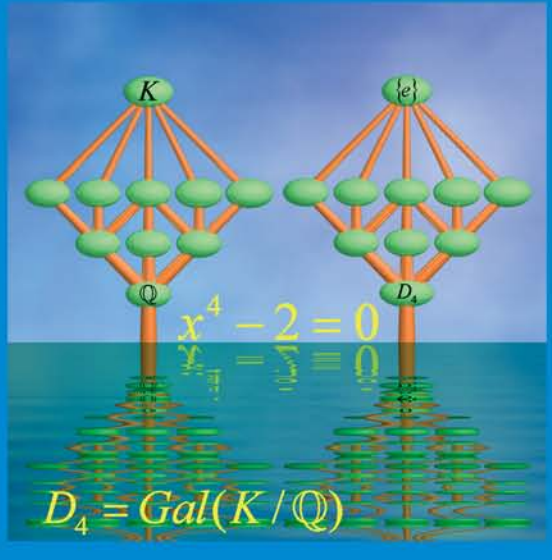
COLLECTION ENSEIGNEMENT SUP //// Mathématiques

L3M1

Algèbre I

GROUPES, CORPS ET THÉORIE DE GALOIS



Daniel Guin et Thomas Hausberger

EDP SCIENCES

ALGÈBRE

Tome 1

GROUPES, CORPS ET THÉORIE DE GALOIS

Daniel Guin – Thomas Hausberger

Collection dirigée par Daniel Guin

EDP SCIENCES

17, avenue du Hoggar
Parc d'activités de Courtabœuf, BP 112
91944 Les Ulis Cedex A, France

TABLE DES MATIÈRES

Première partie

GROUPES

I

GÉNÉRALITÉS SUR LES GROUPES

I.1. Définitions — exemples

Définition I.1.1. **Un groupe est la donnée d'un ensemble non vide G et d'une loi de composition interne**

$$G \times G \longrightarrow G$$

$$(x, y) \longmapsto x * y$$

vérifiant les propriétés suivantes :

(i) $\forall\ x, y, z \in G,\ (x * y) * z = x * (y * z)$

(ii) $\exists\ e \in G,\ tel\ que\ \ \forall\ x \in G, x * e = e * x = x$

(iii) $\forall\ x \in G, \exists\ \overline{x} \in G\ tel\ que\ \ x * \overline{x} = \overline{x} * x = e.$

La propriété (i) est l'**associativité** de la loi ; l'élément e, dont l'existence est assurée par la propriété (ii), est l'élément **neutre** pour la loi ; l'élément $\overline{x}$ est appelé élément **symétrique** de x.

Remarques I.1.1.

a) Cet ensemble de propriétés est redondant. Les propriétés (i), (ii), (iii) sont impliquées par les propriétés (i), (ii)', (iii)' avec :

(ii)' $\exists\ e \in G$ tel que $\forall x \in G, e * x = x$ (élément neutre à gauche)

(iii)' $\forall\ x \in G, \exists\ \overline{x} \in G$ tel que $\overline{x} * x = e$ (élément symétrique à gauche).

En effet, en appliquant deux fois la propriété (iii)', on a

$$\forall x, \exists\, \overline{\overline{x}} \in G \text{ tel que } \overline{\overline{x}} * \overline{x} = e$$

d'où

$$x * \overline{x} = e * (x * \overline{x}) = (\overline{\overline{x}} * \overline{x}) * (x * \overline{x}) = \overline{\overline{x}} * (\overline{x} * x) * \overline{x} = \overline{\overline{x}} * e * \overline{x} = \overline{\overline{x}} * \overline{x} = e.$$

De même,

$$x = e * x = (x * \overline{x}) * x = x * (\overline{x} * x) = x * e.$$

b) L'élément neutre est unique. Pour tout élément x de G, l'élément symétrique $\overline{x}$ est unique.

En effet, soient e' un autre élément neutre et $\overline{x}'$ un autre élément symétrique de x. On a

$$e' = e * e' = e$$

et

$$\overline{x} = \overline{x} * e = \overline{x} * (x * \overline{x}') = (\overline{x} * x) * \overline{x}' = e * \overline{x}' = \overline{x}'.$$

c) Pour tout $x, y, z \in G$, de l'unicité de l'élément symétrique on déduit que

$$\overline{x * y} = \overline{y} * \overline{x}$$

(on notera le changement de l'ordre dans l'écriture des éléments) et, en multipliant à gauche (suivant la loi $*$) par l'élément $\overline{x}$ les deux termes de la première égalité ci-dessous, on a

$$(x * y = x * z) \Leftrightarrow (y = z) \text{ (simplification)}.$$

d) On remarquera qu'un groupe est la donnée d'un ensemble **et** d'une loi de composition interne définie sur cet ensemble, vérifiant les axiomes (i), (ii), (iii). On verra en effet (TR.I.B remarque VI.2.3) que sur tout ensemble on peut définir une loi de composition interne qui le munisse d'une structure de groupe ; il y en a en général plusieurs, voire une infinité si l'ensemble est infini. Par conséquent, une expression du type « un groupe est un ensemble sur lequel il existe une loi de composition interne vérifiant les axiomes (i), (ii), (iii) » est synonyme de « un groupe est un ensemble », ce qui rendrait absurde l'introduction de la structure de groupe. Voir aussi la remarque (I.1.2.b) ci-dessous.

Exemples I.1.1.

a) L'ensemble des nombres entiers relatifs muni de l'addition est un groupe, noté $(\mathbb{Z}, +)$. L'ensemble des nombres rationnels non nuls, muni de la multiplication, est un groupe, noté $(\mathbb{Q}^*, \times)$. Il est évident qu'un ensemble réduit à un élément est muni d'une unique structure de groupe.

b) $(M_n(\mathbb{C}), +)$, où $M_n(\mathbb{C})$ désigne l'ensemble des matrices (n, n) à coefficients dans $\mathbb{C}$; $(GL_n(\mathbb{C}), \times)$, où $GL_n(\mathbb{C})$ désigne l'ensemble des matrices (n, n) inversibles à coefficients dans $\mathbb{C}$. Ce dernier groupe est appelé **groupe général linéaire**.

Table d'un groupe. Si le groupe G muni de la loi $*$ a un cardinal assez petit, il peut être commode de décrire explicitement la structure de groupe à l'aide d'un tableau. Plus précisément, si $G = \{x_0 = e, x_1, \ldots, x_n\}$, où e est l'élément neutre, on décrit la loi de composition interne $*$ par un tableau carré dans lequel le terme situé à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne est le terme $x_i * x_j$. Par exemple, sur l'ensemble $\{0, 1, 2, 3\}$ on définit les lois de composition interne $\bullet$ et $*$ par les tables suivantes :

$\bullet$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$*$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Pour montrer que ces lois munissent l'ensemble $\{0, 1, 2, 3\}$ de deux structures de groupe, il suffit de vérifier qu'elles satisfont aux axiomes de la définition (I.1.1).

On remarquera que chaque élément du groupe apparaît une fois et une fois seulement sur chaque ligne et chaque colonne. Ceci est dû au fait que, dans un groupe G, on a

$$\forall u \in G, \forall v \in G, \exists! x, \exists! y \text{ tels que } u * x = v \text{ et } y * u = v \ ;$$

ces éléments sont donnés par $x = \overline{u} * v$ et $y = v * \overline{u}$.

On prendra garde au fait que la condition « chaque élément de l'ensemble G apparaît une fois et une fois seulement dans chaque ligne et chaque colonne » dans un tableau comme ci-dessus est nécessaire mais pas suffisante pour que la loi interne définie par ce tableau munisse G d'une structure de groupe. En effet, considérons le tableau suivant :

$*$	0	1	2	3	4
0	0	1	2	3	4
1	1	0	4	2	3
2	2	3	0	4	1
3	3	4	1	0	2
4	4	2	3	1	0

Chaque élément de l'ensemble $\{0,1,2,3,4\}$ apparaît une fois et une fois seulement sur chaque ligne et chaque colonne, mais la loi $*$, ainsi définie, ne munit pas cet ensemble d'une structure de groupe, car elle n'est pas associative puisque $(1*2)*3 = 4*3 = 1$ et $1*(2*3) = 1*4 = 3$.

Remarques I.1.2.

a) On remarquera que sur une table comme ci-dessus, on détermine facilement l'existence d'un élément neutre ou d'un élément symétrique, mais que l'associativité de la loi n'apparaît pas de façon évidente.

b) L'exemple ci-dessus des lois $\bullet$ et $*$ définies sur l'ensemble $\{0,1,2,3\}$ montre qu'un ensemble peut être muni de plusieurs lois de composition interne qui définissent des structures de groupes différentes. D'où la nécessité, pour définir un groupe, de donner l'ensemble **et** sa loi de composition interne. Par conséquent, lorsqu'on voudra préciser que la structure de groupe considérée sur un ensemble G est donnée par une loi particulière, par exemple notée $*$, on notera le groupe $(G,*)$.

Exemples I.1.2.

a) Soit E un ensemble. On note S_E le groupe des applications bijectives de E dans E (ou permutations de E) pour la loi de composition interne définie par la composition des applications. Si $E = \{1,2,3\}$ les éléments de S_E sont

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

On notera ce groupe S_3 (écrire sa table), et de façon générale on notera S_n le groupe S_E pour $E = \{1,...,n\}$. Le groupe S_E est appelé **groupe des permutations** de l'ensemble E, ou **groupe symétrique**. Une étude détaillée de ce groupe est proposée dans le TR.I.A en fin de ce chapitre.

b) On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruences des entiers relatifs modulo n. Rappelons que si n est un entier positif, deux entiers relatifs p et q sont congrus modulo n si $p-q = kn$, $k \in \mathbb{Z}$. Ceci définit sur $\mathbb{Z}$ une relation d'équivalence dont $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes. En notant $cl(k)$ la classe de k, on vérifie aisément que l'addition définie par $cl(p) + cl(q) = cl(p+q)$ est indépendante du choix des représentants p et q et qu'elle munit $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe, dont $cl(0)$ est l'élément neutre et $cl(-x)$ est le symétrique de $cl(x)$.

c) On note D_4 le groupe des isométries du carré pour la composition des applications. Les éléments de D_4 sont

I = identité
R_1 = la rotation de centre 0 (le centre du carré) et d'angle $\pi/2$
R_2 = la rotation de centre 0 (le centre du carré) et d'angle π
R_3 = la rotation de centre 0 (le centre du carré) et d'angle $3\pi/2$
H = la symétrie par rapport à l'axe de symétrie horizontal
V = la symétrie par rapport à l'axe de symétrie vertical
Δ_1 = la symétrie par rapport à la première diagonale
Δ_2 = symétrie par rapport à la deuxième diagonale

qui se composent suivant la table

	I	R_1	R_2	R_3	H	V	Δ_1	Δ_2
I	I	R_1	R_2	R_3	H	V	Δ_1	Δ_2
R_1	R_1	R_2	R_3	I	Δ_1	Δ_2	V	H
R_2	R_2	R_3	I	R_1	V	H	Δ_2	Δ_1
R_3	R_3	I	R_1	R_2	Δ_2	Δ_1	H	V
H	H	Δ_2	V	Δ_1	I	R_2	R_3	R_1
V	V	Δ_1	H	Δ_2	R_2	I	R_1	R_3
Δ_1	Δ_1	H	Δ_2	V	R_1	R_3	I	R_2
Δ_2	Δ_2	V	Δ_1	H	R_3	R_1	R_2	I

où les termes de cette table sont $x \circ y$ pour x dans la première colonne et y dans la première ligne.

Ce groupe fait partie d'une suite de groupes D_n, $n \geqslant 3$, appelés **groupes diédraux** (*cf.* TR.IV.A).

***Définition* I.1.2.** Si $(G, *)$ est un groupe tel que la loi $*$ satisfasse à la propriété

(iv) $\forall\, x, y \in G, x * y = y * x$,

le groupe $(G, *)$ *est dit* ***commutatif*** *ou encore* ***abélien***.

***Exemples* I.1.3.**

a) Les groupes $(\mathbb{Z}, +), (\mathbb{Q}^*, \times), (M_n(\mathbb{C}), +)$ sont abéliens.

b) Le groupe $(GL_n(\mathbb{C}), \times)$ ne l'est pas. On constate sur la table ci-dessus que le groupe D_4 n'est pas abélien.

***Proposition* I.1.1.** *Si* $\operatorname{card} E \geqslant 3$, *le groupe* S_E *n'est pas abélien.*

Démonstration. Soient x, y, z trois éléments distincts deux à deux dans E. On considère les deux transpositions τ_{xy} et τ_{yz} (on note τ_{ij} la permutation qui échange i et j), alors $\tau_{xy} \circ \tau_{yz} \neq \tau_{yz} \circ \tau_{xy}$. □

Attention. *En général, dans un goupe non abélien,* $(xy)^n \neq x^n y^n$, $n \in \mathbb{N}$. *Mais si* $xy = yx$, *alors* $(xy)^n = x^n y^n$, $n \in \mathbb{N}$.

Remarques I.1.3. Dans la suite, sauf mention contraire, on notera les lois de groupes multiplicativement $(x, y) \mapsto xy$, on les appellera produits, on notera x^{-1} l'élément symétrique de x qu'on appellera inverse de x, et on notera 1 l'élément neutre. Toutefois, si le groupe considéré est abélien, on notera sa loi additivement $(x, y) \mapsto x + y$, on l'appellera somme, on notera $-x$ l'élément symétrique de x qu'on appellera opposé de x, et on notera 0 l'élément neutre.

I.2. Sous-groupes — morphismes

A - Sous-groupes

Supposons qu'on connaisse le groupe $(\mathbb{Q}, +)$, mais qu'on n'ait pas défini d'addition sur $\mathbb{Z}$. Puisque $\mathbb{Z}$ est un sous-ensemble de $\mathbb{Q}$, on peut considérer l'addition de deux entiers dans $\mathbb{Q}$. Il est facile de vérifier que l'addition, dans $\mathbb{Q}$, de deux entiers est encore un entier. On définit ainsi une addition sur $\mathbb{Z}$, qui est une loi de composition interne.

De plus, quels que soient x, y, z des éléments de $\mathbb{Z}$, les éléments $(x + y) + z$ et $x + (y + z)$ sont égaux dans $\mathbb{Q}$ et appartiennent à $\mathbb{Z}$, ils sont donc égaux dans $\mathbb{Z}$. Autrement dit, l'associativité de la loi définie sur $\mathbb{Z}$ à partir de celle définie sur $\mathbb{Q}$ découle de l'associativité de la loi de $\mathbb{Q}$.

On vérifie de la même manière que 0, qui est l'élément neutre de $\mathbb{Q}$ pour l'addition, est aussi élément neutre pour l'addition dans $\mathbb{Z}$ et que, pour tout $x \in \mathbb{Z}$, $-x$, qui est le symétrique de x dans $\mathbb{Q}$, est aussi le symétrique de x dans $\mathbb{Z}$.

Autrement dit, ceci montre que la structure de groupe de $(\mathbb{Z}, +)$ est déduite de celle de $(\mathbb{Q}, +)$. On dit que $(\mathbb{Z}, +)$ est un **sous-groupe** de $(\mathbb{Q}, +)$.

Le lecteur pourra faire la même analyse en considérant l'ensemble $\mathbb{Z}[i] = \{a + ib | (a, b) \in \mathbb{Z}^2\}$, avec $i^2 = -1$, vu comme sous-ensemble de $(\mathbb{C}, +)$.

On cherche à formaliser cette situation au cas général d'un groupe $(G, *)$ et d'un sous-ensemble H de G. La loi de composition interne de G permet de définir une loi de composition sur H,

$$\forall (x, y) \in H \times H, \quad (x, y) \mapsto x * y.$$

C'est la loi **induite** sur H par celle de G.

Mais, par rapport à la situation de $\mathbb{Z}$ et $(\mathbb{Q},+)$ décrite ci-dessus, un premier écueil peut se présenter : l'élément $x*y$ appartient à G, mais peut ne pas appartenir à H, *i.e.* la loi n'est pas une loi de composition **interne** pour H. Par exemple, pour $G=(M_2(\mathbb{C}),+)$ et $H=GL_2(\mathbb{C})$, les éléments

$$x=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad y=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

appartiennent à H, $(x+y)$ appartient à G mais pas à H.

Même quand ce premier écueil est évité, il peut s'en présenter un second : pour un élément x de H, le symétrique $\overline{x}$, qui appartient à G, peut ne pas appartenir à H. Par exemple, pour $G=(\mathbb{Q}^*,\times)$ et $H=\mathbb{Z}^*$, la multiplication induite sur H par celle de G est une loi de composition interne pour H, mais l'inverse de 2 dans G n'appartient pas à H.

Pour pouvoir étendre la situation décrite pour $(\mathbb{Q},+)$ et $\mathbb{Z}$ à un groupe quelconque G et un sous-ensemble H, il faut donc que la loi induite sur H soit une loi de composition interne pour H, on dit que H est **stable pour la loi de** G, et que le symétrique, dans G, de tout élément de H appartienne à H, on dit que H est **stable par symétrique**. La proposition (I.2.1) ci-dessous montrera que ces conditions sont suffisantes.

Définition I.2.1. Un sous-ensemble non vide H d'un groupe G est un **sous-groupe** de G si, muni de la loi induite par celle de G, c'est un groupe.

