s_1, \ldots, s_n) \Longrightarrow L = K(\alpha_1, \ldots, \alpha_n).$$

Ainsi, L est une extension de K telle que

$$K \subset F \subset L, \quad [L : F] < \infty$$

Par hypothèse, le degré de transcendance de $F : K$ est n. On en déduit (Prop. 9.19) que, nécessairement, le degré de transcendance de $L : K$ est n, donc les zéros $\alpha_1, \ldots, \alpha_n$, du polynôme $g(X)$ sont transcendants, algébriquement indépendants sur K.
On se retrouve dans le contexte de la Prop. 9.25 ; on en conclut que $G(L : F) = S_n$ et $G(L : F)$ est ici, le groupe de Galois du polynôme $g(X)$ (Déf. 9.5). □

Théorème 9.28. *Si K est un corps de caractéristique* 0 *et $n \geq 5$, alors le polynôme général, de degré n sur K,* n'est pas résoluble par radicaux.

Démonstration. D'après le Th. 9.27, le groupe de Galois du polynôme général, de degré n sur K, est le groupe symétrique S_n, qui n'est pas résoluble, pour $n \geq 5$ (Rappels, Par. **A.**).
On en conclut, d'après le Théorème de Galois (Th. 9.7), que, pour $n \geq 5$, le polynôme général, de degré n sur K n'est pas résoluble par radicaux. □

4. Exercices

1. *Notations* : Pour une extension de corps $F : K$, on écrira

$$K \lhd F$$

pour exprimer que $F : K$ est galoisienne, de degré fini.

Etant donné un corps K de *caractéristique* 0, $\overline{K}$ désigne une clôture algébrique de K. Soit $\gamma \in \overline{K}$; on considère les extensions de corps

$$K \subseteq F \subseteq F(\gamma) \subset \overline{K}$$

telles que, par hypothèse,

i) $K \lhd F$;

ii) $\exists n \in \mathbb{N}^*$ tel que $\gamma^n \in F$.

On suppose que n est le plus petit entier vérifiant la condition ii).

1°) On pose $\alpha_1 := \gamma^n$, $p(X) := Irr_K(\alpha_1, X)$ et $k := deg\, p(X)$.

On supposera $k > 1$.

a) Vérifier que $p(X)$ a k racines distinctes dans F ; on les notera $\alpha_1, \alpha_2, \ldots, \alpha_k$.

b) On pose $[F : K] = m$; justifier l'existence d'une base de F sur K pouvant s'écrire $\{\alpha_1, x_2, \ldots, x_m\}$.

En déduire un polynôme $f(X) \in K[X]$ divisible par $p(X)$ et admettant F comme corps de décomposition sur K.

2°) Pour tout $i (1 \leq i \leq k)$, soit $\gamma_i \in \overline{K}$ tel que $\gamma_i^n = \alpha_i$, avec $\gamma_1 = \gamma$.

ε désignant une racine $n^{ème}$ primitive de l'unité de K, on pose

$$L := F(\varepsilon, \gamma_1, \ldots, \gamma_k)$$
$$F_i := F(\varepsilon, \gamma_1, \ldots, \gamma_i), \forall i (1 \leq i \leq k) ; F_0 = F(\varepsilon).$$

Démontrer les propriétés suivantes.

a) $L : F$ est une extension radicale.

b) $F \lhd F(\varepsilon)$, $\forall i (1 \leq i \leq k)$, $F_i \lhd F_{i+1}$ et $F_i \lhd L$.

3°) a) En utilisant le polynôme $q(X) := \prod_{1 \leq i \leq k} (X^n - \alpha_i)$,

montrer que $F \lhd L$.

b) Vérifier que $q(X) \in K[X]$; à l'aide du 1°), prouver que $K \lhd L$.

4°) a) Montrer que les groupes de Galois $G(L : F_i)$, $1 \leq i \leq k$, forment, avec le groupe $G(L : F)$, une suite de composition ([12], Déf. 7.1) du groupe $G(L : K)$.

b) Vérifier que le groupe $G(F_0 : F)$ est abélien.

c) En considérant les quotients de la suite de composition du groupe $G(L : F)$, extraite de la suite de composition de $G(L : K)$, prouver que le groupe $G(L : F)$ est résoluble ([12], Ch. 7).

d) Montrer que, *si l'on suppose de plus* $G(F : K)$ résoluble, alors le groupe $G(L : K)$ est résoluble.

2. K désigne un corps de *caractéristique* 0 et $\overline{K}$ est une clôture algébrique de K. On utilisera la notation « $K \lhd F$ », définie dans l'exercice précédent.

1°) Soit $M \subset \overline{K}$ une extension radicale de K. On suppose

$$M := K(\lambda_0, \lambda_1, \ldots, \lambda_s),\ s \in \mathbb{N}^* \text{ et}$$
$$\forall i (0 \leq i \leq s),\ \exists n_i \in \mathbb{N}^* ;\ \lambda_0^{n_0} \in K,\ \lambda_i^{n_i} \in K(\lambda_0, \ldots, \lambda_{i-1}).$$

a) ε_0 étant une racine $n_0^{ème}$ primitive de l'unité de K, on pose $F := K(\varepsilon_0, \lambda_0)$ et on considère les extensions

$$K \subset F \subset F(\lambda_1).$$

En utilisant les résultats de l'Ex. **1.** précédent, montrer qu'il existe une extension L_1 de K telle que

L_1 est radicale sur K et $K \lhd L_1$,
$K(\lambda_0, \lambda_1) \subset L_1$ et $G(L_1 : K)$ résoluble.

b) En réitérant le raisonnement ci-dessus, à partir des extensions

$$K \subset L_1 \subset L_1(\lambda_2),$$

montrer qu'il existe une extension L de K vérifiant les conditions :

L est radicale sur K, $K \lhd L$, $M \subset L$, et $G(L : K)$ est résoluble.

2°) Montrer que les résultats précédents donnent une preuve du Th. 9.11.

Appendice A
Corps ordonnés - Complétion d'un corps valué

1. Corps ordonnés

Définition A.1. Un corps K est un **corps ordonné** s'il existe une partie P de K telle que

$$\begin{aligned} &i)\ 0 \notin P; \\ &ii)\ a \in K \Longrightarrow (a \in P \quad \text{ou} \quad a = 0 \quad \text{ou} \quad -a \in P); \\ &iii)\ (a,b) \in P \times P \Longrightarrow (a+b \in P \quad \text{et} \quad ab \in P). \end{aligned}$$

P est alors appelé l' **ensemble des éléments positifs** de K.

Proposition A.2. *Si K est un* corps ordonné, *alors la relation binaire, notée $\leq$, et définie dans K par*

$$a \leq b \iff (a = b \quad \textit{ou} \quad (b-a) \in P) \tag{A.1}$$

est une relation d'ordre total *telle que*

$$\begin{aligned} &1)\ a \in P \Longrightarrow 0 < a. \\ &2)\ (a,b,c \ \textit{dans}\ K \quad \textit{et} \quad a \leq b) \Longrightarrow a+c \leq b+c. \\ &3)\ (a,b,c \ \textit{dans}\ K \quad \textit{et} \quad a \leq b,\ 0 \leq c) \Longrightarrow ac \leq bc. \\ &4)\ a \in K \Longrightarrow a^2 \geq 0. \end{aligned}$$

De plus, le corps K est de caractéristique 0.

Démonstration. Tout corps K ayant au moins un élément non nul, si K satisfait aux conditions de la Déf. A.1, alors P est non vide, et on montre facilement que la relation (A.1) définit une relation d'ordre dans K (à vérifier par le lecteur). De plus, la condition *ii)* implique

$$\forall (a,b) \in K \times K, \quad b-a = 0 \quad \text{ou} \quad b-a \in P \quad \text{ou} \quad -(b-a) \in P.$$

On en déduit que

$$\forall (a,b) \in K \times K, \quad a = b \quad \text{ou} \quad a < b \quad \text{ou} \quad a > b,$$

donc K est *totalement ordonné* par la relation (A.1).

Vérifions les propriétés énoncées :

1) $a \in P \Longrightarrow a \neq 0$; alors, $a - 0 \in P \Longrightarrow 0 < a$.
2) Soit a, b dans K tels que $a \leq b$; quel que soit $c \in K$, on a
ou bien $a = b \Longrightarrow a+c = b+c$ ou bien $b-a \in P \Longrightarrow \big((b+c-(a+c)\big) \in P$,
d'où $a+c \leq b+c$.
3) De l'hypothèse ($a \leq b$ et $0 \leq c$), on déduit que

pour $c=0$, on a $ac=bc=0$ et pour $0<c$, on a deux possibilités :

$$b-a=0 \Longrightarrow bc-ac=0 \quad \text{ou} \quad b-a\in P \Longrightarrow bc-ac\in P,$$

d'où la propriété 3).

4) Soit $a\in K$, si $a\neq 0$, alors, moyennant les conditions ii) et iii),

$$(a\in P \quad \text{ou} \quad -a\in P) \Longrightarrow a^2\in P \Longrightarrow 0<a^2,$$

d'où $0\leq a^2$, quel que soit $a\in K$.

En particulier, si 1 désigne l'élément unité du corps K, alors

$$1=1^2 \Longrightarrow 1\in P$$

et la condition iii) entraîne : $n1\in P, \forall n\in\mathbb{N}^*$. On en conclut que $carK=0$. □

Remarque A.3. Posons $N:=\{-a\in K\,;\,a\in P\}$; la Déf. A.1 implique

$$0\notin N, \quad K=P\cup\{0\}\cup N \quad \text{et} \quad P\cap N=\emptyset.$$

Pour vérifier que $P\cap N=\emptyset$, supposons $a\in P\cap N$; alors $a\in N$ implique $-a\in P$ et d'après la condition iii),

$$(a,-a)\in P\times P \Longrightarrow a+(-a)=0\in P,$$

ce qui contredit la condition i).

La propriété 1) de la Prop. A.2 implique alors,

$$(a\in P \iff 0<a) \quad \text{et} \quad (a\in N \iff a<0).$$

N est appelé l'**ensemble des éléments négatifs** de K.

Corollaire A.4. *K étant un corps ordonné, on a*

a) $\big((a,b)\in P\times N\Longrightarrow ab\in N\big)$ *et* $\big((a,b)\in N\times N\Longrightarrow ab\in P\big)$.

b) P est un sous-groupe du groupe multiplicatif K^*.

Démonstration. a) Le 3) de la Prop. A.2 donne

$$(b<0 \quad \text{et} \quad 0<a) \Longrightarrow ba=ab<0.$$

D'autre part,

$$(a<0,\ b<0) \Longrightarrow (0<-a,\ 0<-b) \Longrightarrow 0<(-a)(-b)=ab.$$

b) D'après la Déf. A.1, P est un sous-ensemble non vide de K^*, fermé pour la multiplication de K.

Le 4) de la Prop. A.2 montre que $1\in P$; de plus, tout élément a de P est non nul, donc inversible dans K et

$$(a\in P,\ aa^{-1}=1\in P) \Longrightarrow a^{-1}\in P,$$

d'après le résultat a) du Cor. A.4. □

Exemple A.5. Le corps $\mathbb{Q}$ des nombres rationnels est un *corps ordonné* par la relation d'ordre induite par l'ordre de $\mathbb{Z}$. En effet, $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$ et la partie P de $\mathbb{Q}$ telle que

$$P:=\{\frac{a}{s}\,;\,as>0, \text{ dans } \mathbb{Z}\}$$

répond aux trois conditions de la Déf. A.1.

Notation : On pourra désigner par (K,P), un corps ordonné K, dont l'ensemble des éléments positifs est P.

Remarque A.6. a) Etant donné un corps ordonné (K,P), si $K'\subseteq K$ est un sous-corps de K et si l'on pose $P':=K'\cap P$, alors (K',P') est un corps ordonné (à vérifier).

La relation d'ordre ainsi définie sur K' est dite *induite* par celle de K.

b) Deux corps ordonnés (K,P) et (K',P') sont des *corps ordonnés isomorphes* s'il existe un isomorphisme λ de K sur K' tel que $\lambda(P)\subseteq P'$.

S'il en est ainsi, on a $\lambda(0)=0$ et $\lambda(N)\subseteq N'$, ce qui entraîne $P'=\lambda(P)$ et $N'=\lambda(N)$.