Proposition I.2.1. *Un sous-ensemble non vide H d'un groupe G est un sous-groupe de G si et seulement si*

(i) $\forall\ (x,y)\in H\times H, xy\in H.$

(ii) $\forall\ x\in H, x^{-1}\in H.$

Démonstration. Si H est un sous-groupe de G, les assertions (i) et (ii) sont clairement vérifiées. Réciproquement, d'après l'assertion (i), la loi de G induit sur H une loi interne, et cette loi est associative pour la même raison que celle indiquée ci-dessus pour $(\mathbb{Q},+)$ et $\mathbb{Z}$. D'après (ii), pour tout élément x de H, on a $x^{-1}\in H$, d'où, d'après (i), $xx^{-1}\in H$. Mais xx^{-1} est l'élément neutre de G. On en déduit que l'élément neutre de G est aussi élément neutre de H. Par conséquent, H muni de la loi induite par celle de G est un groupe. □

Remarques I.2.1.

a) Le lecteur vérifiera que les deux assertions (i) et (ii) de la proposition (I.2.1) sont équivalentes à : $\forall (x,y) \in H \times H, xy^{-1} \in H$ et $e_G \in H$.

b) Un groupe G ayant au moins deux éléments admet au moins deux sous-groupes : G et le sous-groupe réduit à l'élément neutre.

c) Il est clair que si H est un sous-groupe d'un groupe G et si K est un sous-groupe de H, alors K est un sous-groupe de G.

Définition I.2.2. On appelle sous-groupe **propre** d'un groupe G tout sous-groupe distinct de G et de l'élément neutre.

Notation. Si H est un sous-groupe de G, on notera $H < G$.

Exemples I.2.1.

a) $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$.

b) $(\mathbb{Q}^*,\times) < (\mathbb{R}^*,\times) < (\mathbb{C}^*,\times)$.

c) Le groupe multiplicatif $\mathbb{U}$ des nombres complexes de module 1 est un sous-groupe de $(\mathbb{C}^*,\times)$.

d) Le groupe multiplicatif $\mathbb{U}_n$ des nombres complexes z tels que $z^n{=}1$ est un sous-groupe de $\mathbb{U}$.

e) Le groupe $GL(E)$ des automorphismes d'un k-espace vectoriel E est un sous-groupe de S_E.

f) Pour tout groupe G, on considère

$$Z(G) = \{g \in G, \forall x \in G, gx = xg\}.$$

C'est un sous-groupe de G, appelé le **centre** de G.

Exercice I.1.

1. Montrer que pour tout $n \geqslant 3$, on a $Z(S_n) = \{1\}$, où 1 est la permutation identité.

2. Montrer que les matrices

$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}, \quad \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix}, \quad \pm\begin{pmatrix}0&i\\i&0\end{pmatrix}, \quad \pm\begin{pmatrix}i&0\\0&-i\end{pmatrix}$$

où i est un nombre complexe tel que $i^2 = -1$, forment un groupe pour la multiplication des matrices. (On montrera que c'est un sous-groupe du groupe $GL_2(\mathbb{C})$.

On remarquera que démontrer directement que cet ensemble de matrices est un groupe impose des calculs longs et fastidieux, en particulier pour vérifier l'associativité, d'où l'intéret de la méthode proposée, qui est fréquemment utilisée.)

On note ce groupe $\mathcal{H}$ et on l'appelle **groupe quaternionique**.

Proposition I.2.2. *Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\}$, pour n parcourant $\mathbb{N}$.*

Démonstration. Il est clair que les $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\}$, pour n parcourant $\mathbb{N}$, sont des sous-groupes de $\mathbb{Z}$. Réciproquement, soit H un sous-groupe de $\mathbb{Z}$. Si $H = 0$, alors $H = n\mathbb{Z}$ avec $n = 0$. Si H est non nul, son intersection avec $\mathbb{N}^*$ est un ensemble non vide d'entiers positifs et possède donc un plus petit élément n. Soit x un élément quelconque de H ; la division euclidienne de x par n donne $x = ny + k$, avec $0 \leqslant k < n$. Comme $k = x - ny$ appartient à H, k est nul par définition de l'entier n. On en déduit que $H = n\mathbb{Z}$. □

Proposition I.2.3. *Soient G un groupe, I un ensemble non vide et $\{H_i\}_{i\in I}$ une famille de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Démonstration. Laissée au lecteur à titre d'exercice. □

Attention. *Une réunion de sous-groupes d'un groupe G n'est, en général, pas un sous-groupe de G.* Par exemple, on vérifiera que $3\mathbb{Z}$ et $5\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$, mais que $3 + 5 = 8$ n'appartient pas à $3\mathbb{Z} \cup 5\mathbb{Z}$.

Exercice I.2. Montrer que si A et B sont des sous-groupes d'un groupe G, $A \cup B$ est un sous-groupe de G si et seulement si A est contenu dans B ou B est contenu dans A.

B - Sous-groupes engendrés

Il est facile de voir que dans le groupe $\mathbb{Z}/n\mathbb{Z}$ (exemple I.1.2.b), tout élément $cl(k)$ est la somme $cl(1) + \cdots + cl(1)$, k-fois. Autrement dit, l'élément $cl(1)$ **engendre** le groupe $\mathbb{Z}/n\mathbb{Z}$.

Définition I.2.3. Soient G un groupe et S une partie de G. On appelle **sous-groupe engendré par** S, et on note $\langle S\rangle$, le plus petit (pour la relation d'inclusion) sous-groupe de G contenant S.

Proposition I.2.4. *C'est l'intersection de tous les sous-groupes de G qui contiennent S.* □

Proposition I.2.5. *Soient G un groupe et S une partie non vide de G. On a*

$$\langle S\rangle = \{x_1 \cdots x_n,\ n \in \mathbb{N}^*, x_i \in S \text{ où } x_i^{-1} \in S,\ \forall i,\ 1 \leqslant i \leqslant n\}.$$

Démonstration. Notons $H = \{\prod_{i=1}^n x_i,\ n \in \mathbb{N}^*,\ x_i \in S \text{ où } x_i^{-1} \in S,\ \forall i,\ 1 \leqslant i \leqslant n\}$. On remarque que S est contenu dans H. Soient $x = x_1 \dots x_n$ et $y = y_1 \dots y_p$ des éléments de H, alors $xy^{-1} = x_1 \dots x_n y_p^{-1} \dots y_1^{-1}$ appartient à H, ce qui prouve que H est un sous-groupe de G. D'où $\langle S\rangle$ est contenu dans H. Il est clair que tout sous-groupe de G contenant S contient H, d'où $\langle S\rangle = H$. □

Cas particulier important. Si $S = \{x\}$ pour $x \in G$, on note alors $\langle x\rangle$ le sous-groupe engendré par x et il est clair que $\langle x\rangle = \{x^n, n \in \mathbb{Z}\}$.

Remarque I.2.2. Si la loi de G est notée additivement, on a

$$\langle S\rangle = \{x_1 + \cdots + x_n, n \in \mathbb{N}^*, \pm x_i \in S, \forall i, 1 \leqslant i \leqslant n\}$$

d'où $\langle x\rangle = \{nx, n \in \mathbb{Z}\}$.

Définition I.2.4. Si S est une partie non vide d'un groupe G, telle que $\langle S\rangle = G$, on dit que S est une **partie génératrice** de G, ou que S est un ensemble de **générateurs** de G, ou que S **engendre** G.

Exemple I.2.2. Dans le groupe S_3, on a

$$\sigma_1^2 = \sigma_2,\ \sigma_1^3 = e,\ \sigma_1 \circ \tau_3 = \tau_2,\ \tau_3 \circ \sigma_1 = \tau_1$$

d'où $\langle \sigma_1, \tau_3\rangle = S_3$.

Exercice I.3.

1. En examinant la table de l'exemple (I.1.2.c), montrer que $D_4 = \langle R_1, H\rangle$ ou $D_4 = \langle R_1, V\rangle$ ou $D_4 = \langle R_1, \Delta_1\rangle$ ou $D_4 = \langle R_1, \Delta_2\rangle$.

2. Montrer qu'un sous-groupe de $(\mathbb{R}, +)$ est, ou bien dense dans $\mathbb{R}$, ou bien engendré par un élément a de $\mathbb{R}$.

Remarque I.2.3. L'exemple ci-dessus montre qu'une partie génératrice d'un groupe n'est, en général, pas unique. En particulier $G = \langle G\rangle$.

C - Ordre d'un groupe, d'un élément

***Définition* I.2.5.** Un groupe G est dit fini s'il n'a qu'un nombre fini d'éléments. Dans ce cas, le cardinal de G s'appelle l'**ordre** du groupe G et est noté $|G|$.

Soient G un groupe et x un élément de G. On appelle **ordre** de x, qu'on note $o(x)$, le cardinal de $\langle x \rangle$. Si ce cardinal est infini, on dit que x est d'ordre infini.

***Remarques* I.2.4.**

a) Soient G un groupe fini et x un élément de G, alors $o(x) \leqslant |G|$.

b) Dans tout groupe G, l'élément neutre est le seul élément d'ordre 1.

c) Dans $(\mathbb{Z}, +)$, tous les éléments non nuls sont d'ordre infini.

***Exemples* I.2.3.**

a) Les groupes D_4 et $\mathcal{H}$ sont d'ordre 8.

b) Dans le groupe S_3, les éléments τ_1, τ_2, τ_3 sont d'ordre 2, les éléments σ_1 et σ_2 d'ordre 3. Le groupe S_3 est d'ordre 6.
Plus généralement, pour tout $n \geqslant 2$, le groupe S_n est d'ordre $n!$.

c) Dans le groupe D_4, les éléments R_1 et R_3 sont d'ordre 4, les éléments H, V, Δ_1, Δ_2 sont d'ordre 2.

***Proposition* I.2.6.** *Soient G un groupe et x un élément d'ordre fini de G. Alors $o(x)$ est le plus petit entier positif s tel que $x^s = 1_G$.*

Démonstration. Si pour tout i et j dans $\mathbb{Z}$, $i \neq j$, on a $x^i \neq x^j$, alors l'ordre de $\langle x \rangle$ est infini, ce qui est contraire à l'hypothèse. Donc il existe $p > q$ tel que $x^p = x^q$, *i.e.* $x^{p-q} = 1_G$, avec $p - q > 0$. L'ensemble $\{s \in \mathbb{N}^*, x^s = 1_G\}$ est un ensemble non vide d'entiers positifs, il admet donc un plus petit élément n. Alors $\langle x \rangle = \{1_G, x, \ldots, x^{n-1}\}$, et $o(x) = n$. □

D - Morphismes

Étudier un groupe, c'est déterminer les propriétés algébriques qui sont attachées à la loi définissant la structure de groupe. L'un des moyens les plus efficaces pour ce faire est de comparer le groupe donné à un autre groupe dont on connaît déjà les propriétés. Si H est un sous-groupe d'un groupe G, le produit des éléments de H est le même, que ces éléments soient considérés dans H ou dans G.

Il est donc simple de comparer les structures des groupes G et H. Par contre, si deux groupes G et G' ne sont pas contenus l'un dans l'autre, ou ne sont pas sous-groupes d'un même groupe, on ne peut plus faire cette comparaison. On est alors amené à considérer une application $f : G \to G'$ qui permette de se ramener à la situation précédente, c'est-à-dire telle que $f(G)$ soit un sous-groupe de G'. Pour cela, il faut que l'application f soit compatible avec la structure de groupe, donc compatible avec les lois qui définissent la structure. C'est la notion de **morphisme**.

Définition I.2.6. Soient $(G, .)$ et $(G', *)$ deux groupes. Un **morphisme** (ou homomorphisme) **de groupes** de G dans G' est une application $f : G \to G'$ vérifiant :

$$\forall\ (x, y) \in G \times G,\ f(x.y) = f(x) * f(y).$$

Notation. On note $Hom(G, G')$ l'ensemble des morphismes de groupes de G dans G'. On note $End(G)$ l'ensemble des morphismes de groupes de G dans lui-même, qu'on appelle **endomorphismes** de G.

Proposition I.2.7. *Tout élément f de $Hom(G, G')$ vérifie les propriétés suivantes :*

(i) $f(1_G) = 1_{G'}$

(ii) $f(x^{-1}) = f(x)^{-1}$ ***pour tout élément*** x ***de*** G

(iii) $H < G \Rightarrow f(H) < G'$

(iv) $H' < G' \Rightarrow f^{-1}(H') < G$ ***avec*** $f^{-1}(H') = \{x \in G, f(x) \in H'\}$.

Démonstration. (i). Notons 1_G et $1_{G'}$ les éléments neutres respectifs de G et G'. Soit x un élément de G, on a $f(x) = f(x1_G) = f(x)f(1_G)$. Or $f(x) = f(x)1_{G'}$, d'où $f(1_G) = 1_{G'}$.

(ii). Pour tout x de G on a $1_{G'} = f(1_G) = f(xx^{-1}) = f(x)f(x^{-1})$, d'où $f(x^{-1}) = f(x)^{-1}$.

(iii). Pour tous y_1 et y_2 dans $f(H)$, il existe x_1 et x_2 dans H tels que $f(x_1) = y_1$ et $f(x_2) = y_2$. D'où $y_1y_2^{-1} = f(x_1)f(x_2)^{-1} = f(x_1)f(x_2^{-1}) = f(x_1x_2^{-1})$ qui appartient à $f(H)$.

(iv). Pour tous x et y dans $f^{-1}(H')$ on a $f(x)$ et $f(y)$ dans H', d'où $f(xy^{-1}) = f(x)f(y)^{-1}$ appartient à H', et xy^{-1} appartient à $f^{-1}(H')$. □

Définition - Proposition I.2.8. *Pour tout élément f de $Hom(G,G')$, $f(G)$ est un sous-groupe de G' appelé image de f et noté $Im(f)$; $f^{-1}(\{1_{G'}\})$ est un sous-groupe de G appelé noyau de f et noté $Ker(f)$.* □

Proposition I.2.9. *Si $f : G \to G'$ est un morphisme de groupes, on a*

$$[f \textbf{ injectif}] \Leftrightarrow [Ker(f) = \{1_G\}]$$

$$[f \textbf{ surjectif}] \Leftrightarrow [Im(f) = G'].$$

Démonstration. On a

$$[f \text{ injectif}] \Leftrightarrow [\forall (x,y) \in G \times G,\ (f(x) = f(y)) \Rightarrow (x = y)].$$

Si f est injectif et $f(x) = 1_{G'} = f(1_G)$, alors $x = 1_G$ et $Ker(f) = \{1_G\}$.

Réciproquement, si $f(x) = f(y)$, on a

$$1_{G'} = (f(x))^{-1} f(y) = f(x^{-1}) f(y) = f(x^{-1}y),$$

d'où $x^{-1}y \in Ker(f)$. Si $Ker(f) = \{1_G\}$, alors $x = y$ et f est injective.

La deuxième assertion est évidente. □

Exemples I.2.4.

a) Si $H < G$, alors l'injection canonique $i : H \hookrightarrow G$ est un morphisme.

b) L'application de $GL_n(\mathbb{C})$ dans $\mathbb{C}^*$, qui à une matrice associe son déterminant, est un morphisme de groupes multiplicatifs dont le noyau, noté $SL_n(\mathbb{C})$, est appelé **groupe spécial linéaire**. (On peut remplacer $\mathbb{C}$ par un corps commutatif quelconque.)

Proposition I.2.10. *Soient G, G', G'' trois groupes. Alors pour tout f de $Hom(G,G')$ et tout g de $Hom(G',G'')$, $g \circ f$ appartient à $Hom(G,G'')$.*

Démonstration. Le lecteur vérifiera facilement que l'application de G dans G'' definie par $g \circ f$ est un morphisme de groupes. □

Définition I.2.7. Un élément f de $Hom(G,G')$ est un **isomorphisme** s'il existe un morphisme réciproque g, *i.e.* un élément g de $Hom(G',G)$ tel que $g \circ f = id_G$ et $f \circ g = id_{G'}$.

Proposition I.2.11. *Soient G et G' deux groupes et $f : G \to G'$ une application.*

(i) *f est un isomorphisme si et seulement si f est un morphisme bijectif*

(ii) *Si f est un isomorphisme, l'application réciproque f^{-1} est un isomorphisme.*

Démonstration. (i). Il est clair qu'un isomorphisme est une application bijective. Il suffit donc de démontrer que si f est un morphisme bijectif, l'application réciproque f^{-1} est un morphisme de groupes. Pour tous x' et y' dans G', il existe x et y uniques dans G tels que $x' = f(x)$ et $y' = f(y)$. On a $f^{-1}(x'y') = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(x')f^{-1}(y')$.

(ii). Évident. □

Attention. *Une application bijective n'est pas nécessairement un isomorphisme.* Le lecteur vérifiera que, pour tout groupe non trivial G et pour tout $g \neq 1_G$ dans G, l'application $f_g : G \to G$ définie par $f_g(x) = gx$ est bijective, mais n'est pas un morphisme de groupes.

Définition I.2.8. Deux groupes G et G' sont **isomorphes** s'il existe un isomorphisme f de G sur G'.

Cette notion est extrêmement importante, car deux groupes isomorphes ont exactement les **mêmes** propriétés algébriques.

Notation. Si deux groupes G et G' sont isomorphes, on note $G \simeq G'$. Les éléments de $End(G)$ qui sont des isomorphismes sont appelés **automorphismes** de G. Ils forment un groupe pour la composition des applications, noté $Aut(G)$.

Remarques I.2.5.

a) Il est clair d'après les propositions (I.2.10) et (I.2.11) que la composition des applications munit $Aut(G)$ d'une structure de groupe.

b) Si deux groupes sont isomorphes, ils ont même ordre.