Théorème A.7. $\mathbb{R}$ *est un corps ordonné.*

Démonstration. On suppose connue la construction du corps $\mathbb{R}$ des nombres réels, à partir de l'anneau $\mathcal{C}$ des suites de Cauchy de $\mathbb{Q}$ (Cf. Ex. **8.**, Ch. 1, ou [4]).
On rappelle que, dans l'anneau $\mathcal{C}$, l'ensemble $\mathcal{C}_0$ des suites qui convergent vers 0, est un idéal maximal et $\mathbb{R} = \mathcal{C}/\mathcal{C}_0$.
On définit dans $\mathcal{C}$, les parties $\mathcal{C}_+$ et $\mathcal{C}_-$ telles que pour $u = (u_n)_{n\in\mathbb{N}} \in \mathcal{C}$:

$$u \in \mathcal{C}_+ \iff \forall \varepsilon \in \mathbb{Q}_+^*, \exists n_\varepsilon \in \mathbb{N}, t.q.\ (n > n_\varepsilon \Longrightarrow u_n > -\varepsilon);$$
$$u \in \mathcal{C}_- \iff \forall \varepsilon \in \mathbb{Q}_+^*, \exists n_\varepsilon \in \mathbb{N}, t.q.\ (n > n_\varepsilon \Longrightarrow u_n < \varepsilon).$$

Or, $u \in \mathcal{C}_0 \iff \forall \varepsilon \in \mathbb{Q}_+^*, \exists n_\varepsilon \in \mathbb{N}, t.q.\ (n > n_\varepsilon \Longrightarrow -\varepsilon < u_n < \varepsilon)$,

d'où, $\mathcal{C} = \mathcal{C}_+ \cup \mathcal{C}_-$ et $\mathcal{C}_+ \cap \mathcal{C}_- = \mathcal{C}_0$.

On pose $\mathcal{C}_+^* := \mathcal{C}_+ \setminus \mathcal{C}_0$ et $\mathcal{C}_-^* := \mathcal{C}_- \setminus \mathcal{C}_0$.

Dans $\mathbb{R} = \mathcal{C}/\mathcal{C}_0 = \{x := \overline{u}\ ;\ u \in \mathcal{C}\}$, on dira que
$x = \overline{u}$ est **positif**, si $u \in \mathcal{C}_+^*$; on écrira $0 < x$;
$x = \overline{u}$ est **négatif**, si $u \in \mathcal{C}_-^*$; on écrira $x < 0$.
D'autre part, on sait que $x = 0$ si et seulement si $x = \overline{u}$, où $u \in \mathcal{C}_0$.
On note $\mathbb{R}_+^*$ (resp. $\mathbb{R}_-^*$) l'ensemble des éléments *positifs* (resp. *négatifs*) de $\mathbb{R}$ et on montre que la partie $P := \mathbb{R}_+^*$ de $\mathbb{R}$ satisfait aux conditions de la Déf. A.1. (à vérifier par le lecteur).
On en conclut que $\mathbb{R}$ est un *corps ordonné* par la relation d'ordre telle que, pour x et y dans $\mathbb{R}$:

$$x \leq y \iff x = y \quad \text{ou} \quad y - x \in \mathbb{R}_+^*. \tag{A.2}$$

On pose alors, $\mathbb{R}_+ := \mathbb{R}_+^* \cup \{0\}$ et $\mathbb{R}_- := \mathbb{R}_-^* \cup \{0\}$. □

Remarque A.8. a) L'ordre « naturel » défini sur $\mathbb{Q}$ (Exemple A.5) correspond à l'ordre *induit* sur $\mathbb{Q}$ par celui de $\mathbb{R}$, puisque $\mathbb{Q}_+^* = \mathbb{R}_+^* \cap \mathbb{Q}$.

b) Le corps $\mathbb{C}$ des nombres complexes *n'est pas un corps ordonné.*

En effet, si $\mathbb{C}$ était un corps ordonné, il existerait une partie non vide P de $\mathbb{C}$ vérifiant les conditions de la Déf. A.1 et les propriétés de la Prop. A.2. Mais, le 4) de la Prop. A.2 impliquerait, à la fois

$$1 = 1^2 \in P \text{ et } -1 = i^2 \in P,$$

d'où une contradiction.
Cependant, comme tout ensemble non vide peut être ordonné ([8]), il est possible de munir l'ensemble des nombres complexes d'une relation d'ordre, mais celle-ci ne vérifiera pas les conditions de la Déf. A.1.
Par exemple, on peut vérifier que la relation binaire $\leq$ définie dans le corps
$\mathbb{C} = \{a + ib\ ;\ (a,b) \in \mathbb{R} \times \mathbb{R}\}$, par

$$a + ib \leq a' + ib' \iff (a \leq a' \text{ et } b \leq b', \text{ dans } \mathbb{R}).$$

est une relation d'ordre dans l'ensemble $\mathbb{C}$.

Moyennant le « *Théorème de la valeur intermédiaire* » (supposé connu, ([4]) nous pouvons démontrer la propriété suivante.

Théorème A.9. *Quel que soit l'entier $n > 0$, tout nombre réel $a \geq 0$ a une racine $n^{ème}$ dans $\mathbb{R}_+$.*

Démonstration. Pour tout $a \geq 0$ dans $\mathbb{R}$, la fonction polynômiale

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^n - a \end{aligned} \qquad \text{est continue.}$$

Si $a = 0$, $0^n = 0$, donc le théorème est vérifié.
Si $a > 0$, on a $f(0) = -a < 0$ et $f(a+1) = (a+1)^n - a > 0$.
On en déduit, d'après le Théorème de la valeur intermédiaire, qu'il existe $\alpha \in \mathbb{R}$ tel que

$$0 < \alpha < 1 + a \quad \text{et} \quad f(\alpha) = 0,$$

donc $\alpha > 0$ et $\alpha^n = a$. □

Corollaire A.10. *Tout nombre réel positif, a, a une unique racine carrée réelle positive.*

Démonstration. En effet, d'après le Th. A.9, quel que soit $a > 0$ dans $\mathbb{R}$, il existe $\alpha > 0$, dans $\mathbb{R}$ tel que $\alpha^2 = a$. Or,

$$\alpha > 0 \Longrightarrow -\alpha < 0 \text{ et } (-\alpha)^2 = \alpha^2 = a.$$

L'équation $X^2 - a = 0$ ayant au plus 2 racines dans $\mathbb{R}$ ([13], Th. 4.39), la racine carrée positive α de $a > 0$ est unique, l'autre racine étant $-\alpha < 0$.
Si $a > 0$ dans $\mathbb{R}$, on note $\sqrt{a}$ la racine carrée positive de a. □

Théorème A.11. *Il existe une* unique *relation d'ordre sur le corps* $\mathbb{R}$, *qui lui confère une structure de corps ordonné.*

Démonstration. D'après le Th. A.7, $\mathbb{R}$ est un corps ordonné dont la partie positive est $\mathbb{R}_+^*$. Supposons qu'il existe une partie P de $\mathbb{R}$ telle que $(\mathbb{R}, P)$ soit aussi un corps ordonné. D'après le Cor. A.10,

$$\forall a \in \mathbb{R}_+^*, \ \exists! \, \alpha \in \mathbb{R}_+^*, \quad t.q. \ a = \alpha^2$$

et d'après la Prop. A.2, dans le corps ordonné $(\mathbb{R}, P)$,

$$a = \alpha^2 \Longrightarrow a \in P, \quad \text{d'où} \quad \mathbb{R}_+^* \subseteq P.$$

On en déduit que $\mathbb{R}_+^* = P$ (Rem. A.6, b)). □

2. Corps valués

Définition A.12. (Rappel) Pour tout $x \in \mathbb{R}$, on pose

$$| x | = max\{x, -x\}. \tag{A.3}$$

$| x |$ est la valeur absolue de x dans le corps ordonné $\mathbb{R}$ et on a, quels que soient les nombres réels x, y,

1) $| x | = x \iff x \geq 0; \quad | x | = -x \iff x \leq 0.$
2) $| xy | = | x | \, | y |$.
3) $| x + y | \leq | x | + | y |$ (Inégalité triangulaire).

Cette valeur absolue, dans le corps ordonné $\mathbb{R}$, permet de définir une notion de *valeur absolue* dans un corps quelconque.

Définition A.13. On appelle **valeur absolue** sur un corps K, toute application, que l'on notera $| \ |$, telle que

$$|\ |: K \longrightarrow \mathbb{R}_+$$

et, quels que soient x, y dans K,

$$i)\ |0|=0;\quad x\neq 0 \Longleftrightarrow |x|>0; \tag{A.4}$$

$$ii)\ |xy|=|x||y|; \tag{A.5}$$

$$iii)\ |x+y|\leq |x|+|y|\,. \tag{A.6}$$

Remarque A.14. L'ensemble $\{|x|\,;\, x\in K^*\}$ forme un sous-groupe du groupe multiplicatif $\mathbb{R}_+^*$.

Définition A.15. Si un corps K est muni d'une valeur absolue $|\ |$, on dira que le couple $(K,|\ |)$ est un **corps valué**.

Exemple A.16. 1) Les corps $\mathbb{Q}$ et $\mathbb{R}$ sont respectivement munis de la valeur absolue (dite « *ordinaire* ») définie par la relation (A.3).

2) Le corps $\mathbb{C}$ est muni de la valeur absolue (dite « *ordinaire* ») telle que, quel que soit $a+ib$ dans $\mathbb{C}$,

$$|a+ib|=\sqrt{a^2+b^2}$$

($|a+ib|$ est le *module* du nombre complexe $a+ib$).
Cet exemple montre qu'un corps *valué* n'est pas nécessairement un corps *ordonné*.

Notation : La valeur absolue *ordinaire* de $\mathbb{Q},\mathbb{R}$ ou $\mathbb{C}$ est généralement notée $|\ |_\infty$.

3) Sur tout corps K, on peut considérer ce qu'on appelle la **valeur absolue triviale**, notée $|\ |_0$ et définie par

$$|0|_0=0 \quad \text{et} \quad \forall x\in K^*,\ |x|_0=1.$$

4) **Valeurs absolues p-adiques** sur $\mathbb{Q}$.
On note $\mathcal{P}$ l'ensemble des nombres premiers (c'est-à-dire des éléments premiers, positifs de $\mathbb{Z}$ [13], App. A).
Soit p fixé dans $\mathcal{P}$; $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$, par suite, la notion de *valuation p-adique* de $\mathbb{Z}$, ([13], App. A, Déf. 0.15) induit, de façon naturelle, la notion de *valuation p-adique* de $\mathbb{Q}$.
Soit $x\in\mathbb{Q}^*$; supposons $x=\dfrac{a}{s}$, a, s non nuls dans $\mathbb{Z}$.
Soit w_p la valuation p-adique de $\mathbb{Z}$; on peut écrire, de façon unique

$$a=\prod_{p\in\mathcal{P}} p^{w_p(a)},\quad s=\prod_{p\in\mathcal{P}} p^{w_p(s)},$$

où seuls un nombre fini de $w_p(a)$ et $w_p(s)$ sont non nuls dans $\mathbb{N}$. On en déduit que

$$x=\frac{a}{s}=\prod_{p\in\mathcal{P}} p^{w_p(a)-w_p(s)}.$$

En posant, dans la relation précédente, pour tout $p\in\mathcal{P}$,

$$v_p(x)=w_p(a)-w_p(s),$$

on obtient, de façon unique,

$$x=\prod_{p\in\mathcal{P}} p^{v_p(x)}, \tag{A.7}$$

où, seuls un nombre fini de $v_p(x)$ sont non nuls dans $\mathbb{Z}$.
Par convention, on pose $v_p(0):=\infty$, quel que soit le nombre premier p.

Définition A.17. L'application $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$, associée, d'après ce qui précède, à tout $p \in \mathcal{P}$, est appelée **valuation p-adique** de $\mathbb{Q}$.

On vérifie facilement les propriétés suivantes ;

Proposition A.18.

$$1)\, v_p(x) = \infty \iff x = 0. \tag{A.8}$$
$$2)\, v_p(xy) = v_p(x) + v_p(y),\ \forall (x,y) \in \mathbb{Q}^* \times \mathbb{Q}^*. \tag{A.9}$$
$$3)\, v_p(x+y) \geq min\{v_p(x), v_p(y)\},\ \forall (x,y) \in \mathbb{Q}^* \times \mathbb{Q}^*. \tag{A.10}$$

Définition A.19. Pour p donné dans $\mathcal{P}$, on dit que $x \in \mathbb{Q}$ est un **p-entier** , si $v_p(x) \geq 0$.