Attention. *La réciproque est fausse* (*cf.* exercice I.4 ci-dessous).

c) Si f est un isomorphisme d'un groupe G sur un groupe G', pour tout élément x de G, les éléments x et $f(x)$ ont même ordre.

d) Si $f : G \to G'$ est un morphisme injectif, alors G est isomorphe à $f(G)$. Ceci permet « d'identifier » G au sous-groupe $f(G)$ de G'.

e) Soient G un groupe et G' un ensemble. Si $f : G \to G'$ est une application bijective, on peut munir G' d'une structure de groupe telle que f soit un isomorphisme, et cela de manière unique.

En effet,

$$\forall x' \in G',\ \forall y' \in G',\ \exists! x \in G,\ \exists! y \in G,\ \text{tels que } x' = f(x), y' = f(y).$$

On pose alors $x'y' = f(xy)$; ceci définit sur G' une loi de composition interne telle que :

$$\forall x \in G, \forall y \in G, f(xy) = f(x)f(y).$$

On vérifie facilement que cette loi est associative, que $f(1_G)$ est élément neutre et que $x'^{-1} = f(x^{-1})$. L'ensemble G' est donc muni d'une structure de groupe et, puisque f est un morphisme bijectif, c'est un isomorphisme.

Évidemment, on obtient un résultat analogue si G est un ensemble et G' un groupe, en considérant l'application f^{-1}.

f) Soient G un groupe, G' un ensemble et $f : G \longrightarrow G'$ une application. L'ensemble $f(G)$ muni de la loi $\star$ définie par $f(x) \star f(y) = f(xy)$ est un groupe. Par exemple $f : \mathbb{Z}^2 \longrightarrow \mathbb{C}$ définie par $f((a, b)) = a + ib$.

***Exemples* I.2.5.**

a) Soit E un k-espace vectoriel de dimension n. Alors les groupes $GL(E)$ (*cf.* exemple I.2.1.e) et $GL_n(k)$ (*cf.* exemple I.1.1.b) sont isomorphes par l'isomorphisme qui, à tout élément φ de $GL(E)$, associe la matrice $M(\varphi)$ de φ dans une base fixée de E.

b) **Automorphismes intérieurs**. Soient G un groupe et g un élément de G. L'application

$$\varphi_g :\ G \longrightarrow G, \quad x \longmapsto gxg^{-1}$$

est un automorphisme de G, appelé **automorphisme intérieur** défini par g. On note $Int(G)$ l'ensemble $\{\varphi_g,\ g \in G\}$ des automorphismes intérieurs de G. C'est un sous-groupe de $Aut(G)$. On remarquera que, en général, on peut avoir $\varphi_g = \varphi_{g'}$ avec $g \neq g'$, si $g^{-1}g' \in Z(G)$, d'où $|Int(G)| \leqslant |G|$.

***Remarque* I.2.6.** En général, pour un groupe G, $Int(G)$ est un sous-groupe strict de $Aut(G)$. Mais pour certains groupes, on peut avoir $Int(G) = Aut(G)$ (comme, par exemple, pour les groupes S_n, $n \neq 6$, (*cf.* TR.II.B)).

***Exercice* I.4.**

1. Montrer que l'ensemble $\{0, 1, 2, 3\}$ muni de la loi $\bullet$ définie en (1.4) est un groupe isomorphe au groupe $\mathbb{Z}/4\mathbb{Z}$ (*cf.* exemple I.1.2.b).

2. Montrer que les groupes D_4 et $\mathcal{H}$, qui sont tous les deux d'ordre 8, ne sont pas isomorphes. (Utiliser la remarque (I.2.5.c).)

3. Montrer que les matrices

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \begin{pmatrix}-1&-1\\1&0\end{pmatrix},\quad \begin{pmatrix}0&1\\-1&-1\end{pmatrix}$$
$$\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \begin{pmatrix}1&0\\-1&-1\end{pmatrix},\quad \begin{pmatrix}-1&-1\\0&1\end{pmatrix}$$

forment un sous-groupe de $GL_2(\mathbb{R})$, isomorphe au groupe $GL_2(\mathbb{Z}/2\mathbb{Z})$.

***Théorème I.2.1* (de Cayley).** *Tout groupe G est isomorphe à un sous-groupe du groupe S_G de ses permutations.*

Démonstration. Soit g un élément de G. L'application $f_g : G \to G$ définie par $f_g(x) = gx$ est bijective, c'est donc une permutation de E. L'application

$$F : G \longrightarrow S_G, \quad g \longmapsto f_g$$

est un morphisme de groupes. En effet $F(gh)$ est l'application de G dans G qui à x associe ghx. Comme $ghx = g(hx)$, cet élément est aussi l'image de x par l'application $F(g) \circ F(h)$. On en déduit que $F(gh) = F(g) \circ F(h)$.

De plus, F est injective. En effet, si $F(g)$ est égal à l'identité, pour tout x de G on a $gx = x$, d'où $g = 1_G$, où 1_G est l'élément neutre de G, et $Ker(F) = \{1_G\}$.

Par conséquent, F est un isomorphisme de G sur son image $F(G)$, qui est un sous-groupe de S_G. □

***Remarque* I.2.7.** On verra au TR.I.A que si deux ensembles E et F sont équipotents, les groupes S_E et S_F sont isomorphes. Donc, si G est un groupe d'ordre n, le théorème de Cayley montre que G est isomorphe à un sous-groupe de S_n. Mais l'entier n n'est pas forcément minimal pour cette propriété, *i.e.* on peut avoir $p < n$ et G isomorphe à un sous-groupe de S_p (*cf.* exercice I.5 ci-dessous). Comme on sait que $|S_n| = n!$, on comprend l'importance de trouver un p inférieur à n tel que G soit isomorphe à un sous-groupe de S_p.

Exercice I.5.

1. Montrer que le groupe D_4 est isomorphe à un sous-groupe de S_4.

2. En comptant le nombre d'éléments d'ordre 4 de S_4, montrer qu'ils n'ont pas tous même carré.

En déduire que $\mathcal{H}$ n'est pas isomorphe à un sous-groupe de S_4.

Montrer, par la même méthode, que $\mathcal{H}$ n'est pas isomorphe à un sous-groupe de S_7. Par conséquent, l'entier n minimal tel que $\mathcal{H}$ soit isomorphe à un sous-groupe de S_n est $n = 8 = |\mathcal{H}|$.

I.3. Produit direct de groupes

A - Produit de sous-groupes d'un groupe

Soient G un groupe, H et K deux sous-groupes de G. On considère les parties de G, $HK = \{hk, h \in H, k \in K\}$ et $KH = \{kh, k \in K, h \in H\}$, où le produit est la loi de G.

***Remarque* I.3.1.** En général, ces deux parties de G ne sont pas égales et ne sont pas des sous-groupes de G. En effet, considérons dans S_3 les sous-groupes $H = \langle \tau_1 \rangle$ et $K = \langle \tau_2 \rangle$: alors $HK = \{e, \tau_1, \tau_2, \tau_1 \circ \tau_2\}$, $KH = \{e, \tau_1, \tau_2, \tau_2 \circ \tau_1\}$ et, puisque $\tau_1 \circ \tau_2 \neq \tau_2 \circ \tau_1$, $HK \neq HK$; de plus $(\tau_1 \circ \tau_2)^{-1} = \tau_2 \circ \tau_1 \notin HK$ et $(\tau_2 \circ \tau_1)^{-1} = \tau_1 \circ \tau_2 \notin KH$, donc HK et KH ne sont pas des sous-groupes de S_3.

***Proposition* I.3.1.** *Soient G un groupe, H et K deux sous-groupes de G. Alors HK est un sous-groupe de G si et seulement si $HK = KH$.*

Démonstration. Remarquons d'abord que HK et KH ne sont pas vides puisqu'ils contiennent l'élément neutre. Si HK est un sous-groupe de G, pour $h \in H$ et $k \in K$, on a $kh = (h^{-1}k^{-1})^{-1} \in HK$, donc KH est contenu dans HK. Soit $z \in HK$, alors $z^{-1} = hk$, et $z = k^{-1}h^{-1} \in KH$, d'où HK est contenu dans KH, et $HK = KH$.

Réciproquement, si $HK = KH$, soient h et h' dans H, k et k' dans K ; alors, $(hk)(h'k')^{-1} = hkk'^{-1}h'^{-1}$. Or, $kk'^{-1}h'^{-1} \in KH = HK$, donc il existe $h'' \in H$ et $k'' \in K$ tels que $kk'^{-1}h'^{-1} = h''k''$, d'où $(hk)(h'k')^{-1} = hh''k'' \in HK$, et HK est un sous-groupe, ainsi que KH. □

***Remarque* I.3.2.** Si G est abélien, pour tous sous-groupes H et K, HK est un sous-groupe de G.

***Exercice* I.6.** Montrer que si HK est un sous-groupe de G, c'est le sous-groupe engendré par $H \cup K$.

***Proposition* I.3.2.** *Soient G un groupe et $\{H_i\}_{1 \leqslant i \leqslant n}$ une famille finie de sous-groupes de G. Si, quels que soient i et j, $1 \leqslant i < j \leqslant n$, H_iH_j est un sous-groupe de G, alors*

$$H_1H_2 \dots H_n = \{x_1 \dots x_n,\ x_i \in H_i, 1 \leqslant i \leqslant n\}$$

est un sous-groupe de G.

Démonstration. Le lecteur montrera, par un raisonnement par récurrence, que cette proposition est un corollaire immédiat de la proposition (I.3.1). □

B - Produit direct de groupes

Proposition I.3.3. *Soient G_1 et G_2 deux groupes d'éléments neutres respectifs 1_{G_1} et 1_{G_2}. Alors l'ensemble $G_1 \times G_2$ muni de la loi de composition interne définie par*

$$((x_1, x_2), (y_1, y_2)) \longmapsto (x_1 y_1, x_2 y_2)$$

est un groupe dont l'élément neutre est $(1_{G_1}, 1_{G_2})$, l'inverse de l'élément (x_1, x_2) étant l'élément (x_1^{-1}, x_2^{-1}).

La démonstration est laissée au lecteur à titre d'exercice. □

Définition I.3.1. Le groupe défini ci-dessus est le **produit direct** des groupes G_1 et G_2, noté $G_1 \times G_2$.

Les projections canoniques

$$p_1 : G_1 \times G_2 \longrightarrow G_1, \quad (x_1, x_2) \longmapsto x_1$$

$$p_2 : G_1 \times G_2 \longrightarrow G_2, \quad (x_1, x_2) \longmapsto x_2$$

sont des morphismes surjectifs, et les injections canoniques

$$q_1 : G_1 \longrightarrow G_1 \times G_2, \quad x_1 \longmapsto (x_1, 1_{G_2})$$

$$q_2 : G_1 \longrightarrow G_1 \times G_2, \quad x_2 \longmapsto (1_{G_1}, x_2)$$

sont des morphismes injectifs.

Remarques I.3.3.

a) Le groupe $G_1 \times G_2$ est abélien si et seulement si les groupes G_1 et G_2 le sont.

b) Le groupe $Im(q_1)$ (resp. $Im(q_2)$) est un sous-groupe de $G_1 \times G_2$ isomorphe à G_1 (resp. G_2).

c) Si G_1 et G_2 sont des groupes d'ordre fini, alors $G_1 \times G_2$ est d'ordre fini et $|G_1 \times G_2| = |G_1||G_2|$.

Exercice I.7. Montrer que l'ensemble $\{0, 1, 2, 3\}$ muni de la loi $*$ définie en (1.4) est un groupe isomorphe au groupe $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Vérifier que ce groupe n'est pas isomorphe au groupe $\mathbb{Z}/4\mathbb{Z}$.

Proposition I.3.4. *Soient deux groupes G_1 et G_2. Un groupe G est isomorphe au produit direct $G_1 \times G_2$ si et seulement s'il contient deux sous-groupes H_1 et H_2 tels que*

(i) $H_i \simeq G_i \quad i = 1, 2$

(ii) $\forall\ h_1 \in H_1, \forall\ h_2 \in H_2,\ h_1 h_2 = h_2 h_1$

(iii) $G = H_1 H_2$

(iv) $H_1 \cap H_2 = \{1_G\}$.

Démonstration. Soit $\phi : G_1 \times G_2 \to G$ un isomorphisme. On pose $H_1 = Im(\phi \circ q_1)$ et $H_2 = Im(\phi \circ q_2)$; alors le groupe H_1 (resp. H_2) est isomorphe à G_1 (resp. G_2). D'autre part,

$$\forall h_i \in H_i\, \exists x_i \in G_i, i = 1, 2 \text{ tels que } h_1 = \phi(x_1, 1_{G_2}),\ h_2 = \phi(1_{G_1}, x_2),$$

d'où,

$$h_1 h_2 = \phi(x_1, 1_{G_2})\phi(1_{G_1}, x_2) = \phi((x_1, 1_{G_2})(1_{G_1}, x_2)) = \phi(x_1, x_2).$$

De la même manière, on a

$$h_2 h_1 = \phi(1_{G_1}, x_2)\phi(x_1, 1_{G_2}) = \phi(x_1, x_2)$$

d'où $h_1 h_2 = h_2 h_1$. Tout élément de G s'écrit $\phi(x_1, x_2) = \phi(x_1, 1_{G_2})\phi(1_{G_1}, x_2)$ qui appartient à $H_1 H_2$, donc $G = H_1 H_2$. De plus, $H_1 \cap H_2 = \{\phi(1_{G_1}, 1_{G_2})\}$ est réduit à l'élément neutre de G.

Réciproquement, soient H_1 et H_2 deux sous-groupes et $\phi_i : G_i \to H_i$, $i = 1, 2$ des isomorphismes, avec $G = H_1 H_2$ et $H_1 \cap H_2 = \{1_G\}$. Pour tout $x = (g_1, g_2) \in G_1 \times G_2$, on pose $\psi(x) = \phi_1(g_1)\phi_2(g_2) \in G$. Si $x' = (g_1', g_2')$ alors $\psi(x)\psi(x') = \phi_1(g_1)\phi_2(g_2)\phi_1(g_1')\phi_2(g_2')$. En utilisant (ii), on obtient donc

$$\psi(x)\psi(x') = \phi_1(g_1)\phi_1(g_1')\phi_2(g_2)\phi_2(g_2') = \phi_1(g_1 g_1')\phi_2(g_2 g_2') = \psi(xx').$$

Cela montre que ψ est un morphisme. Il est surjectif puisque $G = H_1 H_2$. Si $\phi_1(g_1)\phi_2(g_2) = 1_G$, alors $\phi_1(g_1) = \phi_2(g_2)^{-1} \in H_1 \cap H_2$, donc $\phi_1(g_1) = \phi_2(g_2) = 1_G$. On en déduit $g_1 = 1_{G_1}$ et $g_2 = 1_{G_2}$, puis $x = 1_{G_1 \times G_2}$, ce qui montre l'injectivité. Par conséquent, ψ est un isomorphisme de $G_1 \times G_2$ sur G. □

Exercice I.8.

1. Généraliser la proposition (I.3.4) à une famille finie de groupes $G_1, \ldots, G_n$.

Attention. *Cette proposition ne peut être généralisée à une famille infinie de groupes, car seul le produit d'un nombre fini d'éléments a un sens.*

2. Montrer que si G est un groupe fini dont tous les éléments distincts de 1_G sont d'ordre 2, alors G est un groupe abélien et il existe un entier $p \geqslant 1$ tel que $G \simeq \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$ (p facteurs).

***Théorème I.3.1* (propriété universelle du produit direct de groupes).** *Soient G_1 et G_2 deux groupes, p_i les projections canoniques de $G_1 \times G_2$ sur G_i, $i = 1, 2$. Pour tout groupe G et tout morphisme de groupes $f_i : G \to G_i$, $i = 1, 2$, il existe un unique morphisme de groupes $h : G \to G_1 \times G_2$ tel que $p_i \circ h = f_i$, $i = 1, 2$.*

Démonstration. Existence de h : pour tout x de G, posons $h(x) = (f_1(x), f_2(x))$. Il est clair que h est un morphisme de groupes et que $p_i \circ h = f_i$, $i = 1, 2$.

Unicité de h : supposons qu'il existe un autre morphisme de groupes $h' : G \to G_1 \times G_2$ tel que $p_i \circ h' = f_i$, $i = 1, 2$. Alors, pour tout x de G, on a $h'(x) = (f_1(x), f_2(x)) = h(x)$, d'où $h' = h$. □

Remarque I.3.4. Le problème universel de produit de groupes s'énonce de la façon suivante : deux groupes G_1 et G_2 étant donnés, existe-t-il un groupe P et des morphismes de groupes $p_i : P \to G_i$, $i = 1, 2$, tels que, pour tout groupe G et tous morphismes de groupes $f_i : G \to G_i$, $i = 1, 2$, il existe un **unique** morphisme de groupes $g : G \to P$ tel que $p_i \circ g = f_i$, $i = 1, 2$? Si (P, p_1, p_2) existe, on dit que c'est une solution du problème universel de produit des groupes G_1, G_2. La proposition précédente montre que $P = G_1 \times G_2$, p_1 et p_2 étant les morphismes de projection, est une solution du problème.

Il est facile de montrer que la solution d'un problème universel est **unique** à isomorphisme **unique** près. Ceci signifie que deux solutions sont isomorphes et qu'il existe un unique isomorphisme de l'une sur l'autre ; on pourra préciser ce que cela signifie en se reportant au TR.II.A.

En particulier, être solution d'un problème universel est une propriété qui caractérise un objet. Par exemple, un groupe P muni de morphismes de groupes $\alpha_i : P \to G_i$, $i = 1, 2$, est isomorphe au produit direct $G_1 \times G_2$ si et seulement s'il est solution du problème universel de produit des groupes G_1 et G_2.

On rencontrera dans cet ouvrage plusieurs types de problèmes universels. En particulier, on peut se poser le problème universel de **somme** de groupes,

problème dual du précédent, obtenu en « renversant » le sens des morphismes. On verra au TR.III.D et au chapitre VI que ce problème universel de somme admet des réponses très différentes suivant que l'on considère des groupes non abéliens ou des groupes abéliens, ce qui n'est pas le cas pour le problème universel de produit comme cela a été remarqué en (I.3.3.a). Par conséquent, la solution d'un problème universel, lorsqu'elle existe, ne dépend pas seulement du type de problème posé, mais aussi du type de structure algébrique concerné.

Proposition I.3.5. *Soient I un ensemble non vide et $\{G_i\}_{i\in I}$ une famille de groupes d'élément neutre respectif 1_{G_i}, $i \in I$. L'ensemble $\prod_{i\in I} G_i$ muni de la loi de composition interne $((x_i)_{i\in I}, (y_i)_{i\in I}) \longmapsto (x_i y_i)_{i\in I}$ est un groupe, noté $\prod_{i\in I} G_i$ et appelé produit direct des groupes $(G_i)_{i\in I}$, dont l'élément neutre est $1 = (1_{G_i})_{i\in I}$ et dans lequel l'élément inverse de $x = (x_i)_{i\in I}$ est l'élément $x^{-1} = (x_i^{-1})_{i\in I}$.*

Démonstration. Laissée au lecteur à titre d'exercice. □

Exercice I.9. Le lecteur démontrera l'énoncé suivant, qui est la généralisation de l'énoncé du théorème (I.3.1) à une famille quelconque de groupes $(G_i)_{i\in I}$.

Soient I un ensemble non vide, $(G_i)_{i\in I}$ une famille de groupes et les morphismes de projection $p_i : \prod_{i\in I} G_i \to G_i$, $i \in I$. Pour tout groupe G et toute famille de morphismes de groupes $f_i : G \to G_i$, $i \in I$, il existe un **unique** morphisme de groupes $g : G \to \prod_{i\in I} G_i$ tel que, pour tout $i \in I$, $p_i \circ g = f_i$.

THÈMES DE RÉFLEXION

♡ TR.I.A. Étude du groupe symétrique S_n

Pour un ensemble E, on note S_E le groupe des applications bijectives de E dans E, ou ***permutations*** de l'ensemble E, pour la composition des applications. On a vu (proposition I.1.1) que, dès que le cardinal de E est strictement supérieur à 2, ce groupe est non abélien.

Le théorème de Cayley (I.2.1) et surtout les très nombreuses occasions où ils interviennent dans des domaines très variés des mathématiques, rendent l'étude des groupes symétriques très importante. On amorcera ici cette étude qui sera poursuivie et approfondie aux TP.I et TR.II.B.

1. *Montrer que si E et E' sont des ensembles équipotents* (cf. *appendice*), *les groupes S_E et $S_{E'}$ sont isomorphes.*

Par conséquent l'étude du groupe S_E, où E est un ensemble fini de cardinal n, se ramène à l'étude du groupe S_n, groupe des permutations de l'ensemble $[n] = \{1, \ldots, n\}$. On rappelle que le cardinal de S_n est $n!$, *i.e.* le groupe S_n est *d'ordre* $n\,!$.

Soit $\sigma \in S_n$, le ***support*** de σ est l'ensemble

$$supp(\sigma) = \{i \in [n], \sigma(i) \neq i\}.$$

2. *Montrer que, dans S_n, deux éléments dont les supports sont disjoints commutent.*

Pour $\sigma \in S_n$ et pour $i \in [n]$, on appelle σ-***orbite*** de i l'ensemble

$$\Omega_\sigma(i) = \{\sigma^r(i), r \in \mathbb{Z}\}.$$

3. *En remarquant que $\Omega_\sigma(i)$ est la classe de i pour une relation d'équivalence définie sur $[n]$, et en notant $\{i_1, \ldots, i_t\}$ une famille de représentants des σ-orbites distinctes dans $[n]$, montrer que*

$$n = \sum_{1 \leqslant q \leqslant t} |\Omega_\sigma(i_q)|.$$

On va maintenant étudier des permutations particulières, les **cycles**, qui sont les constituants élémentaires du groupe symétrique (*cf.* question 6 ci-dessous).

Un élément $\sigma \in S_n$ est un r-***cycle***, ou cycle de longueur r, s'il existe un ensemble ordonné de r entiers distincts dans $[n]$, $\{i_1, \ldots, i_r\}$, tel que

$$\sigma(i_1) = i_2, \ldots, \sigma(i_j) = i_{j+1}, \ldots, \sigma(i_r) = i_1$$
$$\forall k \in \{[n] - \{i_1, \ldots, i_r\}\}, \sigma(k) = k.$$

On remarquera qu'un 1-cycle est nécessairement l'identité et qu'un 2-cycle est une transposition. Une ***permutation circulaire*** d'un ensemble à n éléments est un n-cycle de S_n (*i.e.* de longueur maximale).

4. *Montrer qu'un r-cycle est un élément d'ordre r dans S_n.*

5. *Montrer qu'un élément $\sigma \in S_n$, $n > 1$, est un r-cycle si et seulement si dans la décomposition de $[n]$ en σ-orbites, il n'existe qu'une seule σ-orbite non ponctuelle* (i.e. *non réduite à un point). Le cardinal de cette orbite est égal à r.*

6. *Montrer que tout élément $\sigma \in S_n$, $\sigma \neq id$, s'écrit sous la forme*

$$\sigma = \gamma_1 \circ \cdots \circ \gamma_s, \ s \geqslant 1$$

où les γ_i sont des cycles à supports disjoints, tous différents de l'identité, et que cette décomposition est unique à l'ordre près des facteurs.

Cette décomposition s'appelle la ***décomposition canonique*** de σ en cycles.

Cette décomposition permet donc de ramener l'étude des permutations à celle des cycles.

7. *Montrer que pour $\sigma \in S_n$, l'ordre de σ est le ppcm des ordres des cycles de sa décomposition canonique.*

8. *Montrer que tout $\sigma \in S_n$ se décompose, de manière non unique, en un produit de transpositions.*

Nous allons maintenant introduire un invariant des permutations. Soit $\sigma \in S_n$; si on note t le nombre de σ-orbites distinctes dans $[n]$, on pose $sgn(\sigma) = (-1)^{n-t}$ et on l'appelle ***signature*** de σ.

9. *Montrer que si γ est un r-cycle, $sgn(\gamma) = (-1)^{r-1}$.*

10. *Montrer que si τ est une transposition, $sgn(\sigma \circ \tau) = -sgn(\sigma)$.* (On considère la tranposition τ qui échange i et j ; on montre que :

- si $\Omega_\sigma(k)$ est une σ-orbite ne contenant ni i ni j, $\Omega_{\sigma\circ\tau}(k) = \Omega_\sigma(k)$;
- si i et j sont dans deux σ-orbites distinctes, les termes de ces deux σ-orbites forment une seule $(\sigma \circ \tau)$-orbite ;

– si i et j sont dans la même σ-orbite, les termes de cette σ-orbite forment deux $(\sigma \circ \tau)$-orbites distinctes.

Donc le nombre de $(\sigma \circ \tau)$-orbites est égal au nombre des σ-orbites, plus ou moins un.)

11. *Montrer que si $\sigma \in S_n$ est un produit de k transpositions, alors $sgn(\sigma) = (-1)^k$, et que les nombres de transpositions dans deux décompositons de σ en produit de transpositions ont même parité.*

L'ensemble $\{-1, 1\}$ muni de la multiplication usuelle est un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$. La signature définit donc une application $sgn : S_n \to \mathbb{Z}/2\mathbb{Z}$.

12. *Montrer que cette application est un morphisme de groupes.*

Le morphisme $sgn : S_n \to \mathbb{Z}/2\mathbb{Z}$ défini ci-dessus s'appelle le ***morphisme signature***.

13. *On dit que deux permutations σ et σ' de S_n sont* conjuguées *dans S_n s'il existe une permutation α tel que $\sigma' = \alpha\sigma\alpha^{-1}$. Démontrer la formule suivante : pour un k-cycle $(x_1, \ldots, x_k)$,*

$$\alpha(x_1, \ldots, x_k)\alpha^{-1} = (\alpha(x_1), \ldots, \alpha(x_k)).$$

En déduire, en particulier, que toutes les transpositions sont conjuguées dans S_n.

14. *Démontrer qu'il existe un unique morphisme non trivial $S_n \to \mathbb{Z}/2\mathbb{Z}$.* (On démontrera que si un tel morphisme vaut $+1$ sur une transposition, alors il est trivial sur les transpositions : c'est donc le morphisme trivial.)

Ce qui précède montre l'unicité du morphisme signature. Son noyau, noté A_n, formé des permutations de signature $+1$, sera étudié au TR.II.B.

♡ TR.I.B. Groupes cycliques

Un groupe ***monogène*** est un groupe engendré par un élément,

$$G = \langle x \rangle = \{x^k, k \in \mathbb{Z}\}.$$

Ces groupes sont des groupes abéliens particulièrement importants. On verra au chapitre VI que tout groupe abélien engendré par un nombre fini d'éléments est isomorphe à un produit direct de groupes monogènes.

1. *Montrer que sur tout ensemble fini, on peut définir une loi de composition interne qui munisse cet ensemble d'une structure de groupe monogène.* (Soit X un ensemble à n éléments ; on note x_1 un élément et on pose $x_2 = 2x_1, \ldots$, $x_k = kx_1, \ldots, x_n = nx_1, (n+1)x_1 = x_1$. On munit X de la loi

$$x_i + x_j = x_j + x_i = kx_1, \text{ avec } k = (i+j)\, mod\, n.)$$

2. *Montrer que si G est un groupe monogène :*

– *ou bien G est infini et isomorphe à $\mathbb{Z}$,*

– *ou bien G est d'ordre fini et isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$, avec $n = |G|$.*

Un groupe monogène d'ordre fini est dit ***cyclique***. Ce qui précède montre que l'étude des groupes cycliques se ramène à celle des groupes additifs $\mathbb{Z}/n\mathbb{Z}$.

3. *Montrer que si p est un nombre premier, tout groupe d'ordre p est cyclique, donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Nous allons établir un résultat technique qui nous sera utile dans la suite.

4. *Montrer que si $G = \langle x \rangle$ est un groupe cyclique d'ordre n, $x^k = 1$ si et seulement si $k \in n\mathbb{Z}$.*

Sous-groupes des groupes cycliques

Nous avons vu (proposition I.2.2) que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$. Ils sont donc isomorphes à $\mathbb{Z}$. On remarquera ici une différence fondamentale entre les groupes abéliens et les espaces vectoriels : le sous-groupe $n\mathbb{Z}$ est strictement contenu dans $\mathbb{Z}$ (par exemple si $n = 2$, $n\mathbb{Z}$ est l'ensemble des nombres pairs) et pourtant isomorphe à $\mathbb{Z}$, alors qu'un sous-espace vectoriel strict d'un espace vectoriel de dimension finie ne peut lui être isomorphe.

5. *Montrer que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ correspondent biunivoquement aux sous-groupes $k\mathbb{Z}$ de $\mathbb{Z}$, avec $k > 0$ divisant n. En déduire qu'un sous-groupe d'un groupe cyclique est un groupe cyclique.*

6. *Montrer que si $G = \langle x \rangle$ est un groupe cyclique d'ordre n, si k est un entier relatif et si $h = pgcd(k, n)$, alors x^k et x^h engendrent le même sous-groupe.*

Le théorème de Lagrange (II.1.1) montre que si G est un groupe fini, l'ordre de tout sous-groupe H de G divise l'ordre de G. En général, si d est un diviseur quelconque de l'ordre de G, il n'existe pas de sous-groupe H de G d'ordre d. Par exemple, on verra au TR.II.B que le groupe A_4, qui est d'ordre 12, n'a pas de sous-groupe d'ordre 6. Cependant,

7. *Si $G = \langle x \rangle$ est un groupe cyclique d'ordre n et si d est un diviseur de n, montrer que $H = \langle x^{n/d} \rangle$ est un sous-groupe d'ordre d de G et que c'est le seul.*

On verra au chapitre VI que, plus généralement, si G est un groupe **abélien** fini d'ordre n, pour tout diviseur d de n, il existe un élément de G d'ordre d.

Générateurs d'un groupe cyclique

En général, si $G = \langle x \rangle$ est un groupe cyclique, il existe dans G d'autres générateurs que x. Par exemple, le groupe des racines cubiques de l'unité $G = \{1, j, j^2\}$ est engendré par j et j^2. Nous allons montrer que les générateurs d'un groupe cyclique G forment un groupe, dont nous allons calculer l'ordre.

8. *Montrer que si $G = \langle x \rangle$ est un groupe d'ordre n, x^k est un générateur de G si et seulement si $pgcd(k, n) = 1$* (i.e. *si k et n sont premiers entre eux*).

On en déduit que le nombre de générateurs d'un groupe cyclique d'ordre n est égal à $\varphi(n)$, où φ est la ***fonction d'Euler***

$$\varphi(n) = card\{k \in \mathbb{N}, 1 \leqslant k \leqslant n-1, pgcd(k, n) = 1\}.$$

9. *Montrer que les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ forment un groupe multiplicatif, noté $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$.* (On utilisera l'identité de Bezout.)

On remarquera que ce groupe n'est pas un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, puisque sa loi n'est pas induite par celle de $\mathbb{Z}/n\mathbb{Z}$.

10. *Montrer que, pour tout $n \in \mathbb{N}^*$, le groupe $Aut(\mathbb{Z}/n\mathbb{Z})$ est isomorphe au groupe $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$.*

Produit direct de groupes cycliques. Application au calcul de $\varphi(n)$

11. *Montrer que si p et q sont des entiers positifs, $p\mathbb{Z} \cap q\mathbb{Z} = pq\mathbb{Z}$ si et seulement si p et q sont premiers entre eux.*

En déduire que les groupes $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et $\mathbb{Z}/pq\mathbb{Z}$ sont isomorphes si et seulement si p et q sont premiers entres eux.

12. *Généraliser cette dernière assertion en montrant que les groupes*

$$\mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/p_1 \ldots p_k\mathbb{Z}$$

sont isomorphes si et seulement si les entiers p_i, $1 \leqslant i \leqslant k$, sont premiers entre eux deux à deux.

On en déduit que pour tout nombre $n \in \mathbb{N}^*$ dont la décomposition en facteurs premiers est $n = p_1^{s_1} \ldots p_k^{s_k}$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est canoniquement isomorphe au groupe $\mathbb{Z}/p_1^{s_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{s_k}\mathbb{Z}$.

13. *En déduire que si $n = p_1^{s_1} \ldots p_k^{s_k}$, où les p_i, $1 \leqslant i \leqslant k$, sont des nombres premiers, alors $\varphi(n) = \prod_{i=1}^{i=k} \varphi(p_i^{s_i})$.* (On établira qu'un isomorphisme de groupes $f : G \to G'$ induit une bijection entre l'ensemble des parties génératrices de G et l'ensemble des parties génératrices de G'.)

14. *Montrer que pour tout nombre premier p et tout entier positif s, on a $\varphi(p^s) = p^{s-1}(p-1)$.*

En déduire que si $n = p_1^{s_1} \dots p_k^{s_k}$ est la décomposition de n en facteurs premiers, on a

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

♣ TR.I.C. Détermination des groupes d'ordre n, pour $1 \leqslant n \leqslant 9$

Il s'agit de déterminer tous les groupes, à isomorphisme près, d'ordre n pour $1 \leqslant n \leqslant 9$.

On sait que le seul groupe d'ordre 1 est le groupe trivial réduit à l'élément neutre. La question TR.I.B.3 donne la réponse pour $n = 2, 3, 5, 7$.

Cas $n = 4$

1. *Montrer qu'un groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et que ces deux groupes ne sont pas isomorphes entre eux.*

Cas $n = 6$

Soit G un groupe d'ordre 6.

2. *Montrer que si G est abélien, il est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ (lui-même isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$).*

3. *Montrer que si G est non abélien, il est isomorphe à S_3.*

Cas $n = 8$

Nous allons montrer qu'il existe, à isomorphisme près, exactement cinq groupes d'ordre 8 qui sont :

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ D_4,\ \mathcal{H}.$$

4. *Montrer que les cinq groupes ci-dessus ne sont pas isomorphes entre eux deux à deux.*

Soit G un groupe d'ordre 8 ; il est clair que s'il possède un élément d'ordre 8, il est isomorphe à $\mathbb{Z}/8\mathbb{Z}$ et on sait que, d'après (***EI.8.2***), si tous ces éléments sont d'ordre 2, il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On suppose qu'aucune des conditions ci-dessus n'est réalisée. Il existe donc un élément a d'ordre 4 dans G.

5. *Montrer qu'il existe dans G un élément b, n'appartenant pas au sous-groupe $\langle a\rangle$ et que $\{a, b\}$ engendre G.*

On voit facilement que $ba \in \{ab, a^2b, a^3b\}$.

6. *Montrer que si $ba = ab$, le groupe G est abélien et il est isomorphe au groupe produit $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

7. *Montrer que l'égalité $ba = a^2b$ est impossible.*

On en déduit donc que si $ab \neq ba$, alors $ba = a^3b$.