Remarque A.20.

$$x \in \mathbb{Z} \iff x \text{ est un } p\text{-entier}, \forall p \in \mathcal{P}.$$

On rappelle que

$$x \mid y \text{ dans } \mathbb{Z}^* \iff v_p(x) \leq v_p(y), \forall p \in \mathcal{P}.$$

Etant donné $p \in \mathcal{P}$ et un nombre réel γ tel que $0 < \gamma < 1$, on pose

$$\forall x \in \mathbb{Q}^*,\ |x|_p := \gamma^{v_p(x)} \quad \text{et} \quad |0|_p = 0. \tag{A.11}$$

Proposition A.21. *Pour tout $p \in \mathcal{P}$, l'application $|\ |_p : \mathbb{Q} \longrightarrow \mathbb{R}_+$ définie par les relations (A.11) satisfait aux propriétés suivantes :*

i) $|0|_p = 0;\quad x \neq 0 \iff |x|_p > 0;$
ii) $|xy|_p = |x|_p |y|_p;$
iii) $|x+y|_p \leq max\left(|x|_p, |y|_p\right) \leq |x|_p + |y|_p,$

donc définit une valeur absolue *de* $\mathbb{Q}$.

Démonstration. laissée au lecteur. □

Définition A.22. Quels que soient le nombre premier p et le nombre réel $\gamma (0 < \gamma < 1)$, on dit que l'application $|\ |_p$, définie par (A.11), est une **valeur absolue p-adique** de $\mathbb{Q}$. Dans le cas particulier où $\gamma = \frac{1}{p}$, la valeur absolue $|\ |_p$ est appelée **valeur absolue p-adique normalisée** de $\mathbb{Q}$. On a alors

$$\forall x \in \mathbb{Q}^*,\ |x|_p = p^{-v_p(x)}. \tag{A.12}$$

Remarque A.23. a) Compte tenu de la définition A.19, si $|\ |_p$ désigne la valeur absolue p-adique normalisée de $\mathbb{Q}$, alors pour $x \in \mathbb{Q}$, on a

$$x \text{ est un } p\text{-entier} \iff 0 \leq |x|_p \leq 1.$$
$$x \in \mathbb{Z} \iff 0 \leq |x|_p \leq 1,\ \forall p \in \mathcal{P}.$$

b) L'inégalité iii) vérifiée par une valeur absolue p-adique :

$$|x+y|_p \leq max\left(|x|_p, |y|_p\right),$$

est appelée : **inégalité ultramétrique** (elle entraîne *l'inégalité triangulaire*).

Définition A.24. On dit que des **corps valués** $(K, |\ |)$ et $(K', |\ |')$ sont **isomorphes**, s'il existe un isomorphisme $\lambda : K \longrightarrow K'$ tel que

$$|\lambda(x)|' = |x|,\ \forall x \in K.$$

Remarque A.25. $(K, |\ |)$ étant un corps valué, si K' est un sous-corps de K, alors la restriction de la valeur absolue $|\ |$ à K' définit une valeur absolue de K'.
Ainsi, les restrictions à $\mathbb{Q}$ et $\mathbb{R}$ de la valeur absolue ordinaire de $\mathbb{C}$ sont les valeurs absolues ordinaires de $\mathbb{Q}$ et $\mathbb{R}$.

Définition A.26. On dit qu'un corps valué $(K, |\ |)$ est **non-archimédien** (ou que sa valeur absolue est **non-archimédienne**) , si

$$\forall n \in \mathbb{Z}, \quad |n1_K| \leq 1, \quad 1_K \text{ désignant l'élément unité de } K.$$

Dans le cas contraire :

$$\exists n \in \mathbb{Z}, \quad \text{tel que} \quad |n1_K| > 1,$$

on dit que le corps valué $(K, |\ |)$ est **archimédien** (ou que sa valeur absolue est **archimédienne**).

Exemple A.27. 1) Les valeurs absolues *ordinaires* définies sur $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, sont *archimédiennes.*
2) Sur tout corps K, la valeur absolue *triviale* (Exemple A.16, 3)) est *non-archimédienne.*
3) Pour tout $p \in \mathcal{P}$, toute valeur absolue p-adique de $\mathbb{Q}$ est *non-archimédienne* (Rem. A.23).

Remarque A.28. a) *Un corps fini n'a pas d'autre valeur absolue que la valeur absolue triviale.*
En effet, soit $(K, |\ |)$ un corps valué fini ; si $car K = p$ et $card K = p^n$, alors, $|0| = 0$ et pour $x \in K^*$,

$$x^{p^n-1} = 1_K \Longrightarrow |x^{p^n-1}| = |x|^{p^n-1} = 1,$$

d'où $|x| = 1$, quel que soit $x \in K^*$.
La valeur absolue de K est donc non-archimédienne.

b) Si $(K, |\ |)$ est un corps valué archimédien (resp. non-archimédien) et K' est un sous-corps de K, alors, $|\ |'$ désignant la restriction de $|\ |$ à K', le corps valué $(K', |\ |')$ est archimédien (resp. non-archimédien).
Cette remarque s'applique, en particulier, lorsque K' est le *sous-corps premier* de K (Déf. 1.3). Par suite, la remarque a) précédente implique la propriété suivante :
Tout corps valué, de caractéristique $p \neq 0$, est non-archimédien.

c) Un corps valué $(K, |\ |)$, de caractéristique 0, peut être archimédien ou non-archimédien, suivant le choix de la valeur absolue $|\ |$.
On a vu, par exemple, que le corps valué $(\mathbb{Q}, |\ |_\infty)$, où $|\ |_\infty$ désigne la valeur absolue *ordinaire* de $\mathbb{Q}$, est archimédien ; par contre, quel que soit le nombre premier p, le corps valué $(\mathbb{Q}, |\ |_p)$ est non-archimédien.

Proposition A.29. *Dans $(\mathbb{R}, |\ |)$, où $|\ |$ est la valeur absolue ordinaire, la condition archimédienne est équivalente à*

$$\forall (a,b) \in \mathbb{R}_+^* \times \mathbb{R}_+, \ \exists N \in \mathbb{N}^* \ ; \ Na > b. \tag{A.13}$$

Démonstration. Supposons la condition (A.13) vérifiée. En prenant $a = b = 1$ dans $\mathbb{R}$ et $N > 1$ dans $\mathbb{Z}$, on obtient $|N1| > 1$, d'où la condition archimédienne dans $(\mathbb{R}, |\ |)$.
Réciproquement, la valeur absolue *ordinaire* de $\mathbb{R}$ étant archimédienne, montrons que la condition (A.13) est vérifiée.
Soit $a > 0$ et $b \geq 0$ dans $\mathbb{R}$.

Si $b = 0$, alors la relation (A.13) est vérifiée pour tout $N > 1$, dans $\mathbb{N}$.
Si $a \geq b > 0$, quel que soit $N > 1$ dans $\mathbb{N}$, on a

$$Na \geq Nb > b, \quad \text{d'où la condition (A.13).}$$

Si $0 < a < b$, on considère ba^{-1} dans $\mathbb{R} = \mathcal{C}/\mathcal{C}_0$ (voir la construction de $\mathbb{R}$, Ex. **8.**, Ch. 1).
D'après la preuve du Th. A.7.,le nombre réel $ba^{-1} > 0$ est la classe d'équivalence $\overline{u}$, d'une suite de Cauchy $u = (u_n)_{n\in\mathbb{N}} \in \mathcal{C}_+^*$.
Or, toute suite de Cauchy de $\mathbb{Q}$ est bornée (Ex. **8**, Ch. 1), donc il existe $N \in \mathbb{Q}^*$ (et on peut supposer $N \in \mathbb{N}^*$) tel que $\forall n \in \mathbb{N}$, $u_n < N$.
En considérant N comme la limite d'une suite constante de $\mathbb{Q}$, on a alors, $\overline{u} < N$, d'où

$$ba^{-1} < N \Longrightarrow b < Na. \qquad \square$$

Proposition A.30. *Pour une valeur absolue $|\ |$ d'un corps K, les conditions suivantes sont équivalentes :*
1) $|\ |$ *est non-archimédienne.*
2) $|\ |$ *vérifie l'inégalité* ultramétrique (Rem. A.23).
3) *Pour tout $r \in \mathbb{R}_+^*$, l'application $|\ |^r$ de K dans $\mathbb{R}_+$ est une valeur absolue de K.*

Démonstration. 1) $\Longrightarrow$ 2) : L'hypothèse implique que quels que soient $x \in K$ et $m \in \mathbb{Z}$,

$$|mx| = |m1_K x| = |m1_K|\,|x| \leq |x|. \tag{A.14}$$

De (A.14), on déduit que, quels que soient $n > 0$ dans $\mathbb{Z}$ et x, y dans K,

$$\begin{aligned} |x+y|^n &= |x^n + C_n^1 x^{n-1}y + \cdots + y^n| \\ &\leq |x|^n + |x|^{n-1}|y| + \cdots + |y|^n \\ &\leq (n+1)max(|x|^n, |y|^n) = (n+1)\big(max(|x|, |y|)\big)^n. \end{aligned}$$

En prenant, dans $\mathbb{R}_+$, les racines $n^{èmes}$ de chacun des deux membres de l'inéquation précédente (Th. A.9), on obtient

$$\frac{1}{\sqrt[n]{n+1}}\,|x+y| \leq max(|x|, |y|);$$

$$\text{alors,} \quad \Big(\lim_{n\longrightarrow\infty} \frac{1}{\sqrt[n]{n+1}} = 1\Big) \Longrightarrow |x+y| \leq max(|x|, |y|).$$

2) $\Longrightarrow$ 3) : Pour tout $x \in K$ et tout nombre réel $r > 0$, on a $|x|^r \geq 0$ et $|x|^r = 0 \Longleftrightarrow x = 0$.
De plus, quels que soient x, y dans K et $r \in \mathbb{R}_+^*$,

$$|x+y|^r \leq \big(max(|x|, |y|)\big)^r = max(|x|^r, |y|^r) \leq |x|^r + |y|^r.$$

3) $\Longrightarrow$ 1) : $|\ |_\infty$ désignant la valeur absolue ordinaire dans $\mathbb{R}$, pour tout $n \in \mathbb{Z}^*$, on a $|n|_\infty = \pm n > 0$.
L'hypothèse entraîne que pour tout nombre réel $r > 0$ et tout $n \in \mathbb{Z}^*$, pour lequel on pose $n' := |n|_\infty$, on a

$$|n1_K|^r = |n'1_K|^r \leq n'\,|1_K|^r \leq n';$$

$$\text{alors,} \quad |n1_K|^r \leq n' \Longrightarrow |n1_k| \leq \lim_{r\longrightarrow\infty} (n')^{\frac{1}{r}} = 1.$$

Ainsi, $|\ |$ est une valeur absolue non-archimédienne de K. $\square$

Définition A.31. Deux valeurs absolues $|\ |$ et $|\ |'$ d'un corps K sont dites **équivalentes**, s'il existe $r \in \mathbb{R}_+^*$ tel que $|\ |' = |\ |^r$.

Remarque A.32. Si $(K, |\ |)$ est un corps valué et si $r > 0$ dans $\mathbb{R}$, alors $|\ |^r$ n'est pas nécessairement une valeur absolue de K.
Par exemple, si $|\ |$ désigne la valeur absolue ordinaire de $\mathbb{Q}$, alors

$$|1+1|^2 = 4 \quad \text{et} \quad |1|^2 + |1|^2 = 2,$$

donc $|\ |^2$ n'est pas une valeur absolue sur $\mathbb{Q}$.

Proposition A.33. *Soit $\{x_1, x_2, \ldots, x_n\}$, $n \geq 2$, des éléments non nuls d'un corps valué, non-archimédien $(K, |\ |)$; alors*

$$(|x_i| < |x_1|, \forall i, 2 \leq i \leq n) \Longrightarrow |x_1 + x_2 + \cdots + x_n| = |x_1|. \tag{A.15}$$

Démonstration. L'inégalité ultramétrique implique

$$|x_1 + x_2 + \cdots + x_n| \leq max(|x_i|,\ 1 \leq i \leq n) = |x_1|;$$
$$|x_2 + \cdots + x_n| \leq max(|x_i|,\ 2 \leq i \leq n) < |x_1|.$$

Si l'on avait $|x_1 + x_2 + \cdots + x_n| < |x_1|$; on aurait alors

$$|x_1| = |(x_1 + x_2 + \cdots + x_n) - (x_2 + \cdots + x_n)|$$
$$\leq max(|x_1 + x_2 + \cdots + x_n|, |x_2 + \cdots + x_n|) < |x_1|;$$

d'où une contradiction, dont on déduit l'égalité (A.15).
On remarque que la relation (A.15), appliquée dans le cas de deux éléments x et y, donne

$$|x| < |y| \Longrightarrow |x+y| = |y|. \qquad \square$$

Proposition A.34. *Toute valeur absolue non-archimédienne, non triviale, de $\mathbb{Q}$ est une valeur absolue p-adique, pour un certain nombre premier p.*

Démonstration. Soit $|\ |$ une valeur absolue non-archimédienne de $\mathbb{Q}$, que l'on suppose non triviale ; on a alors

$$M = \{m \in \mathbb{Z}\ ;\ |m| < 1\} \neq \{0\}.$$

Montrons que M est un idéal de $\mathbb{Z}$.
On a $0 \in M$; d'après la Prop. A.30, $|\ |$ vérifie l'inégalité ultramétrique, d'où, pour m et m' dans M,

$$|m + m'| \leq max(|m|, |m'|) < 1.$$

D'autre part, $m \in M$ implique $-m \in M$; enfin, $|\ |$ étant non-archimédienne, on a, quels que soient $n \in \mathbb{Z}$ et $m \in M$,

$$|nm| = |n|\,|m| < 1,$$

d'où $nm \in M$.
De plus, M est un idéal premier de $\mathbb{Z}$, car pour des entiers n et n'

$$(|n| = 1 \text{ et } |n'| = 1) \Longrightarrow |nn'| = 1 \text{ donc } (n \notin M \text{ et } n' \notin M) \Longrightarrow nn' \notin M.$$

On en conclut qu'il existe un *nombre premier p* tel que $M = p\mathbb{Z}$ et $0 < |p| < 1$; posons $\gamma = |p|$.
Pour tout $x \in \mathbb{Q}$, il existe a, b, k dans $\mathbb{Z}$ tels que $x = \dfrac{a}{b} p^k$, où

$$a \wedge p = 1 = b \wedge p \quad \text{et} \quad k = v_p(x) \text{ (valuation } p\text{-adique de } x).$$
$$a \notin p\mathbb{Z},\ b \notin p\mathbb{Z} \Longrightarrow |a| = 1 = |b|.$$

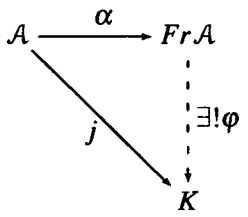
On en déduit que $|x| = \gamma^{v_p(x)}$, où $0 < \gamma = |p| < 1$ dans $\mathbb{R}$, donc $|\ |$ est une valeur absolue p-adique sur $\mathbb{Q}$ (Déf. A.22). $\square$

Théorème A.35. *Soit* $(K, |\ |)$ *un corps valué* non-archimédien ($|\ |$ *non triviale*), *alors*
1) $\mathcal{A} := \{x \in K\ ;\ |x| \leq 1\}$ *est un domaine d'intégrité* ([13], Déf. 1.21).
$\mathcal{A}$ *est appelé* l'anneau des **entiers** du corps valué $(K, |\ |)$.
2) $\mathcal{M} := \{x \in K\ ;\ |x| < 1\}$ *est l'unique idéal maximal de* $\mathcal{A}$, *donc* $\mathcal{A}$ *est un anneau* local ([13], Déf. 2.73)
Le groupe multiplicatif des éléments inversibles de $\mathcal{A}$ *est alors*
$\mathcal{U} := \mathcal{A} \setminus \mathcal{M}$.
On dit que $\mathcal{F} := \mathcal{A}/\mathcal{M}$ *est le* **corps résiduel** du corps valué $(K, |\ |)$.
3) K *est le corps des fractions du domaine d'intégrité* $\mathcal{A}$.

Démonstration. 1) On vérifie que $\mathcal{A}$ est un sous-anneau du corps K, c'est donc un domaine d'intégrité ([13], Ch. 5).
2) On montre facilement que $\mathcal{M}$ est un idéal de $\mathcal{A}$ et pour prouver que c'est l'*unique idéal maximal* de $\mathcal{A}$, il suffit de vérifier que $\mathcal{M}$ est l'ensemble des éléments *non inversibles* de $\mathcal{A}$ ([13], Th. 2.77). Or, pour $x \in \mathcal{A}$, on a

$$x \text{ inversible} \iff |x| = 1, \quad \text{d'où} \quad x \text{ non inversible} \iff x \in \mathcal{M}.$$

3) Soit α l'injection canonique de $\mathcal{A}$ dans son corps de fractions $Fr\mathcal{A}$ et j l'injection de $\mathcal{A}$ dans K.
La propriété universelle du couple $(Fr\mathcal{A}, \alpha)$ ([13], Th. 5.5.) entraîne l'existence d'un unique morphisme φ de $Fr\mathcal{A}$ dans K tel que le diagramme suivant commute



et $\forall \frac{x}{y} \in Fr\mathcal{A},\ \varphi(\frac{x}{y}) = j(x)(j(y))^{-1} = xy^{-1}$ ([13], Th. 5.5).
On sait que le morphisme φ est injectif, vérifions qu'il est surjectif. Soit $z \neq 0$, dans K; alors

$$|z| \leq 1 \Longrightarrow z \in \mathcal{A} \Longrightarrow \varphi(z) = z;$$
$$|z| > 1 \Longrightarrow z^{-1} \in \mathcal{A}^* \Longrightarrow \varphi(\frac{1}{z^{-1}}) = z.$$

Ainsi φ est un isomorphisme. Or, le corps $Fr\mathcal{A}$ est défini à un isomophisme près ([13], Rem. 5.8), d'où le résultat énoncé. □

Exemple A.36. Dans le cas du corps valué non archimédien $(\mathbb{Q}, |\ |_p)$, posons

$$\mathcal{A}_p := \{x \in \mathbb{Q}\ ;\ |x|_p \leq 1\} = \{x \in \mathbb{Q}\ ;\ v_p(x) \geq 0\};$$
$$\mathcal{M}_p := \{x \in \mathbb{Q}\ ;\ |x|_p < 1\} = \{x \in \mathbb{Q}\ ;\ v_p(x) > 0\};$$
$$\mathcal{U}_p := \mathcal{A}_p \setminus \mathcal{M}_p = \{\frac{a}{s} \in \mathbb{Q}^*\ ;\ p \nmid a, p \nmid s\}.$$

On a $\mathbb{Z} \subset \mathcal{A}_p$ et $\mathcal{M}_p = p\mathcal{A}_p$. Tout $x \in \mathcal{A}_p \setminus \{0\}$ s'écrit de façon unique,

$$x = \frac{a}{s} p^{v_p(x)}, \quad \text{où} \quad \frac{a}{s} \in \mathcal{U}_p,\ v_p(x) > 0 \text{ et } a \wedge s = 1, \text{ donc}$$
$$x = u p^{v_p(x)}, \quad \text{où} \quad u \in \mathcal{U}_p.$$

On en déduit que les idéaux non nuls de $\mathcal{A}_p$ sont les $p^k\mathcal{A}_p$, $k \in \mathbb{N}$, donc l'anneau local $\mathcal{A}_p$

est principal.
Les éléments non nuls du corps $\mathcal{F}_p = \mathcal{A}_p/\mathcal{M}_p$, sont les classes d'équivalence, modulo $\mathcal{M}_p$, des éléments u de $\mathcal{U}_p$, notées $\overline{u}$. Si $u = \dfrac{a}{s} \in \mathcal{U}_p$, alors $p \nmid a$ et $p \nmid s$ impliquent que les classes d'équivalence des entiers a et s modulo p, notées $\overline{a}, \overline{s}$, sont des éléments non nuls, donc inversibles, du corps $\mathbb{Z}/p\mathbb{Z}$. Par suite, $\overline{u}$ peut être identifié à l'élément non nul $\overline{a}\overline{s}^{-1}$ de $\mathbb{Z}/p\mathbb{Z}$.
On en conclut que le corps résiduel, $\mathcal{F}_p$, du corps valué $(\mathbb{Q}, |\ |_p)$ s'identifie à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

3. Topologie d'un corps valué

Etant donné un corps valué $(K, |\ |)$, l'application

$$\begin{aligned} d : K \times K &\longrightarrow \mathbb{R}_+ \\ (x,y) &\longmapsto |x-y| \end{aligned}$$

est une **distance** sur K ([19]) ; en effet, on vérifie facilement, que

$$\begin{aligned} &i)\ d(x,y) = 0 \iff x = y; \\ &ii)\ d(y,x) = d(x,y),\ \forall x,y \text{ dans } K; \\ &iii)\ d(x,y) \leq d(x,z) + d(z,y),\ \forall x,y,z \text{ dans } K. \end{aligned}$$

Ainsi tout corps valué $(K, |\ |)$ est un **espace métrique** relativement à la distance d associée à la valeur absolue $|\ |$, donc K est muni de la **topologie** définie par d, qui sera dite induite par $|\ |$ ([19]). Les applications

$$\begin{array}{ll} K \times K \longrightarrow K & K \longrightarrow K \\ (x,y) \longmapsto x+y & x \longmapsto -x \\ (x,y) \longmapsto xy & x \longmapsto x^{-1},\ \text{si } x \neq 0, \end{array}$$

sont *continues* et la relation

$$||x| - |y|| \leq |x-y|$$

implique que l'application $x \longrightarrow |x|$ de K dans $\mathbb{R}_+$ est *uniformément continue* ; donc l'espace métrique (K,d) est un espace topologique *uniforme* ([19]).

Remarque A.37. Si λ est un isomorphisme de corps valués de $(K, |\ |)$ sur $(K', |\ |')$ (Déf. A.24.) et si d et d' sont les distances, respectivement associées aux valeurs absolues de K et K', alors quels que soient x et y dans K,

$$|\lambda(x-y)|' = |x-y| \Longrightarrow d'(\lambda(x), \lambda(y)) = d(x,y).$$

Par suite λ est une **isométrie** de (K,d) sur (K',d').

Rappel ([19]) : Une partie A d'un espace topologique E est *dense* dans E, si toute partie ouverte non vide de E rencontre A.

Théorème A.38. *$\mathbb{Q}$ est dense dans $\mathbb{R}$.*

Démonstration. Toute partie ouverte non vide de $\mathbb{R}$ contient un intervalle ouvert ; il suffit donc de montrer que quels que soient a,b dans $\mathbb{R}^*$ tels que $a < b$, il existe au moins un élément $q \in \mathbb{Q}$ tel que $a < q < b$.

Si $a < 0 < b$, on prend $q = 0$. Supposons $0 < a < b$; $(\mathbb{R}, |\ |_\infty)$ étant archimédien, il existe $n \in \mathbb{N}^*$ tel que $n(b-a) > 1$ (Prop. A.29) ; étant donné un tel entier n, on a $b - a > \frac{1}{n}$. Posons

$$E := \{k \in \mathbb{N}^* \ ; \ \frac{k}{n} \geq b\} \ ; E \text{ est une partie non vide de } \mathbb{N}^*.$$

Notons m le plus petit élément de E ; alors,

$$\frac{m}{n} \geq b \quad \text{et} \quad \frac{m-1}{n} < b.$$

$$\left(\frac{m}{n} - \frac{1}{n} > \frac{m}{n} - (b-a)\right) \Longrightarrow \frac{m-1}{n} > b - (b-a) = a.$$

En posant $q = \frac{m-1}{n}$, on obtient $a < q < b$.

Dans le cas où $a < b < 0$, on a $0 < -b < -a$, donc, d'après ce qui précède, il existe $q' \in \mathbb{Q}$ tel que $-b < q' < -a$; en posant $q := -q'$, on obtient $a < q < b$. □

On rappelle qu'un espace métrique E est dit **complet** si toute suite de Cauchy de E est convergente dans E ([19]).

Théorème A.39. *Le corps valué* $(\mathbb{R}, |\ |_\infty)$ *est un espace métrique* complet.

Démonstration. On note ici $|\ |$ la valeur absolue ordinaire, $|\ |_\infty$, de $\mathbb{R}$.
Soit $(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$, une suite de Cauchy de $\mathbb{R}$.

Pour tout $n \in \mathbb{N}$, $\frac{1}{2^n} \in \mathbb{Q}_+^*$ et, puisque $\mathbb{Q}$ est *dense* dans $\mathbb{R}$ (Prop. A.38), il existe $q_n \in \mathbb{Q}$ tel que

$$|\ q_n - u_n\ | \leq \frac{1}{2^n}. \tag{A.16}$$

On peut ainsi déterminer une suite $q = (q_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$; montrons que q est une suite de Cauchy dans $\mathbb{Q}$.