8. *Montrer qu'alors $b^2 = 1$ ou $b^2 = a^2$, et que :*

- *si $b^2 = 1$, le groupe G est isomorphe au groupe D_4 ;*
- *si $b^2 = a^2$, le groupe G est isomorphe au groupe $\mathcal{H}$.*

Cas $n = 9$

Si le groupe G possède un élément d'ordre 9, il est isomorphe au groupe $\mathbb{Z}/9\mathbb{Z}$.

On suppose que le groupe G ne possède pas d'élément d'ordre 9.

9. *Montrer que le groupe G possède deux éléments a et b d'ordre 3 tels que $a^2 \neq b$ et $b^2 \neq a$, qui engendrent G.*

Il est facile de voir que $ba \in \{ab, ab^2, a^2b, a^2b^2\}$.

10. *Montrer que seule l'égalité $ba = ab$ est possible (calculer $(ba)^2$), et qu'alors le groupe G est isomorphe au groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

Il y a donc, à isomorphisme près, deux groupes d'ordre 9 qui sont :

$$\mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

(vérifier qu'ils ne sont pas isomorphes entre eux).

On aura remarqué que si G est un groupe d'ordre $n = 4$ ou 9, *i.e.* $n = p^2$ où p est un nombre premier, alors G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. On établira ce résultat de façon générale en dans l'exercice (IV.4).

TRAVAUX PRATIQUES

TPI. Étude de quelques groupes de permutations

Dans ce TP, on se propose de manipuler avec MAPLE quelques groupes de permutations, c'est-à-dire des sous-groupes du groupe symétrique S_n, pour différents entiers n. D'après le théorème de Cayley, tout groupe peut être vu comme un groupe de permutations, d'où l'importance de ces derniers. C'est l'occasion d'étudier la structure de groupe (la définition par des générateurs, le calcul du centre, de l'ordre des éléments) et d'appréhender sans formalisme la notion de présentation par générateurs et relations (qui sera étudiée en détail au TP.IV.A). En particulier, on s'intéressera aux deux groupes non abéliens d'ordre 8 : le groupe D_4 des isométries du carré et le groupe quaternionique $\mathcal{H}$.

☞ *Quelques remarques concernant la manipulation des permutations et des groupes de permutations sous* MAPLE : on prendra soin de charger au préalable la librairie *group* de MAPLE (faire `with(group);`).

– *Définition d'une permutation.* On peut soit se donner une « permutation list » $[\sigma(1), \ldots, \sigma(n)]$: ainsi `[1,3,4,5,2]` désigne pour MAPLE la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$, soit se donner la permutation σ comme la liste des cycles à supports disjoints dont le produit est σ : ainsi `[[1,2,3],[4,5]]` désigne la permutation $(1,2,3)(4,5)$. On passe de l'un à l'autre comme suit :

```
>convert([1,3,4,5,2],disjcyc);
>convert([[1,2,3],[4,5]],permlist,5);
>convert([[1,2,3],[4,5]],permlist,9);
>map(g->convert(g,disjcyc),[[2,3,1,5,4],[2,3,1,5,4,6,7,8,9]]);
>map(g->convert(g,disjcyc),{[2,3,1,5,4],[2,3,1,5,4,6,7,8,9]});
```

Noter que, dans la deuxième commande, la permutation est vue comme un élément de S_5 et comme un élément de S_9 dans la troisième. La commande

`type(g,disjcyc(n))` renvoie `true` si g est un élément de S_n donné comme une liste de cycles à supports disjoints et `false` sinon.

Remarque. Concernant toutes les commandes Maple suivantes (et toutes les procédures que vous serez amenés à écrire), sauf mention du contraire, il sera sous-entendu que les permutations sont entrées comme listes de cycles à supports disjoints.

– *Opérations sur les permutations.* Elles sont données par les commandes `invperm, mulperms` (inverse et produit respectivement). Le neutre est `[ ]`.

– *Définition d'un groupe de permutations.* La commande Maple `G:=permgroup(n,{g1,...,gr})` définit le sous-groupe G de S_n par un ensemble $g_1, \ldots, g_r$ de générateurs. On peut alors tester si g appartient à G par `groupmember(g,G)` et calculer le cardinal par `grouporder(G)`.

Remarque. A priori, tous les algorithmes à la base des commandes Maple utilisés dans cette feuille sont connus du lecteur, à l'exception précisément de `groupmember` et de `grouporder` dont l'implémentation dépassant le cadre de ce TP sera passée sous silence (voir cependant la question **4.**). Le lecteur intéressé pourra consulter [10], chapitre 8, ou attendre le TP.II.

Les groupes S_n et A_n

☞ *Quelques commandes* Maple *utiles :* `seq`, `nops`, `op`, `type( ,odd)`.

1. Calculer `mulperms([[1,2]],[[1,3]])` et `mulperms([[1,3]],[[1,2]])`. Que constate-t-on ? Écrire une procédure `multperm:=proc(g1,g2)` renvoyant $g1 \circ g2$.

2. La commande `combinat[permute](n)` renvoie la liste de tous les éléments de S_n en tant que « permutation lists ». Définir S_3 avec la commande `permgroup` et donner la liste de ses éléments à l'aide de la commande `elements`. Comparer avec le résultat de la commande `combinat[permute](3)`.

3. Écrire des fonctions définissant sous Maple, pour n un entier quelconque donné, le groupe S_n à partir des systèmes de générateurs suivants :

– les transpositions $(1,2), (2,3), \ldots, (n-1,n)$;

– la transposition $(1,2)$ et le n-cycle $(1,2,\ldots,n)$.

Vérifier, pour différentes valeurs de n, que l'on obtient bien S_n tout entier (et le démontrer au papier-crayon pour tout n).

4. Soit G le sous-groupe de S_n défini par un ensemble $S_0 = \{g_1, \dots, g_r\}$ de générateurs et soit $S = S_0 \cup \{g_1^{-1}, \dots, g_r^{-1}\}$ (on conserve les inverses, bien que le groupe soit fini, par souci d'efficacité algorithmique). Partant de $L = S \cup \{1_G\}$ et $N = S$, quels types de « mots » en les générateurs et leurs inverses obtient-on dans L et N après exécution de la ligne suivante ?

```
N:={seq(seq(multperm(g,h),g=N),h=S)} minus L; L:=L union N;
```

Et après exécution de cette ligne deux fois de suite ? Tester avec Maple sur S_n, pour $n = 3, 4$, engendré par la transposition (12) et le n-cycle $(1, 2, \dots, n)$. Conclusion ? Écrire une procédure `elements1:=proc(G)` donnant la liste des éléments du groupe G, par itération de la ligne de commandes précédente autant de fois que nécessaire. À l'aide de la commande `time`, comparer sur des exemples les temps de calcul entre cette procédure naïve et la procédure `elements` de Maple dont l'implémentation est passée sous silence : conclusion ?

5. Soit $G(n)$, pour $n \geqslant 3$, le sous-groupe de S_n engendré par :

- les cycles $(1, 2, 3)$ et $(3, \dots, n)$ si n est impair ;
- les permutations $(1, 2, 3)$ et $(1, 2)(3, \dots, n)$ si n est pair.

Que dire de la parité des éléments de $G(n)$? Vérifier avec la commande `parity` puis observer les cardinaux. Quelle conjecture cela suggère-t-il ? La démontrer (*indication :* commencer par remarquer que $(1, 2, i)(1, 2, j)^{-1} = (1, i)(1, j)$ et que S_n est engendré par les transpositions de la forme $(1, i)$; en déduire que le groupe alterné A_n est, pour $n \geqslant 3$, engendré par les 3-cycles $(1, 2, i)$, $i = 3, \dots, n$). Écrire enfin une procédure `A:=proc(n)` définissant A_n sous Maple pour tout entier $n \geqslant 2$.

6. On sait que le centre de S_n est trivial, sauf pour $n = 2$ où le groupe est abélien. En testant avec Maple (commande `center`), faire une conjecture pour A_n et la démontrer.

Deux groupes de permutations de cardinal 8

☞ *Quelques commandes* Maple *utiles :* `sort`, `Matrix`.

Préliminaires : on rappelle que le *type* d'une permutation $\sigma \in S_n$ est la liste $[1, \dots, 1, n_1, \dots, n_r]$, où les n_i, rangés par ordre croissant, sont les longueurs des cycles dans la décomposition canonique en produit de cycles disjoints, avec au préalable autant de 1 que de points fixes : la somme des éléments de la liste vaut donc n (en analyse combinatoire, on dit qu'une telle liste est une partition de n).

7. Écrire une procédure `typ:=proc(g,n)` renvoyant le type de la permutation $g \in S_n$. Tester avec les éléments $(1, 2, 3)$ et $(1, 2, 3)(4, 5)$ de S_6. Comment trouver

l'ordre d'une permutation lorsque l'on connaît son type ? Écrire une procédure `ord` calculant l'ordre d'une permutation. Donner la liste des ordres des éléments de S_4 et vérifier que ces nombres divisent tous le cardinal de S_4. Dénombrer à la main les éléments d'ordre 4 et comparer.

Étude du premier groupe : avec les notations de l'exemple I.1.2.c, on rappelle que le groupe des isométries du carré est $D_4 = \{I, R_1, R_2, R_3, H, V, \Delta_1, \Delta_2\}$.

8. Une isométrie du carré permutant les sommets du carré, justifier que D_4 s'identifie, quitte à numéroter les sommets, à un sous-groupe de S_4 (précisément, on montrera que la restriction aux sommets définit un morphisme injectif de groupes de D_4 dans S_4 ; on identifie alors D_4 à son image). Décrire, en tant que permutations, les éléments de D_4. Enfin, définir D_4 avec la commande `permgroup` et donner la liste des éléments avec la commande `elements`. En déduire qu'il s'agit effectivement d'un sous-groupe de S_4 de cardinal 8.

9. Vérifier que $D_4 = \langle R_1, H\rangle = \langle R_1, V\rangle = \langle R_1, \Delta_1\rangle = \langle R_1, \Delta_2\rangle$ et que, dans chacun de ces cas, $D_4 = \langle a, b\rangle$, où a est d'ordre 4, b d'ordre 2 et $ba = a^3b$. Démontrer que ces relations déterminent complètement le groupe (*i.e.* la liste de ses éléments et sa table de multiplication). Existe-t-il d'autres systèmes de générateurs à deux éléments ? Sont-ils tous de la forme précédente ?

Étude du second groupe : le groupe quaternionique $\mathcal{H}$ est le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ constitué des matrices

$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}, \quad \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix}, \quad \pm\begin{pmatrix}0&i\\i&0\end{pmatrix}, \quad \pm\begin{pmatrix}i&0\\0&-i\end{pmatrix}.$$

On pose, pour g et g' dans $\mathcal{H}$, $\sigma_g(g') = gg'$. D'après le théorème de Cayley, l'application $g \mapsto \sigma_g$ permet de voir $\mathcal{H}$ comme un sous-groupe de S_8.

10. Définir $\mathcal{H}$ sous Maple comme un groupe de permutations en utilisant la remarque précédente (on pourra effectuer le calcul matriciel avec Maple en chargeant au préalable la libraire `LinearAlgebra`). Vérifier par Maple qu'il s'agit bien d'un sous-groupe de S_8 d'ordre 8. Enfin, démontrer que $\mathcal{H}$ est engendré par deux générateurs a et b soumis aux relations $a^4 = b^4 = 1$, $a^2 = b^2$ et $ba = ab^3$.

11. Que dire du sous-groupe de S_8 engendré par les permutations (1234)(5678) et (1537)(2846) ?

12. Est-il possible de voir $\mathcal{H}$ comme un sous-groupe de S_n avec $n < 8$? On écrira une procédure `test:=proc(a,b)` testant si deux éléments d'ordre 4 engendrent un groupe isomorphe à $\mathcal{H}$ et l'on recherchera avec Maple les éléments d'ordre 4 de S_7 (combien en dénombre-t-on à la main ?).

Remarque. Se reporter à l'exercice I.5 pour une méthode utilisant uniquement le papier-crayon.

II

GROUPES QUOTIENTS

On a vu au chapitre I que, pour tout n de $\mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ et la loi interne de $\mathbb{Z}$, c'est-à-dire l'addition, induit une loi interne sur $\mathbb{Z}/n\mathbb{Z}$ qui munit cet ensemble d'une structure de groupe. De plus, la projection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes.

L'objectif de ce chapitre est de formaliser cette situation pour un groupe quelconque. Autrement dit, étant donné un groupe G et un sous-groupe H, à quelles conditions peut-on définir un ensemble quotient G/H et une application canonique $\pi : G \to G/H$, de telle sorte que la loi de G induise sur G/H une loi interne le munissant d'une structure de groupe et que π soit un morphisme de groupes ?

On va montrer qu'à tout sous-groupe H d'un groupe G est associée une relation d'équivalence $\mathcal{R}$ définie sur G. Si cette relation d'équivalence satisfait certaines conditions de compatibilité, la loi interne de G induit une loi interne sur l'ensemble des classes d'équivalence $G/\mathcal{R}$ qui munit cet ensemble d'une structure de groupe et la projection canonique $\pi : G \to G/\mathcal{R}$ est un morphisme de groupes. On montrera qu'inversement, à toute relation d'équivalence $\mathcal{R}$ définie sur un groupe G et satisfaisant les conditions de compatibilité, est associé un sous-groupe H de G tel que la relation $\mathcal{R}$ soit la relation associée au sous-groupe H. Ceci conduit à la notion de sous-groupe **normal**.

II.1. Classes modulo un sous-groupe

On considère un groupe G, H un sous-groupe de G, et on définit sur G la relation

$$(x\mathcal{R}y) \iff (x^{-1}y \in H).$$

Proposition II.1.1.

(i) *La relation $\mathcal{R}$ est une relation d'équivalence.*

(ii) *Soit x un élément de G, sa classe d'équivalence pour la relation $\mathcal{R}$ est l'ensemble $xH = \{xh, h \in H\}$.*

Démonstration. (i). Pour tout x de G, on a $x^{-1}x = 1_G \in H$, d'où $x\mathcal{R}x$ et la relation $\mathcal{R}$ est réflexive. Pour tout x et tout y dans G, on a $(x^{-1}y)^{-1} = y^{-1}x$, d'où si $x\mathcal{R}y$ alors $y\mathcal{R}x$ et la relation $\mathcal{R}$ est symétrique. Si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x^{-1}y \in H$ et $y^{-1}z \in H$, d'où $x^{-1}yy^{-1}z = x^{-1}z \in H$ et $x\mathcal{R}z$, la relation $\mathcal{R}$ est donc transitive.

(ii). Si $x\mathcal{R}y$ il existe $h \in H$ tel que $x^{-1}y = h$, *i.e.* $y = xh$. □

Définition II.1.1. La relation $\mathcal{R}$ est appelée ***relation d'équivalence à gauche modulo*** H, et xH la ***classe à gauche*** de x ***modulo*** H***.***

Remarques II.1.1.

a) On définit une relation d'équivalence à droite modulo H par

$$(x\mathcal{R}y) \Longleftrightarrow (xy^{-1} \in H)$$

et la classe à droite de x modulo H est l'ensemble $Hx = \{hx, h \in H\}$.

Lorsque nous aurons à considérer les relations à gauche et à droite modulo H, nous noterons ces deux relations respectivement ${}_H\mathcal{R}$ et $\mathcal{R}_H$.

b) Quel que soit h dans H, on a $Hh = H = hH$ et H est la classe à droite et à gauche de l'élément neutre de G modulo H.

c) Si le groupe G est abélien, en notant sa loi additivement, les relations d'équivalences définies ci-dessus s'écrivent

$$(x\mathcal{R}y) \Leftrightarrow ((x - y) \in H),$$

et les relations d'équivalences (resp. les classes) à gauche et à droite modulo H coïncident.

Si le groupe G n'est pas abélien, ce n'est plus le cas, en général. On considère dans S_3 le sous-groupe $H = \langle\tau\rangle$ avec $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. En remarquant que $S_3 = \{e, \tau, \sigma, \sigma^2, \tau \circ \sigma, \sigma \circ \tau\}$ avec $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, les classes à gauche et à droite modulo H sont respectivement :

$$\begin{array}{ll} \sigma H = \{\sigma, \sigma \circ \tau\} & H\sigma = \{\sigma, \tau \circ \sigma\} \\ \sigma^2 H = \{\sigma^2, \sigma^2 \circ \tau = \tau \circ \sigma\} & H\sigma^2 = \{\sigma^2, \tau \circ \sigma^2 = \sigma \circ \tau\} \end{array}$$

qui sont deux à deux distinctes puisque $\tau \circ \sigma \neq \sigma \circ \tau$.

***Exemple* II.1.1.** On considère un élément n de $\mathbb{Z}$ et on pose $H = n\mathbb{Z}$, sous-groupe de $\mathbb{Z}$. La relation d'équivalence (resp. les classes) modulo H coïncide(nt) avec la relation (resp. les classes) de congruence modulo n.

Notation. On note $(G/H)_g$ (resp. $(G/H)_d$) l'ensemble des classes d'équivalence des éléments de G pour la relation à gauche (resp. à droite) modulo H. Ces ensembles sont aussi appelés ***ensembles quotients*** à gauche (resp. à droite) ***modulo*** H.

***Proposition* II.1.2.** *Soient G un groupe et H un sous-groupe de G.*

(i) *Toute classe à gauche xH (resp. à droite Hx) est équipotente à H.*

(ii) *Les ensembles $(G/H)_g$ et $(G/H)_d$ sont équipotents.*

Démonstration. (i). Pour tout élément x de G, l'application $H \longrightarrow xH$ qui à h associe xh, est évidemment bijective.