Soit $\varepsilon \in \mathbb{R}_+^*$; la suite $(\frac{1}{2^n})_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ converge vers 0, donc il existe $N_1 \in \mathbb{N}$ tel que

$$n \geq N_1 \Longrightarrow \frac{1}{2^n} \leq \frac{\varepsilon}{3}.$$

D'autre part, la suite $(u_n)_{n\in\mathbb{N}}$ est une suite de Cauchy de $\mathbb{R}$, alors il existe $N_2 \in \mathbb{N}$ tel que

$$(m \geq N_2,\ n \geq N_2) \Longrightarrow |\ u_m - u_n\ | \leq \frac{\varepsilon}{3}.$$

Posons $N := max\{N_1, N_2\}$; compte tenu de (A.16), la condition $m \geq N, n \geq N$ dans $\mathbb{N}$ implique

$$|\ q_m - q_n\ | \leq |\ q_m - u_m\ | + |\ u_m - u_n\ | + |\ u_n - q_n\ | \leq \varepsilon.$$

La suite de Cauchy $(q_n)_{n\in\mathbb{N}}$ définit un nombre réel $r := \lim\limits_{n\longrightarrow\infty} q_n$.

Montrons que la suite de Cauchy $(u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ converge aussi vers r. La définition de r, entraîne qu'étant donné $\varepsilon > 0$ dans $\mathbb{R}$, il existe $\nu_1 \in \mathbb{N}$ tel que

$$n \geq \nu_1 \Longrightarrow |\ q_n - r\ | \leq \frac{\varepsilon}{2}.$$

D'autre part, $\lim\limits_{n\longrightarrow\infty} \frac{1}{2^n} = 0$ implique qu'il existe $\nu_2 \in \mathbb{N}$ tel que

$$n \geq \nu_2 \Longrightarrow \frac{1}{2^n} \leq \frac{\varepsilon}{2}.$$

En posant $\nu := max\{\nu_1, \nu_2\}$, on obtient, moyennant la relation (A.16),

$$n \geq \nu \Longrightarrow |\ u_n - r\ | \leq |\ u_n - q_n\ | + |\ q_n - r\ | \leq \varepsilon,$$

d'où $\lim\limits_{n\longrightarrow\infty} u_n = r \in \mathbb{R}$. □

4. Complétion d'un corps valué - Corps p-adiques

A. Complétion d'un corps valué

Théorème A.40. *Etant donné un corps valué* $(K, |\ |)$, *il existe un corps valué* $(\hat{K}, \hat{|\ |})$ *tel que*
1) $\hat{K}$ *est une extension de* K *et* $|\ |$ *est la restriction de* $\hat{|\ |}$ *à* K.
2) K *est* dense *dans* $\hat{K}$.
3) $(\hat{K}, \hat{|\ |})$ *est un corps valué* complet.

Démonstration. (non détaillée) : On suppose la valeur absolue de K non triviale.
1) Soit $C(K)$ l'ensemble des suites de Cauchy de $(K, |\ |)$ et $C_0(K)$ l'ensemble des éléments de $C(K)$ qui convergent vers 0.
Posons $C := C(K)$ et $C_0 := C_0(K)$; on a $C_0 \subset C \subset K^{\mathbb{N}}$.
En identifiant tout élément a de K à la suite constante, dont tous les éléments sont égaux à a, on obtient l'inclusion $K \subset C$.
On vérifie que C est un sous-anneau de $K^{\mathbb{N}}$ et que C_0 est un idéal de C (voir le cas où $K = \mathbb{Q}$, Ex. **8.**, Ch. 1).
Montrons que C_0 est un idéal *maximal* de C.
Supposons qu'il existe un idéal B de C tel que $C_0 \subsetneq B \subseteq C$.
Soit $u = (u_n)_{n\in\mathbb{N}} \in B \setminus C_0$; il existe alors $\eta \in \mathbb{R}_+^*$ et $N \in \mathbb{N}$, tels que

$$n > N \text{ dans } \mathbb{N} \Longrightarrow |\ u_n\ | > \eta.$$

Considérons la suite $v = (v_n)_{n\in\mathbb{N}}$ définie par :

$$v_n = 1, \text{ si } 0 \leq n \leq N \quad \text{et} \quad v_n = u_n, \text{ si } n > N.$$

La suite $(u_n - v_n)_{n\in\mathbb{N}} \in C_0 \subsetneq B$ et la suite v est inversible dans l'anneau C ; B étant un idéal de C,

$$v^{-1}v = v^{-1}u - v^{-1}(u - v) \in B\,;$$

alors $1 \in B$ entraîne $B = C$, donc C_0 est un idéal maximal de C.
Posons $\hat{K} := C/C_0$; $\hat{K}$ est un corps ; j étant l'injection canonique de K dans C et φ la surjection canonique de C sur C/C_0, $\varphi \circ j$ est un morphisme non nul de K dans $\hat{K}$, donc $\hat{K}$ est une *extension* de K (Ch. 1).
Soit $\overline{u} \in \hat{K}$; $\overline{u}$ est la classe d'équivalence modulo C_0 d'une suite
$u = (u_n)_{n\in\mathbb{N}} \in C$. Quel que soit $\varepsilon \in \mathbb{R}_+^*$, il existe $N_\varepsilon \in \mathbb{N}$, tel que, pour des entiers m et n,

$$(m > N_\varepsilon, n > N_\varepsilon) \Longrightarrow |\ u_n - u_m\ | < \varepsilon.$$

Par suite, dans $(\mathbb{R}, |\ |_\infty)$, on a

$$||\ u_n\ | - |\ u_m\ ||_\infty \leq ||\ u_n - u_m\ ||_\infty = |\ u_n - u_m\ |, \text{ donc}$$
$$(m > N_\varepsilon, n > N_\varepsilon) \Longrightarrow ||\ u_n\ | - |\ u_m\ ||_\infty < \varepsilon.$$

Ainsi $(|\ u_n\ |)_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\mathbb{R}$ et, puisque $(\mathbb{R}, |\ |_\infty)$ est complet (Th. A.39), $(|\ u_n\ |)_{n\in\mathbb{N}}$ converge dans $\mathbb{R}$; alors,

$$\overline{u} = 0 \iff u = (u_n)_{n\in\mathbb{N}} \in C_0 \iff \lim_{n\longrightarrow\infty} |\ u_n\ | = 0;$$
$$\overline{u} \neq 0 \iff \lim_{n\longrightarrow\infty} |\ u_n\ | > 0.$$

Pour tout $\overline{u} \in \hat{K}$, on pose $|\ \hat{\overline{u}}\ | := \lim_{n\longrightarrow\infty} |\ u_n\ |$ et on vérifie que l'application $\hat{|\ |}$ de $\hat{K}$ dans $\mathbb{R}_+$ ainsi définie, est une valeur absolue de $\hat{K}$, prolongeant la valeur absolue $|\ |$ de K.

2) Etant donné $\overline{u}$ et $\overline{v}$ dans $\hat{K}$, quels que soient leurs représentants respectifs, $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ dans C, on a

$$\overline{u} = \overline{v} \iff \lim_{n\longrightarrow\infty} (u_n - v_n) = 0 \iff \lim_{n\longrightarrow\infty} u_n = \lim_{n\longrightarrow\infty} v_n.$$

On convient alors d'identifier tout élément $\overline{u}$ de $\hat{K}$, à $\lim_{n\longrightarrow\infty} u_n$, quel que soit le représentant $(u_n)_{n\in\mathbb{N}}$, modulo C_0, de $\overline{u}$ dans C.
Ainsi, tout élément de $\hat{K}$ est la limite d'une suite d'éléments de K ; on en déduit que K est *dense* dans $\hat{K}$, muni de la topologie induite par $\hat{|\ |}$.

3) On démontre que le corps valué $(\hat{K},\hat{|\ |})$ est *complet*, c'est-à-dire que toute suite de Cauchy d'éléments de $\hat{K}$ converge dans $\hat{K}$, par une méthode analogue à celle qui à permis de prouver que $(\mathbb{R},|\ |_\infty)$ est complet (Th. A.39). □

Définition A.41. On appelle **complétion** d'un corps valué $(K,|\ |)$, tout corps valué $(\hat{K},\hat{|\ |})$, qui vérifie les conditions du Th. A.40.
On dit aussi que $\hat{K}$ est un **complété** de K relativement à la valeur absolue $|\ |$.

Théorème A.42. Propriété universelle de la complétion d'un corps valué
$(\hat{K},\hat{|\ |})$ étant la complétion de $(K,|\ |)$ définie dans le Th. A.40., *soit λ le morphisme canonique de K dans $\hat{K}$; alors quels que soient le corps valué complet $(K',|\ |')$ et le morphisme f de K dans K' tel que, pour tout $a\in K$, $|\ f(a)\ |'=|\ a\ |$, il existe un unique morphisme ψ de $\hat{K}$ dans K' tel que $\psi\circ\lambda = f$, ce qui implique*

$$|\ \hat{\overline{u}}\ | = |\ \psi(\overline{u})\ |', \forall \overline{u}\in\hat{K}.$$

Démonstration. On utilise les notations de la preuve du Th. A.40.
Les éléments de K sont identifiés aux suites de Cauchy constantes et quel que soit a dans K, $\lambda(a) = a$.
Soit $\overline{u}\in\hat{K}$ et $(u_n)_{n\in\mathbb{N}}\in C$ un représentant de $\overline{u}$ modulo C_0 ; on écrit alors (voir preuve du Th. A.40),

$$\overline{u} = \lim_{n\longrightarrow\infty} u_n.$$

Moyennant l'hypothèse concernant le morphisme f, on montre que,
$(u_n)_{n\in\mathbb{N}}$ étant une suite de Cauchy de K, $(f(u_n))_{n\in\mathbb{N}}$ est une suite de Cauchy de K' ; alors puisque K' est complet, cette suite converge dans K' et on vérifie que sa limite est indépendante du choix de la suite $(u_n)_{n\in\mathbb{N}}$ représentant l'élément $\overline{u}$ de $\hat{K}$.
On considère l'application

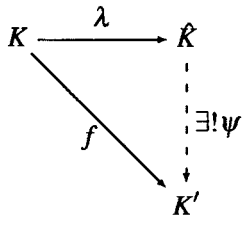
$$\begin{aligned}\psi : \hat{K} &\longrightarrow K'\\ \overline{u} = \lim_{n\longrightarrow\infty} u_n &\longmapsto l := \lim_{n\longrightarrow\infty} f(u_n).\end{aligned}$$

ψ est alors un morphisme de $\hat{K}$ dans K' tel que $\psi\circ\lambda = f$, dont on vérifiera l'unicité. De plus, quel que soit $\overline{u} = \lim_{n\longrightarrow\infty} u_n$ dans $\hat{K}$,

$$\begin{aligned}|\ \hat{\overline{u}}\ | = \lim_{n\longrightarrow\infty} |\ u_n\ | &= \lim_{n\longrightarrow\infty} |\ f(u_n)\ |'\\ &= |\ \lim_{n\longrightarrow\infty} f(u_n)\ |' = |\ \psi(\overline{u})\ |'.\end{aligned}$$

□

Le Th. A.42 se traduit par le diagramme commutatif suivant :



Corollaire A.43. *Tout corps valué* $(K,|\ |)$ *admet une complétion* $(\hat{K},\hat{|\ |})$, unique *à une isométrie près.*

Démonstration. Le Th. A.40 prouve l'existence d'une complétion $(\hat{K},\hat{|\ |})$ d'un corps valué $(K,|\ |)$.
Si l'on suppose que $(K',|\ |')$ est aussi une complétion de $(K,|\ |)$, alors, λ' désignant le monomorphisme canonique de K dans K', la propriété universelle appliquée au couple (K',λ') implique qu'il existe un unique morphisme $\psi' : K' \longrightarrow \hat{K}$ tel que

$$\psi' \circ \lambda' = \lambda \quad \text{et} \quad |x|' = |\psi(x)|, \forall x \in K'.$$

On vérifie que $\psi' = \psi^{-1}$; par suite, ψ est une isométrie de $\hat{K}$ sur K' (Rem. A.37). □

Exemple A.44. Les théorèmes A.38. et A.39. montrent que $(\mathbb{R},|\ |_\infty)$ est la complétion du corps valué $(\mathbb{Q},|\ |_\infty)$.

Remarque A.45. Un corps valué $(K,|\ |)$ est complet s'il coïncide avec sa complétion.

B. Corps des nombres p-adiques

Définition A.46. Le complété du corps $\mathbb{Q}$, relativement à la valeur absolue p-adique normalisée $|\ |_p$ (Déf. A.22), est appelé le **corps des nombres p-adiques** et noté $\mathbb{Q}_p$.

On notera encore $|\ |_p$, la valeur absolue de $\mathbb{Q}_p$ induite par la valeur absolue p-adique *normalisée* de $\mathbb{Q}$ (Cf. Th. A.40)

L'application du Th. A.35 au cas du corps valué complet $(\mathbb{Q}_p,|\ |_p)$ donne les résultats suivants.

Définition A.47. L'anneau des entiers du corps valué complet $(\mathbb{Q}_p,|\ |_p)$ est noté $\mathbb{Z}_p$ et ses éléments sont appelés les **entiers p-adiques** .