(ii). Pour tout xH de $(G/H)_g$, posons $\varphi(xH) = Hx^{-1}$, qui est un élément de $(G/H)_d$. Montrons que φ est une application. En effet, $xH = yH$ est équivalent à $x^{-1}y \in H$, d'où $x^{-1} \in Hy^{-1}$, et $Hx^{-1} = Hy^{-1}$, c'est-à-dire $\varphi(xH) = \varphi(yH)$. D'autre part, $Hx^{-1} = Hy^{-1}$ est équivalent à $x^{-1}y \in H$, autrement dit, $xH = yH$. Ceci signifie que $\varphi(xH) = \varphi(yH)$ implique $xH = yH$ et donc que φ est injective. De plus, pour tout Hx dans $(G/H)_d$, on a $Hx = \varphi(x^{-1}H)$, par conséquent φ est surjective. Il existe donc une application bijective de $(G/H)_g$ sur $(G/H)_d$, ce qui prouve que ces deux ensembles sont équipotents. □

Définition* II.1.2.** Soient G un groupe et H un sous-groupe de G. On appelle ***indice de H dans G, qu'on note $[G : H]$, le cardinal de l'ensemble $(G/H)_g$ (ou $(G/H)_d$).

***Théorème* II.1.1 (de Lagrange).** *Si G est un groupe fini, pour tout sous-groupe H de G on a*

$$|G| = |H|[G : H].$$

Démonstration. Puisque les xH, $x \in G$, sont les classes d'équivalences pour la relation d'équivalence $\mathcal{R}$, elles forment une partition de G. De plus, d'après la proposition précédente, chacune de ces classes est équipotente à H. On en déduit que le cardinal de G est égal au cardinal de H, multiplié par le nombre de classes, qui est précisément le cardinal de l'ensemble quotient $(G/H)_g$. D'où la formule $|G| = |H|[G : H]$. □

***Remarque* II.1.2.** Ce théorème est souvent énoncé de la façon suivante : dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe.

***Corollaire* II.1.1.** *Pour tout groupe fini, l'ordre de tout élément divise l'ordre du groupe.*

Démonstration. Pour tout x de G, l'ordre de x est l'ordre du sous-groupe $\langle x\rangle$ de G. On applique alors le théorème de Lagrange avec $H = \langle x\rangle$. □

***Proposition* II.1.3.** *Dans un groupe, l'intersection d'un nombre fini de sous-groupes d'indice fini est un sous-groupe d'indice fini.*

Démonstration. Soient G un groupe et H_i, $i = 1, \ldots, n$, une famille de sous-groupes de G qui sont tous d'indice fini dans G. Supposons que $n = 2$. Il est clair que pour tout x de G, on a $(H_1 \cap H_2)x \subseteq (H_1x \cap H_2x)$. D'autre part, pour tout y dans $(H_1x \cap H_2x)$, on a $yx^{-1} \in H_1$ et $yx^{-1} \in H_2$, *i.e.* $yx^{-1} \in H_1 \cap H_2$, d'où $(H_1 \cap H_2)\, x = H_1x \cap H_2x$. On en déduit que $[G : (H_1 \cap H_2)] \leqslant [G : H_1][G : H_2]$.

Si le résultat est vrai pour les $(n-1)$ sous-groupes $H_1, \ldots, H_{n-1}$, on applique le raisonnement ci-dessus aux sous-groupes $(\cap_{i=1}^{n-1} H_i)$ et H_n. □

Attention. *L'énoncé ci-dessus n'est plus vrai, en général, pour un nombre infini de sous-groupes d'indice fini* (considérer les sous-groupes de $\mathbb{Z}$ ou, plus généralement, *cf.* TR.III.C).

***Théorème* II.1.2 (formule de l'indice).** *Si H est un sous-groupe d'indice fini d'un groupe G et si K est un sous-groupe de G contenant H ($H \subseteq K \subseteq G$), alors K est d'indice fini dans G et*

$$[G : H] = [G : K][K : H].$$

Démonstration. Soit $\{x_i\}_{i\in I}$ une famille de représentants des classes à droites distinctes des éléments de G modulo K. Les Kx_i, $i \in I$, forment une partition de G et $card(I) = [G : K]$. Soit $\{y_j\}_{j\in J}$ une famille de représentants des classes à droites distinctes des éléments de K modulo H. Les Hy_j, $j \in J$, forment une partition de K, et $card(J) = [K : H]$. Pour tout g dans G, il existe un unique $i \in I$ tel que $g \in Kx_i$ et il existe un unique $k \in K$ tel que $g = kx_i$. D'autre part, il existe un unique $j \in J$ tel que $k \in Hy_j$, d'où g appartient à Hy_jx_i. On en déduit que $G = \bigcup_{(i,j)\in I\times J}(Hy_jx_i)$.

***Lemme* II.1.1.** *Les ensembles Hy_jx_i, $(i, j) \in I \times J$, forment une partition de G.*

Démonstration. Supposons que $Hy_{j'}x_{i'} = Hy_jx_i$, alors $KHy_{j'}x_{i'} = KHy_jx_i$. Mais, puisque $H \subseteq K$, on a $KH = K$ et $KHy_j = Ky_j = K$, car $y_j \in K$. De la même manière, $KHy_{j'} = K$. On en déduit que $Hy_{j'}x_{i'} = Hy_jx_i$ implique $Kx_{i'} = Kx_i$ et, puisque les Kx_i forment une partition de G, que $i' = i$. Par conséquent $Hy_{j'} = Hy_j$ et, pour une raison analogue, $j' = j$. D'où le lemme.

Ceci prouve que $[G : H] = card(I \times J) = card(I) \times card(J) = [G : K][K : H]$. Comme $[G : H]$ est fini, cette égalité implique que $[G : K]$ est fini. □

***Remarque* II.1.3.** La démonstration ci-dessus montre que la formule de l'indice est vraie de façon plus générale dès que deux quelconques des trois termes qui apparaissent dans la formule sont finis, le troisième étant alors nécessairement fini.

***Exercice* II.1.** Soient H et K deux sous-groupes finis d'un groupe G. Montrer que

$$card(HK) = card(KH) = \frac{|H||K|}{|H \cap K|}.$$

II.2. Compatibilité avec la structure

***Définition* II.2.1.** Soit E un ensemble muni d'une loi de composition interne (notée multiplicativement) sur lequel est définie une relation d'équivalence $\mathcal{R}$.

(i) $\mathcal{R}$ est ***compatible à droite*** (resp. à gauche) avec la loi si, quels que soient x, y, a dans E, on a $(x\mathcal{R}y) \Longrightarrow (xa\mathcal{R}ya)$ (resp. $(x\mathcal{R}y) \Longrightarrow (ax\mathcal{R}ay)$).

(ii) $\mathcal{R}$ est ***compatible*** avec la loi si elle est compatible à droite et à gauche.

***Proposition* II.2.1.** *Avec les mêmes notations que ci-dessus, $\mathcal{R}$ est compatible avec la loi si et seulement si*

$$\forall\ x, x', y, y' \in E, [(x\mathcal{R}x') \text{ et } (y\mathcal{R}y')] \Longrightarrow [xy\mathcal{R}x'y'].$$

Démonstration. Supposons que $\mathcal{R}$ soit compatible avec la loi : alors si $x\mathcal{R}x'$ et $y\mathcal{R}y'$, on a $xy\mathcal{R}x'y$ et $x'y\mathcal{R}x'y'$, d'où $xy\mathcal{R}x'y'$ par transitivité.

Réciproquement, l'assertion de l'énoncé étant vraie pour tout x, x', y, y', c'est en particulier vrai pour $y = y'$, d'où si $x\mathcal{R}x'$ alors $xy\mathcal{R}x'y$ et la relation est compatible à droite avec la loi. De même, en considérant $x = x'$, on montre qu'elle est compatible à gauche. □

Proposition II.2.2. *Soient G un ensemble muni d'une loi de composition interne, $\mathcal{R}$ une relation d'équivalence définie sur G et $G/\mathcal{R}$ l'ensemble quotient de G par la relation d'équivalence $\mathcal{R}$. Alors la loi interne de G induit une loi interne sur $G/\mathcal{R}$, $(\overline{x},\overline{y}) \mapsto \overline{xy}$ (où pour $z \in G$, $\overline{z}$ désigne la classe d'équivalence de z) si et seulement si $\mathcal{R}$ est compatible avec la loi de G.*

Démonstration. La correspondance $(\overline{x},\overline{y}) \mapsto \overline{xy}$ définit une loi interne sur $G/\mathcal{R}$ si et seulement si elle définit une application $G/\mathcal{R} \times G/\mathcal{R} \to G/\mathcal{R}$, autrement dit, si et seulement si

$$(\overline{x} = \overline{x_1}, \overline{y} = \overline{y_1}) \Longrightarrow (\overline{xy} = \overline{x_1 y_1}),$$

d'où le résultat d'après la proposition (II.2.1). □

Remarque II.2.1. Si la relation $\mathcal{R}$ est compatible avec la loi de G, ***la loi induite*** sur $G/\mathcal{R}$ par celle de G est définie par $\overline{x}\ \overline{y} = \overline{xy}$. Il est clair que si la loi de G est associative (resp. commutative, resp. admet un élément neutre e, resp. tout élément x admet un élément symétrique x^{-1}), il en est de même pour la loi induite sur $G/\mathcal{R}$, $\overline{e}$ est l'élément neutre, l'élément symétrique de $\overline{x}$ est $\overline{x^{-1}}$.

Exemple II.2.1. Pour tout entier n, la relation d'équivalence définie par la congruence modulo n dans $\mathbb{Z}$ est compatible avec l'addition et la multiplication des entiers. Ces deux lois induisent donc des lois de compositions internes sur l'ensemble des entiers modulo n, qui sont associatives, commutatives, qui possèdent un élément neutre ; de plus tout élément admet un symétrique pour la loi induite par l'addition.

II.3. Groupes quotients

On va maintenant étudier la situation où G est un groupe.

Proposition II.3.1. *Soient G un groupe et $\mathcal{R}$ une relation d'équivalence définie sur G, compatible avec la loi de G. Alors l'ensemble quotient $G/\mathcal{R}$, muni de la loi induite par la loi de G (définie par $(\overline{x},\overline{y}) \mapsto \overline{xy}$), est un groupe.*

Démonstration. C'est une conséquence directe de la proposition II.2.2, qui assure que la loi sur le quotient est bien définie, et de la remarque II.2.1. □

Une autre façon de dire les choses est la suivante : notant $\pi : G \longrightarrow G/\mathcal{R}$ l'application de passage au quotient, la loi sur le quotient $G/\mathcal{R}$ est définie par $\pi(x)\pi(y) = \pi(xy)$. On applique alors la remarque (I.2.5.e)

On est donc amené à déterminer les relations d'équivalences compatibles avec la loi de G.

Proposition II.3.2. *Pour tout sous-groupe H d'un groupe G, la relation $\mathcal{R}_H$ (resp. ${}_H\mathcal{R}$) est compatible à droite (resp. à gauche) avec la loi de composition de G.*

Réciproquement, si une relation $\mathcal{R}$ définie sur un groupe G est compatible à droite (resp. à gauche) avec la loi de composition du groupe G, alors il existe un unique sous-groupe H de G tel que $\mathcal{R} = \mathcal{R}_H$ (resp. $\mathcal{R} = {}_H\mathcal{R}$).

Démonstration. Soient x, y, a des éléments de G tels que $x\mathcal{R}_H y$, *i.e.* $xy^{-1} \in H$. Alors, $(xa)(ya)^{-1} = xaa^{-1}y^{-1}$ appartient à H, *i.e.* $xa\mathcal{R}_H ya$. Une démonstration analogue donne le résultat pour ${}_H\mathcal{R}$.

Soit $\mathcal{R}$ une relation d'équivalence définie sur G, compatible à droite avec la loi de G. On note H la classe d'équivalence de l'élément neutre 1_G de G. Montrons que H est un sous-groupe de G. Puisque $1_G \in H$, H est non vide. Pour tous x et y dans H, on a $x\mathcal{R}1_G$ et $y\mathcal{R}1_G$. La compatibilité de $\mathcal{R}$ avec la loi de G implique que $xy^{-1}\mathcal{R}y^{-1}$; de plus, puisque $y\mathcal{R}1_G$, on a $yy^{-1}\mathcal{R}y^{-1}$, d'où $1_G\mathcal{R}y^{-1}$ et $y^{-1}\mathcal{R}1_G$. On en déduit que $xy^{-1}\mathcal{R}1_G$, *i.e.* $xy^{-1} \in H$, ce qui prouve que H est un sous-groupe de G. Vérifions que $\mathcal{R} = \mathcal{R}_H$. Si $x\mathcal{R}y$ alors, d'après la compatibilité, $xy^{-1}\mathcal{R}1_G$, d'où $xy^{-1} \in H$ et $x\mathcal{R}_H y$. Si $x\mathcal{R}_H y$, $xy^{-1} \in H$, donc $xy^{-1}\mathcal{R}1_G$ et, d'après la compatibilité, $x\mathcal{R}y$. L'unicité de H découle du fait que si $\mathcal{R} = \mathcal{R}_H$, alors H est la classe d'équivalence de 1_G. □

La relation d'équivalence $\mathcal{R}$ est donc compatible avec la loi de G si et seulement si il existe un sous-groupe H de G tel que $\mathcal{R} = {}_H\mathcal{R} = \mathcal{R}_H$. Cela conduit à la définition suivante.

Définition II.3.1. Un sous-groupe H d'un groupe G est dit **normal** (ou **distingué**) dans G si ${}_H\mathcal{R} = \mathcal{R}_H$. On note alors $H \triangleleft G$.

Et nous avons démontré :

Théorème II.3.1. *Si H est un sous-groupe normal d'un groupe G, la loi de composition interne induite sur l'ensemble G/H par celle de G munit G/H d'une structure de groupe. La surjection canonique $\pi : G \to G/H$ qui, à un élément de G associe sa classe modulo H, est un morphisme de groupes.*

Exemple II.3.1. Pour tout $n \in \mathbb{N}^*$, l'addition de $\mathbb{Z}$ induit une structure de groupe sur $\mathbb{Z}/n\mathbb{Z}$, qui est celle définie dans l'exemple (I.1.2.b).

Proposition II.3.3. *Un sous-groupe H d'un groupe G est normal dans G si et seulement s'il vérifie les conditions équivalentes suivantes :*

(i) $\forall x \in G,\ xH \subset Hx$

(i') $\forall x \in G,\ xH = Hx$

(ii) $\forall x \in G,\ xHx^{-1} \subset H$

(ii') $\forall x \in G,\ xHx^{-1} = H$

(iii) $\forall h \in H,\ \forall x \in G,\ xhx^{-1} \in H$

(iv) *Il existe un groupe G' et un morphisme de groupes $f : G \longrightarrow G'$ tel que $H = Ker(f)$.*

Démonstration. Le sous-groupe H est normal dans G si et seulement si les relations ${}_H\mathcal{R}$ et $\mathcal{R}_H$ sont égales, donc si et seulement si les classes à gauche et les classes à droite sont égales.

Les assertions (i) et (i') ainsi que (ii) et (ii') sont clairement équivalentes. D'autre part, (i) implique (ii), qui est équivalente à (iii). Si $xhx^{-1} \in H$, $(x \in G,\ h \in H)$, alors il existe $h' \in H$ tel que $xh = h'x$, donc $xH \subseteq Hx$ et (iii) implique (i).

Si H est un sous-groupe normal de G, H est le noyau du morphisme canonique de projection $\pi : G \longrightarrow G/H$. Réciproquement, si $f : G \longrightarrow G'$ est un morphisme de groupes, en posant $H = Ker(f)$, on a :

$$\forall h \in H, \forall x \in G, f(xhx^{-1}) = f(x)f(h)f(x)^{-1} = 1_{G'}$$

d'où $xhx^{-1} \in H$ et H est un sous-groupe normal de G. □

***Remarque* II.3.1.** Un sous-groupe H d'un groupe G est normal dans G s'il est stable par les éléments de $Int(G)$ (*cf.* exemple I.2.5.b).

***Exemples* II.3.2.**

a) Il est clair que si G est un groupe abélien, tout sous-groupe H de G est normal et G/H est un groupe abélien. En particulier, d'après l'exemple (II.2.1), le groupe additif des entiers modulo n est le groupe quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.

b) On a vu (exemple I.2.2) que S_3 est engendré par σ_1 et τ_3. Considérons le sous-groupe $H = \langle\sigma_1\rangle = \{e, \sigma_1, \sigma_1^2\}$. On vérifie que les classes à gauche et à droite de S_3 modulo H sont égales, donc $H \triangleleft S_3$. De plus $S_3/H \simeq S_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

c) Le groupe spécial linéaire $SL_n(k)$, étant le noyau du morphisme déterminant $det : GL_n(k) \to k^*$, est un sous-groupe normal de $GL_n(k)$.

d) On note A_n le sous-groupe de S_n formé des permutations de signature $+1$. C'est le noyau du morphisme signature $sgn : S_n \to \mathbb{Z}/2\mathbb{Z}$, c'est donc un sous-groupe normal de S_n.

Exercice II.2.