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p\ ;\ |x|_p \leq 1\}. \tag{A.17}$$

Théorème A.48. *Pour tout nombre premier* p,
1) *L'anneau local* $\mathbb{Z}_p$ *est principal et son unique idéal maximal est* $p\mathbb{Z}_p$.
2) *Le corps résiduel du corps valué* $(\mathbb{Q}_p,|\ |_p)$ *est isomorphe à* $\mathbb{Z}/p\mathbb{Z}$.
3) $\mathbb{Q}_p$ *est le corps des fractions de l'anneau* $\mathbb{Z}_p$.

Démonstration. La propriété 3) résulte directement du Th. A.35
1) Comme dans le cas de $(\mathbb{Q},|\ |_p)$ (Exemple A.36), $p\mathbb{Z}_p$ est l'idéal maximal de l'anneau local $\mathbb{Z}_p$ dont les idéaux non nuls sont alors les $p^k\mathbb{Z}_p$, $k \in \mathbb{N}$; donc l'anneau local $\mathbb{Z}_p$ est principal.
2) D'après le Th. A.40, tout $x \in \mathbb{Q}_p$ est la limite d'une suite de Cauchy $(x_n)_{n\in\mathbb{N}}$ du corps valué non-archimédien $(\mathbb{Q},|\ |_p)$; alors, quel que soit $\varepsilon \in \mathbb{Q}$ tel que $0 < \varepsilon < |x|_p$, il existe $N \in \mathbb{N}$ tel que

$$n \geq N \Longrightarrow |x - x_n|_p \leq \varepsilon < |x|_p\ .$$

En appliquant la Prop. A.33 aux éléments $x_n - x$ et x, on obtient

$$n \geq N \Longrightarrow |x_n|_p = |x|_p\ .$$

On en conclut que, quel que soit $x \in \mathbb{Q}_p$, il existe $y \in \mathbb{Q}$ tel que

$$|x - y|_p < |x|_p, \text{ donc } |y|_p = |x|_p\ . \tag{A.18}$$

Par ailleurs, les éléments non nuls, $\overline{u}$, du corps résiduel $\mathbb{Z}_p/p\mathbb{Z}_p$ sont les classes modulo $p\mathbb{Z}_p$ des éléments $u \in (\mathbb{Z}_p \setminus p\mathbb{Z}_p)$, donc des éléments u tels que $|\, u \,|_p = 1$.
On en déduit (voir relation (A.18)) que, quel que soit $u \in (\mathbb{Z}_p \setminus p\mathbb{Z}_p)$, il existe $v \in \mathbb{Q}$ tel que

$$|\, v \,|_p = |\, u \,|_p = 1 \text{ et } |\, v - u \,|_p < 1.$$

Compte tenu des notations utilisées dans l'étude de $(\mathbb{Q}, |\ |_p)$ (Exemple A.36), on a alors, $v \in \mathcal{U}_p$ et

$$|\, v - u \,|_p < 1 \Longrightarrow \overline{v} = \overline{u}, \text{ dans } \mathbb{Z}_p/p\mathbb{Z}_p.$$

Par suite, moyennant le résultat obtenu dans l'Exemple A.36., le corps $\mathbb{Z}_p/p\mathbb{Z}_p$ s'identifie au corps $\mathbb{Z}/p\mathbb{Z}$.
Le corps valué $(\mathbb{Q}, |\ |_p)$ et son complété $(\mathbb{Q}_p, |\ |_p)$ admettent donc le même corps résiduel $\mathbb{Z}/p\mathbb{Z}$. □

Remarque A.49. D'une façon générale, on démontre qu'un corps valué et son complété ont le même corps résiduel (à un isomorphisme près) ([33]).

Nous énoncerons, sans démonstration, le théorème donnant le *Développement de Hensel* d'un nombre p-adique ([18, 30, 38]).

Théorème A.50. Developpement de Hensel
Quel que soit $x \in \mathbb{Q}_p$, il existe une unique suite d'entiers $(a_i)_{i \geq m}$ tels que, $0 \leq a_i \leq p-1$, $m = v_p(x) \in \mathbb{Z}$ et la série

$$\sum_{i \geq m} a_i p^i$$

converge vers x dans le corps valué complet $(\mathbb{Q}_p, |\ |_p)$. On écrit

$$x = \sum_{i \geq m} a_i p^i. \tag{A.19}$$

La relation (A.19) *définit ce qu'on appelle le* développement de Hensel *de x.*

Remarque A.51. Nous avons défini le corps des nombres p-adiques comme le complété du corps valué $(\mathbb{Q}, |\ |_p)$, mais on peut aussi définir le corps $\mathbb{Q}_p$, en utilisant la notion de « limite projective », qui est une notion de Théorie des Catégories, non introduite dans ce livre ([30, 43]).

Appendice B
Transcendance de e et de π

Préliminaires :

Cet appendice est consacré aux preuves, données en *Analyse*, de la transcendance des nombre réels e et π sur le corps des nombres rationnels $\mathbb{Q}$ (Cf. Exemple 2.30).
La transcendance de e a été démontrée par Hermite en 1873 ; en utilisant des méthodes analogues, Lindemann a démontré la transcendance de π en 1882.
Ces démonstrations utilisent la méthode du « *raisonnement par l'absurde* » conduisant à une contradiction avec le lemme suivant.

Lemme B.1. *Une fonction $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, telle que $f(n)$ tend vers 0 quand la variable n tend vers $+\infty$, est nécessairement nulle, à partir d'un certain entier n_0.*

Démonstration. L'hypothèse du lemme implique qu'il existe un entier n_0 tel que

$$\forall n \in \mathbb{Z}, \quad n \geq n_0 \Longrightarrow | f(n) - 0 | < \frac{1}{2} ;$$

or, $f(n)$ est entier, par suite, $f(n) = 0, \forall n \geq n_0$. □

1. Transcendance de e sur $\mathbb{Q}$

Théorème B.2. *(Hermite)*
Le nombre réel e est transcendant sur $\mathbb{Q}$.

Démonstration. La preuve originale de Hermite (1873) a été successivement simplifiée par Weierstrass, Hilbert, Hurwitz et Gordan ; c'est cette démonstration simplifiée que nous développons ici.

On suppose e non transcendant sur $\mathbb{Q}$, donc algébrique sur $\mathbb{Q}$.
Il existe alors un polynôme non constant $q(X) \in \mathbb{Q}[X]$, tel que $q(e) = 0$.
Posons $q(X) = \sum_{0 \leq i \leq n} a_i X^i$, avec $a_0 \neq 0$ et $n > 0$.
$\mathbb{Q}$ étant le corps des fractions de $\mathbb{Z}$, il existe $\gamma \in \mathbb{Q}$ et $q_1(X) \in \mathbb{Z}[X]$ tels que

$$q(X) = \gamma q_1(X) \quad \text{et} \quad q_1(e) = 0.$$

On peut donc, dès le départ, supposer que les coefficients $a_i, 0 \leq i \leq n$, du polynôme $q(X)$ sont des *entiers*.

Soit p un nombre premier quelconque ; on considère, dans $\mathbb{Q}[X]$,

$$f(X) := \frac{X^{p-1}(X-1)^p(X-2)^p \ldots (X-n)^p}{(p-1)!}. \tag{B.1}$$

$$\text{On pose} \quad F(X) := f(X) + f'(X) + \cdots + f^{(np+p-1)}(X), \tag{B.2}$$

où les $f^{(k)}(X), 1 \leq k \leq np+p-1$, sont les polynômes dérivés à l'ordre k de $f(X)$ ([13], Déf. 4.30) ; on note que

$$deg\, f = np+p-1 \Longrightarrow f^{(np+p)}(X) = 0.$$

Les polynômes $f(X)$ et $F(X)$ étant considérés dans $\mathbb{R}[X]$, notons encore, f et F les fonctions polynômes réelles qui leurs sont associées ([13], Déf. 4.21). Pour $x \in \mathbb{R}$, on a

$$\frac{d}{dx}(e^{-x}F(x)) = e^{-x}\big(F'(x) - F(x)\big) = -e^{-x}f(x). \tag{B.3}$$

Les entiers $a_i, 0 \leq i \leq n$, étant les coefficients du polynôme $q(X)$ tel que $q(e) = 0$, la relation (B.3) permet d'écrire, pour tout entier $i, 0 \leq i \leq n$,

$$a_i \int_0^i e^{-x}f(x)\,dx = a_i[-e^{-x}F(x)]_0^i \tag{B.4}$$

$$= a_i\big(F(0) - e^{-i}F(i)\big). \tag{B.5}$$

On en déduit

$$\sum_{i=0}^{n} a_i e^i \int_0^i e^{-x}f(x)\,dx = F(0)\sum_{i=0}^{n} a_i e^i - \sum_{i=0}^{n} a_i F(i);$$

alors la définition de F et l'hypothèse $q(e) = \sum_{i=0}^{n} a_i e^i = 0$ impliquent

$$\sum_{i=0}^{n} a_i e^i \int_0^i e^{-x}f(x)\,dx = -\sum_{i=0}^{n}\Big(\sum_{k=0}^{np+p-1} a_i f^{(k)}(i)\Big). \tag{B.6}$$

Compte tenu de la relation (B.1) donnant l'expression de $f(x)$, en appliquant la règle de Leibnitz, on obtient les résultats suivants, pour les valeurs de $f^{(k)}(i)$.

$$\text{Pour } i = 0, \quad f^{(k)}(0) = 0,\ \forall k(0 \leq k \leq np-p+1,\ k \neq (p-1)),$$

$$\text{et} \quad f^{(p-1)}(0) = \frac{(p-1)!}{(p-1)!}(-1)^p \ldots (-n)^p = (-1)^{np}(n!)^p.$$

$$\text{Pour } 1 \leq i \leq n, \quad f^{(k)}(i) = 0,\ \forall k(0 \leq k \leq p-1) \text{ et}$$

quel que soit $k(p \leq k \leq np+p-1)$, les seuls termes non nuls, intervenant dans $f^{(k)}(i)$, sont des entiers provenant des facteurs $(X-i)^p$ dérivables p fois ; on en déduit que tous ces entiers sont divisibles par p, car

$$f^{(k)}(i) = \frac{p!}{(p-1)!}\lambda_i = p\lambda_i \quad \text{où } \lambda_i \in \mathbb{Z}^*.$$

Par suite, la relation (B.6) entraîne

$$\sum_{i=0}^{n} a_i e^i \int_0^i e^{-x}f(x)\,dx = -\sum_{i=0}^{n} a_i p\lambda_i - a_0(-1)^{np}(n!)^p \tag{B.7}$$

$$= mp - a_0(-1)^{np}(n!)^p, \quad \text{où } m \in \mathbb{Z}^*. \tag{B.8}$$

Pour $p > max(n, \mid a_0 \mid)$, l'entier $a_0(-1)^{np}(n!)^p$ est non nul et non divisible par p.
On en déduit qu'en choisissant le nombre premier p suffisamment grand, le premier membre de la relation (B.6) est un entier *non nul.*

Pour $x \in \mathbb{R}$ et $0 \leq x \leq n$, on a, pour tout entier $i (1 \leq i \leq n)$,

$$0 \leq |x-i|^p \leq n^p, \quad \text{d'où} \quad |f(x)| \leq \frac{1}{(p-1)!} n^{np+p-1}.$$

Par suite,

$$|\sum_{i=0}^{n} a_i e^i \int_0^i e^{-x} f(x)\,dx| \leq \sum_{i=0}^{n} |a_i e^i| \int_0^i \frac{n^{np+p-1}}{(p-1)!} dx \tag{B.9}$$

$$\leq \sum_{i=0}^{n} |a_i e^i| \, i \frac{n^{np+p-1}}{(p-1)!} \tag{B.10}$$

qui tend vers 0 quand p tend vers $+\infty$; or le premier membre de l'inégalité (B.9) est un entier *non nul*, ce qui contredit le lemme B.1.
On en conclut que e est transcendant sur $\mathbb{Q}$. □

2. Transcendance de π sur $\mathbb{Q}$

Démontrons, dans un premier temps, que $\pi \notin \mathbb{Q}$, autrement dit,

Théorème B.3. *Le nombre réel π est irrationnel.*

Démonstration. Pour $\alpha \in \mathbb{R}^*$ et tout $n \in \mathbb{N}$, on considère l'intégrale

$$I_n = \int_{-1}^{+1} (1-x^2)^n \cos \alpha x\,dx.$$

Intégrons I_n par parties, dans le cas $n \geq 2$.

$$\begin{aligned} I_n &= \frac{1}{\alpha} \int_{-1}^{+1} (1-x^2)^n d(\sin \alpha x) \\ &= \frac{1}{\alpha} [(1-x^2)^n \sin \alpha x]_{-1}^{+1} - \frac{1}{\alpha} \int_{-1}^{+1} \sin \alpha x \left(-2nx(1-x^2)^{n-1}\right) dx \\ &= \frac{1}{\alpha} \int_{-1}^{+1} 2nx(1-x^2)^{n-1} \sin \alpha x\,dx \\ &= -\frac{1}{\alpha^2} \int_{-1}^{+1} 2nx(1-x^2)^{n-1} d(\cos \alpha x). \end{aligned}$$

On intègre, de nouveau, par parties :

$$\begin{aligned} I_n = &-\frac{1}{\alpha^2} [2nx(1-x^2)^{n-1} \cos \alpha x]_{-1}^{+1} \\ &+ \frac{1}{\alpha^2} \int_{-1}^{+1} \left(-4n(n-1)x^2(1-x^2)^{n-2}\right) \cos \alpha x\,dx \\ &+ \frac{1}{\alpha^2} \int_{-1}^{+1} 2n(1-x^2)^{n-1} \cos \alpha x\,dx. \\ I_n = &\frac{1}{\alpha^2} \int_{-1}^{+1} 4n(n-1)(1-x^2)^{n-1} \cos \alpha x\,dx \\ &- \frac{1}{\alpha^2} \int_{-1}^{+1} 4n(n-1)(1-x^2)^{n-2} \cos \alpha x\,dx \\ &+ \frac{1}{\alpha^2} \int_{-1}^{+1} 2n(1-x^2)^{n-1} \cos \alpha x\,dx. \end{aligned}$$

On en déduit

$$\forall n \geq 2, \quad \alpha^2 I_n = 2n(2n-1)I_{n-1} - 4n(n-1)I_{n-2}. \tag{B.11}$$

D'autre part, $I_0 = \int_{-1}^{+1} \cos \alpha x\, dx = [\frac{1}{\alpha} \sin \alpha x]_{-1}^{+1} = \frac{2}{\alpha} \sin \alpha$, d'où

$$\alpha I_0 = 2 \sin \alpha. \tag{B.12}$$

$$\begin{aligned} I_1 &= \int_{-1}^{+1} (1-x^2) \cos \alpha x\, dx \\ &= [\frac{1}{\alpha}(1-x^2) \sin \alpha x]_{-1}^{+1} - \frac{1}{\alpha} \int_{-1}^{1} -2x \sin \alpha x\, dx \\ &= \frac{2}{\alpha} \int_{-1}^{+1} x \sin \alpha x\, dx \\ &= [-\frac{2}{\alpha^2} x \cos \alpha x]_{-1}^{+1} - \frac{2}{\alpha} \int_{-1}^{+1} -\frac{\cos \alpha x}{\alpha}\, dx \\ I_1 &= -\frac{4}{\alpha^2} \cos \alpha + \frac{4}{\alpha^3} \sin \alpha, \end{aligned}$$

d'où la relation

$$\alpha^3 I_1 = 4 \sin \alpha - 4\alpha \cos \alpha. \tag{B.13}$$

Pour $n = 2$, les relations (B.11), (B.12), (B.13) impliquent

$$\begin{aligned} \alpha^2 I_2 &= 12 I_1 - 8 I_0, \\ &= 12(\frac{4}{\alpha^3} \sin \alpha - \frac{4}{\alpha^2} \cos \alpha) - 8 \frac{2}{\alpha} \sin \alpha. \end{aligned}$$

Par suite,

$$\alpha^5 I_2 = 2! \left((24 - 8\alpha^2) \sin \alpha - 24\alpha \cos \alpha\right). \tag{B.14}$$

Par récurrence sur n, démontrons que pour tout $n \in \mathbb{N}$, l'intégrale I_n satisfait, quel que soit $\alpha \in \mathbb{R}^*$, à une relation de la forme :

$$\alpha^{2n+1} I_n = n! \left(P_n(\alpha) \sin \alpha + Q_n(\alpha) \cos \alpha\right), \tag{B.15}$$

où $P_n(X)$ et $Q_n(X)$ sont de degré *inférieur ou égal* à $n+1$, dans $\mathbb{Z}[X]$.
Les relations (B.12), (B.13) et (B.14) montrent que la relation (B.15) est vérifiée pour $0 \leq n \leq 2$; on suppose alors $n > 2$ et la relation (B.15) vraie pour tout entier positif $k \leq n-1$. Ecrivons la relation (B.15) pour I_{n-1} et I_{n-2} :

$$\begin{aligned} \alpha^{2n-1} I_{n-1} &= (n-1)! \left(P_{n-1}(\alpha) \sin \alpha + Q_{n-1}(\alpha) \cos \alpha\right), \\ \alpha^{2n-3} I_{n-2} &= (n-2)! \left(P_{n-2}(\alpha) \sin \alpha + Q_{n-2}(\alpha) \cos \alpha\right). \end{aligned}$$

En utilisant la relation (B.11), on obtient

$$\begin{aligned} \alpha^{2n+1} I_n &= n! \big(2(2n-1)(P_{n-1}(\alpha) + Q_{n-1}(\alpha)) \\ &\qquad - 4\alpha^2 (P_{n-2}(\alpha) \sin \alpha + Q_{n-2}(\alpha) \cos \alpha)\big) \\ \alpha^{2n+1} I_n &= n! \big((2(2n-1)P_{n-1}(\alpha) - 4\alpha^2 P_{n-2}(\alpha)) \sin \alpha \\ &\qquad + (2(2n-1)Q_{n-1}(\alpha) - 4\alpha^2 Q_{n-2}(\alpha)) \cos \alpha\big). \end{aligned}$$

Posons

$$\begin{aligned} P_n(X) &:= 2(2n-1)P_{n-1}(X) - 4X^2 P_{n-2}(X), \\ Q_n(X) &:= 2(2n-1)Q_{n-1}(X) - 4X^2 Q_{n-2}(X). \end{aligned}$$

L'hypothèse de récurrence entraîne que les polynômes $P_n(X)$ et $Q_n(X)$ sont dans $\mathbb{Z}[X]$ et

$$(deg\,P_{n-1} \leq n, \quad deg\,P_{n-2} \leq n-1) \Longrightarrow deg\,P_n \leq n+1.$$

De même, on a $deg\,Q_n \leq n+1$, d'où la relation (B.15).

Supposons, π rationnel; on peut écrire $\pi = \frac{a}{s}$, où $(a,s) \in \mathbb{Z} \times \mathbb{Z}^*$, a et s positifs; en appliquant la relation (B.15) pour $\alpha = \frac{\pi}{2}$, on obtient

$$(\frac{a}{2s})^{2n+1} I_n = n!\,P_n(\frac{a}{2s}).$$

$$deg\,P_n \leq n+1 \leq 2n+1 \Longrightarrow (2s)^{2n+1} P_n(\frac{a}{2s}) \in \mathbb{Z}.$$

On en déduit que $a^{2n+1}\frac{I_n}{n!} \in \mathbb{Z}$, donc

$$J_n := \frac{a^{2n+1}}{n!}\int_{-1}^{+1}(1-x^2)^n \cos\frac{\pi}{2}x\,dx \in \mathbb{Z}.$$

Posons $f(x) := (1-x^2)^n \cos\frac{\pi}{2}x$.
L'étude de la fonction f de la variable réelle x montre que l'on a

$$\int_{-1}^{+1} f(x)\,dx > 0,$$

donc, $\forall n \in \mathbb{N}$, $J_n > 0$, en particulier, $J_n \neq 0$ mais

$$0 < J_n \leq \frac{a^{2n+1}}{n!}\int_{-1}^{+1}\cos\frac{\pi}{2}x\,dx \Longrightarrow J_n \leq \frac{a^{2n+1}}{n!}\lambda,$$

où λ est positif dans $\mathbb{R}$, ce qui entraîne que J_n tend vers 0 quand n tend vers $+\infty$, d'où une contradiction avec le lemme B.1., donc $\pi \notin \mathbb{Q}$. □

Théorème B.4. *(Lindemann)*
Le nombre réel π est transcendant sur $\mathbb{Q}$.

Démonstration. On sait que $\pi \notin \mathbb{Q}$, (Th. B.3), supposons π *algébrique* sur $\mathbb{Q}$. On considère alors π dans la *clôture algébrique* $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, dans $\mathbb{C}$ (Ch. 5). Par ailleurs, le nombre complexe i étant algébrique sur $\mathbb{Q}$ ($i^2 = -1$), on a aussi $i\pi$ algébrique sur $\mathbb{Q}$.
Posons $p_1(X) := Irr_{\mathbb{Q}}(i\pi, X)$ et $n := deg\,p_1 > 1$ (Cf. Ch. 2).
Le polynôme irréductible $p_1(X)$ a n racines distinctes et non nulles dans $\overline{\mathbb{Q}}$ (Th. 3.24); on les notera : $\alpha_1 := i\pi, \alpha_2, \ldots, \alpha_n$. Par ailleurs, on a

$$e^{i\pi} = \cos\pi + i\sin\pi = -1 \iff e^{\alpha_1} + 1 = 0,$$

ce qui permet d'écrire, dans $\mathbb{C}$,

$$(e^{\alpha_1}+1)(e^{\alpha_2}+1)\ldots(e^{\alpha_n}+1) = 0. \tag{B.16}$$

En développant le premier membre de (B.16), on obtient une relation de la forme :

$$e^{\gamma_1} + e^{\gamma_2} + \cdots + e^{\gamma_s} + 1 = 0, \tag{B.17}$$

où l'on considère que $1 = e^0$.
Nous allons montrer qu'il existe un polynôme à *coefficients entiers,* dont les racines sont les *exposants* de e qui apparaissent dans le premier membre de la relation (B.17).
Ces exposants s'écrivent, d'une façon générale,

$$\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_k},\ 1 \le i_1 < i_2 < \cdots < i_k \le n,\ 1 \le k \le n. \tag{B.18}$$

Le cas : $k = 1$, correspond aux exposants de e qui sont les racines α_i, $1 \le i \le n$, du polynôme $p_1(X) \in \mathbb{Q}[X]$.
Le cas : $k = 2$, correspond aux exposants de e de la forme $\beta_{i,j} = \alpha_i + \alpha_j$, où $1 \le i < j \le n$.
On en déduit que les coefficients du polynôme

$$p_2(X) := \prod_{1 \le i < j \le n} (X - \beta_{i,j})$$

sont des polynômes symétriques en les racines de $p_1(X)$, donc s'expriment rationnellement en fonction des coefficients de ce polynôme ([13], Ch. 8), d'où $p_2(X) \in \mathbb{Q}[X]$.
D'une façon générale, pour tout entier k fixé, $1 \le k \le n$), on considère le polynôme

$$p_k(X) = \prod_{1 \le i_1 < i_2 < \cdots < i_k \le n} (X - \sum_{1 \le j \le k} \alpha_{i_j}),$$

dont les coefficients sont encore des polynômes symétriques en les racines de $p_1(X)$; on en déduit que pour tout k, $1 \le k \le n$, $p_k(X) \in \mathbb{Q}[X]$. On a, en particulier, $p_n(X) = X - \sum_{1 \le i \le n} \alpha_i$. Posons alors,

$$q(X) := X p_1(X) p_2(X) \ldots p_n(X). \tag{B.19}$$

Le polynôme $q(X) \in \mathbb{Q}[X]$ et a pour racines l'ensemble des exposants de e qui apparaissent dans le premier membre de la relation (B.17).
Moyennant une éventuelle réindexation des exposants de e dans (B.17), notons $\gamma_1, \ldots, \gamma_r$ les racines *non nulles*, distinctes ou confondues, de $q(X)$ et $m \ge 1$, l'ordre de multiplicité de la racine 0 ; on a nécessairement, $1 < r \le s$ et $m \ge 1$. La relation (B.17) s'écrit alors,

$$e^{\gamma_1} + e^{\gamma_2} + \cdots + e^{\gamma_r} + m = 0. \tag{B.20}$$

Par suite X^m divise $q(X)$ dans $\mathbb{Q}[X]$.
D'autre part, $\mathbb{Q}$ étant le corps des fractions de $\mathbb{Z}$, il existe un entier d tel que $dq(X) \in \mathbb{Z}[X]$.
On en déduit qu'il existe $\rho(X) \in \mathbb{Z}[X]$ tel que $dq(X) = X^m \rho(X)$; et les racines de $\rho(X)$, dans $\overline{\mathbb{Q}}$, sont les γ_j, $1 \le j \le r$.
Dans $\mathbb{Z}[X]$, supposons

$$\rho(X) = c_r X^r + c_{r-1} X^{r-1} + \cdots + c_0, \tag{B.21}$$

où, compte tenu de ce qui précède, on a $r > 0$ et c_0, c_r non nuls.
Etant donné un nombre premier p, considérons, dans $\mathbb{Q}[X]$,

$$f(X) := \frac{c^{rp-1}}{(p-1)!} X^{p-1} (\rho(X))^p, \quad \text{où } c := c_r \tag{B.22}$$

$$\text{et} \qquad F(X) := f(X) + f'(X) + \cdots + f^{(rp+p-1)}(X), \tag{B.23}$$

où, les $f^{(k)}(X)$, $0 \le k \le rp + p - 1$ sont les polynômes dérivés successifs de $f(X)$;
$\deg f = rp + p - 1$ implique $f^{(rp+p)}(X) = 0$.