1. Montrer que pour tout groupe G, $Int(G)$ est un sous-groupe normal de $Aut(G)$.

2. Soient G un groupe et H un sous-groupe de G. Montrer que si $[G : H] = 2$, alors H est un sous-groupe normal de G.

3. Montrer que tous les sous-groupes du groupe quaternionique $\mathcal{H}$ sont normaux dans $\mathcal{H}$.

Remarque II.3.2. Si H et K sont deux sous-groupes d'un groupe G, avec $H \subseteq K$, alors :

$$(H \lhd G) \text{ implique } (H \lhd K).$$

Attention. *En général,*

$$(H \lhd K) \text{ n'implique pas } (H \lhd G), \quad (H \lhd G) \text{ n'implique pas } (K \lhd G),$$

$$(H \lhd K \text{ et } K \lhd G) \text{ n'implique pas } (H \lhd G).$$

Autrement dit la propriété pour un sous-groupe d'être normal n'est pas transitive. Un exemple d'une telle situation est donné dans le TR.II.B.

II.4. Caractérisation des sous-groupes normaux

Il est clair qu'un sous-groupe H d'un groupe G n'est pas nécessairement normal dans G. Nous allons introduire un sous-groupe intermédiaire entre H et G, appellé le **normalisateur** de H dans G, dans lequel H sera un sous-groupe normal et qui permettra de déterminer si H est normal dans G.

Définition II.4.1. Soient G un groupe et $\mathcal{P}(G)$ l'ensemble de ses parties. On dit que deux éléments S et S' de $\mathcal{P}(G)$, $(S \neq \emptyset)$, sont ***conjugués*** s'il existe un élément x de G tel que $S' = xSx^{-1} = \{xsx^{-1}, s \in S\}$.

En convenant que la partie vide est conjuguée d'elle-même, la relation de conjugaison est une relation d'équivalence sur $\mathcal{P}(G)$. Pour une partie $S \neq \emptyset$ de G, sa classe d'équivalence pour cette relation est l'ensemble $\{xSx^{-1}, x \in G\}$, qu'on appelle ***classe de conjugaison*** de S.

Remarques II.4.1.

a) Si $S = \{g\}$, où g est un élément de G, les éléments de sa classe de conjugaison sont appelés les ***conjugués*** de g dans G.

b) Une partie S' est conjuguée d'une partie S si elle est l'image de S par un automorphisme intérieur de G. Par conséquent, deux parties conjuguées sont équipotentes.

c) Si H est un sous-groupe de G, toute partie de G conjuguée de H est un sous-groupe de G, isomorphe à H.

Exercice II.3. Montrer que dans le groupe S_n, pour tout k, $1 \leqslant k \leqslant n$, les k-cycles sont conjugués (*cf.* TR.I.A.3).

On sera amené à utiliser la notion plus générale suivante :

Définition II.4.2. Soient S et S' deux parties d'un groupe G et H un sous-groupe de G. Alors S et S' sont ***conjuguées sous*** H s'il existe un élément x de H tel que $S' = xSx^{-1}$.

Proposition - Définition II.4.1. *Soient S une partie d'un groupe G et H un sous-groupe de G.*

(i) *L'ensemble $N_H(S) = \{x \in H, xSx^{-1} = S\}$ est un sous-groupe de H (donc de G) appelé le normalisateur de S dans H.*

(ii) *L'ensemble $Z_H(S) = \{x \in H \,|\, \forall s \in S,\ xsx^{-1} = s\}$ est un sous-groupe de H (donc de G) appelé le centralisateur de S dans H.*

(iii) $Z_H(S) \triangleleft N_H(S)$.

Démonstration. (i). Il est clair que $1_H \in N_H(S)$. Soient $x, y \in N_H(S)$, $xSx^{-1} = ySy^{-1} = S$, d'où $xy^{-1}Syx^{-1} = S = (xy^{-1})S(xy^{-1})$, donc $xy^{-1} \in N_H(S)$.

(ii). Se démontre de la même façon.

(iii). Soient $x \in Z_H(S)$ et $a \in N_H(S)$, alors pour tout $s \in S$, $(axa^{-1})\ s\ (ax^{-1}a^{-1}) = axs'x^{-1}a^{-1}$, avec $s' = a^{-1}sa$. Puisque $x \in Z_H(S)$, $xs'x^{-1} = s'$, d'où

$$(axa^{-1})\ s\ (ax^{-1}a^{-1}) = as'a^{-1} = aa^{-1}saa^{-1} = s,$$

d'où le résultat. □

Proposition II.4.2. *Soient G un groupe et H un sous-groupe de G. Alors H est un sous-groupe normal de $N_G(H)$, et H est un sous-groupe normal de G si et seulement si $N_G(H) = G$.* □

Proposition II.4.3. *Soient G un groupe, S une partie de G, H un sous-groupe de G. L'ensemble des classes de conjugaison de S sous H a pour cardinal l'indice de $N_H(S)$ dans H.*

Démonstration. Deux classes de conjugaison xSx^{-1} et ySy^{-1} sont égales si et seulement si $(xy^{-1})S(xy^{-1})^{-1} = S$, *i.e.* $xy^{-1} \in N_H(S)$. Autrement dit, deux classes de conjugaison xSx^{-1} et ySy^{-1} sont égales si et seulement si les éléments x et y sont dans la même classe modulo $N_H(S)$. On en déduit que le nombre de classes de conjugaison de S distinctes est égal à $[H : N_H(S)]$. □

Exercice II.4. Montrer que $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal.

II.5. Sous-groupes normaux et morphismes

Théorème II.5.1. *Soient G et G' deux groupes et f un élément de $Hom(G, G')$. Alors f induit un isomorphisme $\overline{f}$ de $G/Ker(f)$ sur $Im(f)$.*

Démonstration. Soit $\pi : G \to G/Ker(f)$ la projection canonique. Tout élément de $G/Ker(f)$ est la classe $\pi(x)$ d'un élément x de G. Posons $\overline{f}(\pi(x)) = f(x)$ et montrons que $\overline{f}$ est une application : si x' est un autre représentant de la classe $\pi(x)$, on a $xx'^{-1} \in Ker(f)$, d'où $f(x') = f(x)$ et f est bien définie. On vérifie aisément que $\overline{f}$ est un morphisme de groupes. Par construction, $\overline{f}$ est surjective. D'autre part, si $\overline{f}(\pi(x)) = \overline{f}(\pi(y))$, on a $f(x) = f(y)$, *i.e.* $xy^{-1} \in Ker(f)$, d'où $\pi(x) = \pi(y)$, donc $\overline{f}$ est injective. D'où le résultat. □

Remarque II.5.1. Le théorème ci-dessus peut être démontré à partir du théorème de factorisation des applications. En effet, on sait que si E et E' sont des ensembles et $f : E \to E'$ est une application, on définit sur E une relation d'équivalence $\mathcal{R}$ par $x\mathcal{R}y$ si et seulement si $f(x) = f(y)$. On considère $E/\mathcal{R}$ l'ensemble des classes d'équivalence des éléments de E et l'application $\overline{f}$ définie comme ci-dessus est une bijection de $E/\mathcal{R}$ sur $Im(f)$. Il suffit alors de vérifier que sous les hypothèses du théorème (II.5.1), l'application $\overline{f}$ est un morphisme de groupes.

Exercice II.5. Soit G un groupe :

a) Montrer que le centre $Z(G)$ de G est un sous-groupe normal de G.

b) Montrer que le groupe $G/Z(G)$ est isomorphe au groupe $Int(G)$.
(On considérera l'homomorphisme $G \to Int(G)$ défini par $g \mapsto \varphi_g$ (exemple I.2.5.b).) On en déduit que pour tout groupe G tel que $Z(G) = \{1\}$, on a $G \simeq Int(G)$.

c) Montrer que si le groupe $G/Z(G)$ est cyclique, alors le groupe G est abélien.

Proposition II.5.1. *Soient G et G' deux groupes et f un élément de $Hom(G, G')$. Alors*

(i) $H \triangleleft G \Longrightarrow f(H) \triangleleft f(G)$,

(ii) $H' \triangleleft G' \Longrightarrow f^{-1}(H') \triangleleft G$.

Démonstration. (i). Soient $y \in f(H)$ et $z \in f(G)$, alors il existe $h \in H$ et $g \in G$ tels que $f(h) = y$ et $f(g) = z$. On a $zyz^{-1} = f(ghg^{-1}) \in f(H)$ et $f(H)$ est normal dans $f(G)$.

(ii). Soient $h \in f^{-1}(H')$ et $g \in G$. On a $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H'$, d'où $ghg^{-1} \in f^{-1}(H')$. □

Attention. *Sous les hypothèses de la proposition (II.5.1), on n'a pas $f(H)$ normal dans G', sauf si, par exemple, f est surjectif.*

Exercice II.6.

1. Soient G_1 et G_2 des groupes, H_1 et H_2 des sous-groupes normaux respectifs de G_1 et G_2. Montrer que les projections canoniques $\pi_i : G_i \to G_i/H_i$, $i = 1, 2$, induisent un isomorphisme de groupes $(G_1 \times G_2)/(H_1 \times H_2) \simeq (G_1/H_1) \times (G_2/H_2)$.

2. Montrer que si H et K sont deux sous-groupes conjugués d'un groupe G, alors $N_G(H)$ et $N_G(K)$ sont des sous-groupes de G conjugués.

II.6. Sous-groupes d'un groupe quotient

Lemme II.6.1. *Soient G un groupe, H et K deux sous-groupes de G. Si H est normal dans G, alors HK est un sous-groupe de G et H est un sous-groupe normal de HK.*

Démonstration. Puisque H est un sous-groupe normal de G et que $K \subseteq G$, pour tout $k \in K$ on a $kH = Hk$, d'où $KH = HK$ et HK est un sous-groupe de G d'après la proposition (I.3.1). De plus, pour tout $h \in H$ et tout $g \in G$, on a $ghg^{-1} \in H$, donc *a fortiori* pour $g \in HK$, par conséquent H est un sous-groupe normal de HK. □

Théorème II.6.1. *Soient G un groupe, H un sous-groupe normal de G, $\pi : G \to G/H$ la projection canonique.*

(i) *Le morphisme π induit une correspondance biunivoque entre les sous-groupes (resp. sous-groupes normaux) de G contenant H et les sous-groupes (resp. sous-groupes normaux) de G/H.*

(ii) *Si K est un sous-groupe de G, alors HK est un sous-groupe de G contenant H et $\pi(K) = HK/H$.*

Démonstration. (i). Soit $\overline{K}$ un sous-groupe de G/H et considérons $K = \pi^{-1}(\overline{K})$ l'image réciproque de $\overline{K}$ par π. Puisque l'application π est surjective, $\pi(K) = \overline{K}$ et puisque π est un morphisme, d'après la proposition (I.2.7.(iv)), K est un sous-groupe de G. Si $\overline{K}$ est un sous-groupe normal de G/H, d'après la proposition (II.5.1.(ii)) K est normal dans G. De plus K contient H qui est l'image réciproque de l'élément neutre de G/H.

Inversement, soit K un sous-groupe de G contenant H. Alors H est normal dans K et $\pi(K) = K/H$ est un sous-groupe de G/H, qu'on notera $\overline{K}$. D'après la proposition (II.5.1.(i)), si K est normal dans G, $\overline{K}$ est un sous-groupe normal de $\pi(G) = G/H$.

Les applications $K \mapsto \overline{K}$ et $\overline{K} \mapsto K$ sont des bijections réciproques l'une de l'autre de l'ensemble des sous-groupes (resp. sous-groupes normaux) de G contenant H sur l'ensemble des sous-groupes (resp. sous-groupes normaux) de G/H.

(ii). Le sous-groupe H étant normal dans G, on a déjà vu que HK est un sous-groupe de G qui contient H comme sous-groupe normal. Donc $\pi(HK) = HK/H$. D'autre part, il est clair que $\pi(K) \subset \pi(HK)$; réciproquement, si $y = \pi(hk)$, $(h \in H,\ k \in K)$ alors $y = \pi(h)\pi(k) = \pi(k)$, donc $\pi(HK) \subset \pi(K)$. Finalement, $\pi(K) = HK/H$. □

Exemple II.6.1. Les sous-groupes du groupe $\mathbb{Z}/n\mathbb{Z}$ sont les groupes $k\mathbb{Z}/n\mathbb{Z}$ avec $n\mathbb{Z} \subset k\mathbb{Z}$, c'est-à-dire avec k divisant n dans $\mathbb{N}^*$. Le nombre de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ est donc égal au nombre de diviseurs de n dans $\mathbb{N}^*$.

Proposition II.6.1. *Soient G un groupe et H un sous-groupe normal de G. Si K et K' sont deux sous-groupes de G contenant H, alors*

$$K < K' \Longrightarrow (K/H) < (K'/H).$$

Démonstration. On a $K/H = \pi(K) < \pi(K') = K'/H$. □

Exercice II.7.

1. Soient $f : G \to G'$ un morphisme de groupes et H un sous-groupe de G. Montrer que $f(N_G(H)) \subseteq N_{G'}(f(H))$. Que peut-on dire quand f est surjectif ?

2. Soient G un groupe, H un sous-groupe normal de G, $\pi : G \to G/H$ la projection canonique. Si K est un sous-groupe de G contenant H, comparer $N_G(K)$ et $N_{G/H}(\pi(K))$.

Théorème II.6.2 **(de passage au quotient).** *Soient G et G' deux groupes, H (resp. H') un sous-groupe normal de G (resp. G'), $\pi : G \to G/H$ (resp. $\pi' : G' \to G'/H'$) la projection canonique. Pour tout $f \in Hom(G, G')$ tel que $f(H) \subseteq H'$, il existe un unique $\overline{f} \in Hom(G/H, G'/H')$ tel que $\overline{f} \circ \pi = \pi' \circ f$.*

Convention. L'expression « le diagramme suivant

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g'} \\ C & \xrightarrow[f']{} & D \end{array}$$

est commutatif » signifie que les applications f, f', g, g' satisfont à la condition $g' \circ f = f' \circ g$.

Démonstration du théorème (II.6.2). Considérons le diagramme suivant :

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \pi'} \\ G/H & \xrightarrow[\overline{f}]{} & G'/H' \end{array}$$

Si le morphisme $\overline{f}$ existe et fait commuter le diagramme, il doit vérifier $\overline{f}(\pi(x)) = \pi'(f(x))$ et, tout élément de G/H s'écrivant $\pi(x)$ pour $x \in G$, cette égalité impose l'unicité de $\overline{f}$.

Montrons que l'égalité ci-dessus définit bien une application $\overline{f}$, *i.e.* que $\overline{f}(\pi(x))$ est indépendant du représentant x choisi dans G pour décrire sa classe dans G/H. Si $\pi(x) = \pi(y)$, on a $xy^{-1} \in H$, donc $f(xy^{-1}) = f(x)f(y)^{-1} \in f(H) \subseteq H'$. D'où $\pi'(f(x)) = \pi'(f(y))$.

Montrons que $\overline{f}$ est un morphisme de groupes. On a

$$\begin{aligned}\overline{f}(\pi(x)\pi(y)) &= \overline{f}(\pi(xy)) = \pi'(f(xy)) = \pi'(f(x)f(y)) \\ &= \pi'(f(x))\pi'(f(y)) = \overline{f}(\pi(x))\overline{f}(\pi(y)).\end{aligned}$$

□

Remarque* II.6.1.** En particulier, si $H \subseteq Ker(f)$, il existe un unique morphisme $\overline{f} \in Hom(G/H, G')$ tel que $f = \overline{f} \circ \pi$. On dit que f ***factorise à travers π.

***Théorème* II.6.3.** *Soient G un groupe et H un sous-groupe normal de G. Pour tout sous-groupe K de G, $H \cap K$ est un sous-groupe normal de K, H est un sous-groupe normal de HK, et les groupes quotients $K/H \cap K$ et HK/H sont isomorphes.*

Démonstration. Si le sous-groupe H est normal dans G, alors il est normal dans HK et $H \cap K$ est normal dans K, donc les groupes quotients $K/(H \cap K)$ et HK/H existent. Considérons les morphismes canoniques

$$\pi : K \to K/(H \cap K), \quad \pi' : HK \to HK/H, \quad i : K \to HK.$$

Alors $i(H \cap K) = (H \cap K) \subseteq H$ et, d'après le théorème (II.6.2), il existe un unique morphisme $\overline{i} : K/(H \cap K) \to HK/H$ tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} K & \xrightarrow{\ i\ } & HK \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ K/(H \cap K) & \xrightarrow[\ \overline{i}\ ]{} & HK/H \end{array}$$

On a vu au théorème (II.6.1.(ii)) que $\pi'(K) = HK/H$, donc le morphisme $\pi' \circ i = \overline{i} \circ \pi$ est surjectif, il en est donc de même du morphisme $\overline{i}$. D'autre part, on a

$$[\overline{i}(\pi(x)) = 0] \Leftrightarrow [\pi'(i(x)) = 0] \Leftrightarrow [x \in H \cap K]$$

d'où $\overline{i}(\pi(x)) = 0$ équivaut à $\pi(x) = 0$ et $\overline{i}$ est injective. Par conséquent $\overline{i}$ est un isomorphisme. □

***Théorème* II.6.4.** *Soient G un groupe, H et K deux sous-groupes normaux de G tels que $H \subseteq K$. Alors les groupes $(G/H)/(K/H)$ et G/K sont isomorphes.*

Démonstration. On sait, d'après le théorème (II.6.1), que K/H est un sous-groupe normal de G/H et le groupe quotient $(G/H)/(K/H)$ est bien défini. Considérons les morphismes canoniques

$$\pi_H : G \to G/H, \quad \pi_K : G \to G/K, \quad \pi : G/H \to (G/H)/(K/H).$$

Puisque $\pi_H(K) = K/H$, d'après le théorème de passage au quotient, il existe un unique morphisme $\varphi : G/K \to (G/H)/(K/H)$ tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} G & \xrightarrow{\pi_H} & G/H \\ {\scriptstyle \pi_K}\downarrow & & \downarrow{\scriptstyle \pi} \\ G/K & \xrightarrow[\varphi]{} & (G/H)/(K/H) \end{array}$$

Le morphisme $\pi \circ \pi_H$ étant surjectif, il en est de même du morphisme φ. D'autre part, on a

$$[\varphi(\pi_K(x)) = 0] \Leftrightarrow [\pi_H(x) \in K/H] \Leftrightarrow [x \in K],$$

d'où $\varphi(\pi_K(x)) = 0$ équivaut à $\pi_K(x) = 0$ et φ est injective. Par conséquent φ est un isomorphisme. □

THÈMES DE RÉFLEXION

♣ TR.II.A. Sous-groupes dérivés et abélianisation

À tout groupe G on associe un sous-groupe normal $D(G)$, appelé sous-groupe **dérivé** de G, tel que le groupe quotient $G/D(G)$ soit un groupe abélien. On montre que ce dernier groupe est solution du *problème universel d'abélianisation*.