Comme dans la preuve du Th. A.2, on note encore f et F les fonctions polynômes de la variable réelle x, respectivement associées aux polynômes f et F définis par les relations (B.22) et (B.23) et on obtient (voir la relation (B.3))

$$\frac{d}{dx}(e^{-x}F(x)) = -e^{-x}f(x),$$
$$e^{-x}F(x) - F(0) = -\int_0^x e^{-y}f(y)dy.$$

Supposons x fixé et posons $y = \lambda x$; alors, $dy = xd\lambda$ et

$$e^{-x}F(x) - F(0) = -x\int_0^1 e^{-\lambda x}f(\lambda x)d\lambda, \tag{B.24}$$

$$\text{d'où} \quad F(x) - e^{x}F(0) = -x\int_0^1 e^{(1-\lambda)x}f(\lambda x)d\lambda. \tag{B.25}$$

Dans la relation (B.25), donnons successivement à x les valeurs $\gamma_1, \ldots, \gamma_r$ et sommons; en tenant compte de l'égalité (B.20), on obtient

$$\sum_{j=1}^{r} F(\gamma_j) + mF(0) = -\sum_{j=1}^{r} \gamma_j \int_0^1 e^{(1-\lambda)\gamma_j} f(\lambda\gamma_j)\, d\lambda, \tag{B.26}$$

où $\quad m = -\sum_{j=1}^{r} e^{\gamma_j}$.

Montrons qu'en choisissant le nombre premier p suffisamment grand, le premier membre de la relation (B.26) est un *entier non nul.*

$$\sum_{j=1}^{r} F(\gamma_j) = \sum_{j=1}^{r}\Big(\sum_{k=0}^{rp+p-1} f^{(k)}(\gamma_j)\Big) = \sum_{k=0}^{rp+p-1}\Big(\sum_{j=1}^{r} f^{(k)}(\gamma_j)\Big).$$

Le calcul des $f^{(k)}(x)$ montre que, quel que soit $j\,(1 \le j \le r)$, on a
- pour $0 \le k \le p-1$, $\quad \rho(\gamma_j) = 0 \Longrightarrow f^{(k)}(\gamma_j) = 0$.
- pour $p \le k \le rp+p-1$, $\quad deg\, f^{(p)}(X) = rp-1 \Longrightarrow deg\, f^{(k)}(X) \le rp-1$;

de plus, $f^{(k)}(X)$ contient pc^{rp-1} en facteur. On a, en particulier,

$$\forall j\,(1 \le j \le r),\ f^{(p)}(\gamma_j) = p(\gamma_j)^{p-1}c^{rp-1}(\rho'(\gamma_j))^p.$$

On en déduit que, pour $p \le k \le rp+p-1$, $\sum_{j=1}^{r} f^{(k)}(\gamma_j)$ est une fonction polynômiale symétrique en $\gamma_1, \gamma_2, \ldots, \gamma_r$, de degré *inférieur ou égal* à $rp-1$. Par suite ([13], p. 259), pour $p \le k \le rp+p-1$, $\sum_{j=1}^{r} f^{(k)}(\gamma_j)$ est une fonction polynômiale de degré *inférieur ou égal* à $rp-1$ en les fonctions symétriques élémentaires des $\gamma_j, 1 \le j \le r$, donc en les $\frac{c_i}{c_r} = \frac{c_i}{c}$, où les
c_i, $0 \le i \le r$, sont les coefficients du polynôme $\rho(X) \in \mathbb{Z}[X]$ (Cf. (B.21)).
Sachant que pour $p \le k \le rp+p-1$, les $f^k(X)$, contiennent pc^{rp-1} en facteur, on obtient

$$p \le k \le rp+p-1 \Longrightarrow \sum_{j=1}^{r} f^{(k)}(\gamma_j) = ps_k, \quad \text{où } s_k \in \mathbb{Z}. \tag{B.27}$$

Examinons $F(0)$; en utilisant toujours la notation $c = c_r$, on a

$$f^{(k)}(0) = \begin{cases} 0 & \text{pour } 0 \leq k \leq p-1, \\ c^{rp-1}c_0^p & \text{pour } k = p-1, \\ ph_k,\ h_k \in \mathbb{Z} & \text{pour } p \leq k \leq rp+p-1. \end{cases}$$

Le premier membre de la relation (B.26) est donc de la forme

$$l\,p + m\,c^{rp-1}c_0^p, \quad \text{où } l \in \mathbb{Z}.$$

On sait que les entiers m, c, c_0 sont non nuls, par suite, en choisissant le nombre premier p tel que

$$p > max(m, |\,c\,|, |\,c_0\,|),$$

on peut affirmer que l'entier $l\,p + m\,c^{rp-1}c_0^p$ est *non nul.*

Considérons, maintenant, le second membre de la relation (B.26).

$$\mu(j) := sup_{0\leq\lambda\leq 1}(|\,p(\lambda\gamma_j)\,|) \Longrightarrow |\,f(\lambda\gamma_j)\,| \leq \frac{|\,c\,|^{rp-1}}{(p-1)!}\,|\,\gamma_j\,|^{p-1}\,(\mu(j))^p,$$

$$|\,-\sum_{j=1}^{r}\gamma_j\int_0^1 e^{(1-\lambda)\gamma_j}f(\lambda\gamma_j)\,d\lambda\,| \leq \sum_{j=1}^{r}\frac{|\,c\,|^{rp-1}}{(p-1)!}\,|\,\gamma_j\,|^p\,|\,\mu(j)\,|^p\,M,$$

$$\text{où} \qquad M = |\,sup_{1\leq j\leq r}\int_0^1 e^{(1-\lambda)\gamma_j}\,d\lambda\,|\,.$$

Ainsi le second membre de la relation (B.26) tend vers 0, quand p tend vers ∞, ce qui entraîne encore une contradiction avec le lemme B.1. ; donc π est transcendant sur $\mathbb{Q}$. □

Bibliographie

[1] Allenby R.B.J.T., *Rings, Fields and Groups*, Edward Arnold, 1983.

[2] Arnaudiès J.M., Bertin J., *Groupes, Algèbres et Géométrie*, T.1, Ellipses, 1993.

[3] Arnaudiès J.M., Fraysse H., *Cours de Mathématiques-1, Algèbre*, Dunod, 1987.

[4] Arnaudiès J.M., Fraysse H., *Cours de Mathématiques-2, Analyse*, Dunod, 1988.

[5] Artin E., *Galois Theory*, Notre Dame Press, 1959.

[6] Bell E.T., *Men of Mathematics* (2 vol.) Penguin, Harmondsworth, Middlesex, 1965.

[7] Blanchard A., *Les corps non commutatifs*, PUF., 1972.

[8] Bourbaki N., *Théorie des ensembles*, Hermann, 1970.

[9] Bourbaki N., *Algèbre*, chap. 1 à 3, Hermann, 1970.

[10] Bourbaki N., *Eléments d'histoire des Mathémathiques*, Hermann, Paris, 1969.

[11] Bourgne R., Azra J.-P., *Ecrits et Mémoires mathématiques d'Evariste Galois*, Editions Jacques Gabay, 1997.

[12] Calais J., *Éléments de théorie des groupes*, PUF, 1984 (3ème éd. 1998).

[13] Calais J., *Anneaux-Corps, Vol. 1, Éléments de théorie des anneaux*, PUF, 2002. Réédition Ellipses, 2005.

[14] Carrega J-C., *Théorie des corps - La règle et le compas*, Hermann, 1981.

[15] Chih-Han Sah, *Abstract algebra*, Academic Press, 1967.

[16] Cohn P.M., *Algebra, Vol. 1*, John Wiley and Sons, 1974.

[17] Cohn P.M., *Algebra, Vol. 2*, John Wiley and Sons, 1977.

[18] Descombes R., Eléments de théorie des nombres, PUF, 1986.

[19] Dixmier J., *Topologie générale* , PUF, 1981.

[20] Eisenbud D., *Commutative Algebra with a View Toward Algebric Geometry*, Springer-Verlag, 1995.

[21] Ellis G., *Rings and Fields*, Carendon Press, 1992.

[22] Fresnel J., *Algèbre des matrices*, Hermann, 1997.

[23] Fulton W., *Algebraic Curves*, Benjamin, Inc., 1969

[24] Gauss C.F., *Disquisitiones Arithmeticae*, Yale University Press, New Haven, 1966.

[25] Gostiaux B., *Géométrie affine*, PUF 1992.

[26] Greub W.H., *Linear Algebra*, Springer-Verlag, Third Edition 1967.

[27] Hardy G.H., *A course of Pure Mathematics*, Cambridge, 1960.

[28] Hardy G.H. and Wright E.M., *An introduction to the Theory of Numbers*, Oxford, 1962.

[29] Jacobson N., *Basic Algebra I*, W.H. Freeman and company, 1974.

[30] Jacobson N., *Basic Algebra II*, W.H. Freeman and company, 1980.

[31] Kaplansky I., *Fields and Rings*, The University of Chicago Press, 1969.

[32] Klein F., *Famous Problems and other monographs*, Chelsa, 1962.

[33] Lang S., *Algebra*, Addison-Wesley, 1967.

[34] Lelong-Ferrand J., Arnaudiès J.-M., *Cours de mathématiques, tome 2 : Analyse*, Dunod, 1972.

[35] Naudin P., Quitté C., *Algorithmique algébrique*, Masson, 1992.

[36] Perrin D., *Cours d'Algèbre*, Ellipses, 1996.

[37] Ribenboim P., *Algebraic Numbers*, Wiley-Interscience, 1972.

[38] Ribenboim P., *L'arithmétique des corps*, Hermann, 1972.

[39] Ribenboim P., *Nombres Premiers : mystères et records*, PUF, 1994.

[40] Roman S., *Field Theory*, Springer-Verlag, 1995.

[41] Rotman J., *Galois Theory*, Springer-Verlag, 1990.

[42] Samuel P., *Théorie algébrique des nombres*, Hermann, 1967.

[43] Serre J-P., *Cours d'arithmétique* Collection SUP, PUF, 1970.

[44] Stewart I.N. and Tall D.O., *Algebraic Number Theory*, Chapman and Hall, 1979.

[45] Stewart I., *Galois Theory*, Chapman and Hall, 1973.

[46] Taton R., *Etudes d'histoires des Sciences*, Brepols Publishers n.v., Turnhout, Belgium, 2000.

[47] Tits J., *Groupes Finis Simples Sporadiques*, Séminaire Bourbaki 22ième année, 1969/70, no 375.

[48] Toti Rigatelli L., Evariste Galois 1811-1832, Birkhäuser Verlag, 1996.

Index

La collection Mathématiques à l'Université se propose de mettre à la disposition des étudiants de troisième, quatrième et cinquième années d'études supérieures en mathématiques des ouvrages couvrant l'essentiel des programmes actuels des universités françaises. Certains de ces ouvrages pourront être utiles aussi aux étudiants qui préparent le CAPES ou l'agrégation, ainsi qu'aux élèves des grandes écoles.
Nous avons voulu rendre ces livres accessibles à tous : les sujets traités sont présentés de manière simple et progressive, tout en respectant scrupuleusement la rigueur mathématique. Chaque volume comporte un exposé du cours avec des démonstrations détaillées de tous les résultats essentiels et de nombreux exercices. Les auteurs de ces ouvrages ont tous une grande expérience de l'enseignement des mathématiques au niveau supérieur.

Ce livre sur les Extensions de corps, incluant la Théorie de Galois, est une suite logique de l'ouvrage du même auteur, *Éléments de théorie des anneaux* dans la même collection. Il fait naturellement référence au livre *Éléments de théorie des groupes* publié aux Presses Universitaires de France, en raison du rôle important des groupes en Théorie de Galois.

Ces trois ouvrages constituent un ensemble cohérent de connaissances de base, en Algèbre générale, pour un étudiant se dirigeant vers la préparation à l'agrégation ou vers un master recherche, en mathématiques.

9 782729 827809

ISBN 2-7298-2780-3