Soit G un groupe : pour tous x et y éléments de G, on pose $[x, y] = xyx^{-1}y^{-1}$. Cet élément de G est appelé ***commutateur*** de x et y. On remarquera que le groupe G est abélien si et seulement si, pour tous x et y éléments de G, on a $[x, y] = 1$.

On note $D(G)$ le sous-groupe de G *engendré* par les commutateurs $[x, y]$ pour x et y parcourant G et on l'appelle sous-groupe ***dérivé*** de G.

1. *Montrer que $D(G)$ est un sous-groupe normal de G.*

2. *Montrer que le groupe $G/D(G)$ est abélien.*

3. *Soit H un sous-groupe normal de G. Montrer que G/H est abélien si et seulement si $D(G) \subseteq H$.*

Problème universel d'abélianisation

Pour tout groupe G, on appelle ***abélianisé*** de G la donnée d'un groupe abélien G_{ab} et d'un morphisme de groupes $\lambda : G \to G_{ab}$ tels que, pour tout groupe abélien A et tout morphisme de groupes $f : G \to A$, il existe un **unique** morphisme de groupes abéliens $\overline{f} : G_{ab} \to A$ tel que $\overline{f} \circ \lambda = f$. Si (G_{ab}, λ) existe, on dit que c'est une solution du problème universel d'abélianisation du groupe G.

4. *Montrer que si le problème universel d'abélianisation admet deux solutions, elles sont isomorphes et que l'isomorphisme permettant de passer de l'une à l'autre est unique.* (On considérera deux solutions (G_{ab}, λ) et (G'_{ab}, λ') et on considérera le problème précédent en remplaçant (A, f) par (G_{ab}, λ) d'une part et (G'_{ab}, λ')

d'autre part. L'unicité de l'isomorphisme provient de la condition d'unicité imposée au morphisme $\overline{f}$ par l'énoncé.)

On reformule la question précédente en disant que, si le problème universel d'abélianisation admet une solution, elle est unique à un unique isomorphisme près. C'est-à-dire que, dès qu'on connaît une solution, on connaît toutes les autres, sans ambiguïté sur le passage de l'une à l'autre. Comme on l'a remarqué à la question précédente, c'est la condition d'unicité du morphisme $\overline{f}$ imposée par l'énoncé du problème qui impose « l'unicité de la solution » et « l'unicité de l'isomorphisme », *i.e.* qui confère à ce problème son caractère universel.

5. *Montrer que $(G/D(G), \pi)$, où π est la projection canonique $\pi : G \to G/D(G)$, est solution du problème universel d'abélianisation de G.*

On déduit de la question 4 que $(G/D(G), \pi)$ est **la** solution du problème d'abélianisation de G.

♡ TR.II.B. Étude des sous-groupes normaux de S_n

Le goupe A_n, $n \geqslant 3$, formé des permutations de signature $+1$ d'un ensemble à n éléments, est le noyau du morphisme signature (*cf.* TR.I.A), c'est donc un sous-groupe normal propre de S_n. Nous allons montrer que pour tout $n \neq 4$, c'est le seul sous-groupe normal de S_n.

Nous allons plus précisément montrer que, pour $n \geqslant 3, n \neq 4$, le groupe A_n n'a pas de sous-groupes normaux propres.

Un groupe G n'ayant pas de sous-groupes normaux propres est dit ***simple***.

L'étude des groupes finis simples est une partie importante de la théorie des groupes. Le résultat suivant, dont la démonstration est l'une des plus difficiles des mathématiques (et dépasse donc très largement le cadre de ce livre), en est une étape cruciale :

Les groupes simples finis, autres que les groupes cycliques d'ordre premier, sont d'ordre pair.

Le but de ce TR est évidemment beaucoup plus modeste, néanmoins, le fait que les groupes A_n, $n \geqslant 5$, soient simples a des conséquences très importantes. En particulier, c'est la raison fondamentale pour laquelle les équations polynomiales de degré supérieur ou égal à 5 ne sont pas résolubles par radicaux, contrairement aux équations polynomiales de degré inférieur ou égal à 4 (*cf.* chapitre XVI).

1. *Montrer que les groupes abéliens simples sont les groupes cycliques d'ordre premier.*

2. *Montrer que si H est un sous-groupe normal non trivial de S_n, $n \geqslant 3$, alors $H \cap A_n$ est un sous-groupe normal non trivial de A_n. Montrer que A_n est l'unique sous-groupe d'indice 2 de S_n.*

3. *Montrer que si $n \geqslant 3$, le groupe A_n est engendré par les 3-cycles $(1, 2, i)$ avec $3 \leqslant i \leqslant n$.*

Cas $n = 3$

4. *Montrer que le seul sous-groupe normal propre de S_3 est A_3.*

Cas $n = 4$

On considère les éléments de S_4 suivants :

$$\sigma_1 = (1,2)(3,4),\ \ \sigma_2 = (1,3)(2,4),\ \ \sigma_3 = (1,4)(2,3),$$

où (i, j) est la transposition (ou 2-cycle) échangeant i et j et on pose

$$V_4 = \{1, \sigma_1, \sigma_2, \sigma_3\},$$

où 1 est la permutation identité.

5. *Montrer que*

- *il contient tous les éléments d'ordre 2 de A_4 ;*
- *V_4 est un sous-groupe abélien normal de A_4 et S_4 ;*
- *c'est le seul sous-groupe d'ordre 4 de A_4.*

6. *Montrer que V_4 admet trois sous-groupes propres $K_i, i = 1, 2, 3$, et qu'ils sont normaux dans V_4, mais pas dans A_4.* (On a ainsi un exemple illustrant le fait que la propriété d'être un sous-groupe normal n'est pas transitive, comme cela a été souligné dans les exemples (II.3.2).)

7. *Montrer qu'il n'y a pas de sous-groupe d'ordre 6 dans A_4 et que $Z(A_4) = \{1\}$.*

8. *Montrer que le groupe S_4/V_4 est isomorphe au groupe S_3. En déduire que A_4 est le seul sous-groupe normal propre de S_4 contenant strictement V_4.* (Indication : identifiant S_3 avec l'ensemble des permutations σ dans S_4 vérifiant $\sigma(1) = 1$, démontrer que tout élément de S_4 s'écrit de manière unique comme un produit xy, $x \in V_4$, $y \in S_3$. En déduire que le groupe S_4/V_4 est isomorphe au groupe S_3. Finalement, démontrer que A_4 est le seul sous-groupe normal propre de S_4 contenant strictement V_4. (Si H est un tel sous-groupe, considérer l'application $S_3 \simeq S_4/V_4 \longrightarrow S_4/H$).)

9. *En déduire que les seuls sous-groupes propres normaux de S_4 sont V_4 et A_4.*

Cas $n \geqslant 5$

10. *Soit H un sous-groupe normal de A_n. Montrer que si H contient un 3-cycle, alors $H = A_n$.*

Soit H un sous-groupe normal non trivial de A_n. On va démontrer que si H contient une permutation σ, alors il existe un 3-cycle γ tel que $\sigma' = \gamma\sigma\gamma^{-1}\sigma^{-1}$ soit un 3-cycle. Pour cela, on note $l(\sigma)$ la longueur du cycle le plus long dans la décomposition canonique de σ en produit de cycles.

11. *Démontrer, en distinguant successivement les cas $l(\sigma) > 3$, $l(\sigma) = 3$, $l(\sigma) = 2$, que dans chaque cas H contient un 3-cycle.* (On calculera d'abord $\sigma\gamma^{-1}\sigma^{-1}$.)

12. *En déduire que pour $n \geqslant 5$, A_n est un groupe simple.*

13. *Montrer que A_n est le seul sous-groupe normal de S_n.*

14. *Montrer que $D(A_n) = A_n$.*
Nous allons maintenant établir que $D(S_n) = A_n$.

15. *Montrer que $D(S_n) \subseteq A_n$.*
On considère la projection canonique $\pi : S_n \to S_n/D(S_n)$.

16. *Montrer que pour tout couple (τ, τ') de transpositions, on a $\pi(\tau) = \pi(\tau')$. En déduire que pour tout élément σ de A_n, on a $\pi(\sigma) = 1$.*

17. *En déduire que $D(S_n) = A_n$.*

Application. Pour tout entier $n > 1$, il n'existe pas de sous-groupe de S_n *strictement compris entre* S_{n-1} et S_n.

Le groupe S_{n-1} n'étant pas un sous-groupe de S_n, la phrase ci-dessus est incorrecte : elle nécessite donc une précision. Les éléments de S_n qui laissent fixe le point n forment un sous-groupe K qui est isomorphe à S_{n-1} : c'est *via* cet isomorphisme que l'on considère S_{n-1} comme un sous-groupe de S_n.

Nous allons montrer le résultat suivant :

Pour tout entier $n > 1$, si H est un sous-groupe de S_n contenant strictement K, alors $H = S_n$.

Le résultat est évident pour $n = 2, 3$.

18. *Montrer que A_4 est le seul sous-groupe d'ordre 12 de S_4 et en déduire le résultat pour $n = 4$.*

On suppose maintenant que $n \geqslant 5$ et soit H un sous-groupe de S_n contenant strictement K. On pose $K_1 = K \cap A_n$ et $H_1 = H \cap A_n$.

19. *Justifier que $K_1 \simeq A_{n-1}$ et montrer que K_1 est strictement contenu dans H_1. En déduire que l'indice de H_1 dans A_n est strictement inférieur à n.*

On considère l'ensemble $E = A_n/H_1$ des classes à gauche de A_n modulo H_1. D'après le dernier résultat de la question 19, on a $1 \leqslant card(E) < n$.

À tout élément xH_1 de E et tout élément $g \in A_n$, on associe l'élément gxH_1 de E.

20. *Montrer que ceci définit un morphisme de groupes* $\varphi : A_n \longrightarrow S_E$.

21. *On suppose que* $card(E) \neq 1$. *Montrer alors que* $Ker(\varphi)$ *est strictement contenu dans* A_n *et en déduire que* φ *est injectif.* (On utilisera la question 12.)

22. *Déduire de ce qui précède que* $card(E) = 1$, *d'où* $card(H) = card(S_n)$.

Ce dernier résultat prouve que $H = S_n$.

♠ TR.II.C. Étude des automorphismes de S_n

Le but de cette étude est de montrer que pour tout $n \in \mathbb{N}^*$, $n \geqslant 2$, $n \neq 6$, on a $Int(S_n) = Aut(S_n)$.

1. *En remarquant que le groupe* S_n, $n \geqslant 2$, *est engendré par les transpositions* $\tau_i = (1, i)$, *montrer que tout automorphisme de* S_n *qui transforme toute transposition en une transposition est intérieur.*

Pour démontrer le résultat annoncé, il suffit donc de prouver que, pour $n \neq 6$, tout automorphisme de S_n transforme toute transposition en une transposition. Pour cela, nous allons d'abord étudier les centralisateurs de certains éléments de S_n (questions 2 et 3), puis faire un raisonnement par l'absurde.

On considère $\tau = (i, j)$ une transposition donnée et $C(\tau)$ son centralisateur, *i.e.* $C(\tau) = Z_{S_n}(\langle\tau\rangle)$.

2. *En considérant* $E = [n] \setminus \{i, j\}$, *montrer que l'application qui à un élément* γ *de* $C(\tau)$ *associe sa restriction à* E, *induit un morphisme surjectif de groupes* $f : C(\tau) \to S_E \simeq S_{n-2}$, *dont le noyau est isomorphe à* $\mathbb{Z}/2\mathbb{Z}$.

3. *En déduire que si* σ *est un produit de* k *transpositions à supports disjoints, ces transpositions engendrent un sous-groupe normal de* $C(\sigma)$ *qui est isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^k$.

Soit $\varphi \in Aut(S_n)$. On suppose qu'il existe une transposition τ telle que $\varphi(\tau) = \sigma$, où σ est égale à un produit de k transpositions, avec $k \geqslant 2$.

4. *En remarquant que les centralisateurs* $C(\tau)$ *et* $C(\sigma)$ *sont isomorphes, montrer que* S_{n-2} *possède un sous-groupe normal isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^l$, *avec* $l > 0$.

L'étude faite au TR.II.B ci-dessus montre que ceci n'est possible que si $n - 2 = 2$ (*i.e.* $n = 4$), ou $n - 2 = 4$ (*i.e.* $n = 6$).

5. *Montrer que, dans la situation ci-dessus, le cas $n = 4$ est impossible.* (On aurait alors $|C(\tau)| = 4$ et $|C(\sigma)| = 8$, ce qui est en contradiction avec $C(\tau) \simeq C(\sigma)$.)

On déduit donc que, pour tout $n \neq 6$, tout automorphisme de S_n transforme toute transposition en une transposition.

On déduit de ce qui précède, ainsi que de l'exercice (I.1.1) et de l'exercice (II.5.b), que pour tout $n \geqslant 3$, $n \neq 6$, on a $S_n \simeq Int(S_n) \simeq Aut(S_n)$.

Pour compléter cette étude, on montrera au TR.V.A que $Int(S_6) \neq Aut(S_6)$.

TRAVAUX PRATIQUES

TP.II. Classes, structure quotient et systèmes générateurs forts

On poursuit dans ce TP l'étude des groupes de permutations, autour des notions de classes et de quotient. On liste les classes de conjugaison, ce qui est l'occasion de discuter « l'équation aux classes » pour la conjugaison (voir le corollaire 2.1 du chapitre IV pour une version plus générale), puis les classes à gauche et à droite modulo un sous-groupe afin d'illustrer la notion de sous-groupe distingué. En particulier, on regarde le quotient de S_4 par le groupe de Klein V_4, quotient isomorphe à S_3. Pour finir, on répond au problème du calcul effectif de l'ordre et des éléments d'un groupe de permutations G défini par un système de générateurs, ainsi que du test d'appartenance à G d'un élément donné : quels algorithmes se cachent derrière les commandes `grouporder`, `elements` et `groupmember` de MAPLE, qui sont vraisemblablement plus performants que les algorithmes naïfs vus dans le cadre du TP.I ?

Conjugaison et équation aux classes

1. Dénombrer à la main le nombre de conjugués de $\sigma = (123)(45)$ dans S_6 ; vérifier avec la commande `SnConjugates`.

Dans le cas d'un groupe de permutations G quelconque, disons de degré n, deux éléments a et b conjugués sous G sont conjugués dans S_n, donc de même type. Écrire une procédure `areconj:=proc(G,a,b)` testant si a et b sont conjugués dans G. On utilisera la condition nécessaire précédente afin d'éliminer de suite ces cas où la réponse est négative.

Soient $a = (1,2)(3,4)$, $b = (1,3)(2,4)$ et D_4 le sous-groupe de S_4 engendré par $(1,2,3,4)$ et $(1,3)$ (c'est le groupe des isométries du carré déjà rencontré dans

le TP.I). Vérifier que a et b appartiennent à D_4. Sont-ils conjugués dans S_4 ? Et dans D_4 ? Vérifier également avec la commande `areconjugate` de Maple.

2. Écrire une procédure `classeconj:=proc(a,G)` renvoyant la classe de conjugaison de a dans G. Reprenant l'exemple de la question précédente, calculer les classes de a et b dans S_4 et dans G. *L'équation aux classes* d'un groupe G est la formule $\mathrm{Card}(G) = \sum_i \mathrm{Card}(C_i)$, où les C_i sont les classes de conjugaison distinctes de G. Cela résulte tout bonnement du fait que la conjugaison est une relation d'équivalence sur G. Écrire une procédure nommée `listeclasses:=proc(G)` donnant l'équation aux classes pour le groupe G sous la forme de la liste des cardinaux des classes de conjugaison de G, rangés par ordre croissant. Vérifier la validité de l'équation aux classes pour S_4 et le groupe D_4 de la question précédente.

3. Deux groupes ayant même équation aux classes sont-ils isomorphes en tant que groupes abstraits ? (*Indication :* rechercher parmi les groupes de permutations abéliens.)

Classes modulo un sous-groupe, sous-groupes distingués

☞ *Quelques commandes* Maple *utiles :* `isnormal`, `evalb(E=F)` *(teste par exemple l'égalité de deux ensembles E et F).*

Dans ce paragraphe, G est un groupe et H est un sous-groupe de G.

4. Soit x un élément de G. Écrire deux procédures `classeg:=proc(x,H)` et `classed:=proc(x,H)` renvoyant respectivement la classe à gauche xH et à droite Hx de x modulo H.

5. La commande `cosets` renvoie une liste de représentants des classes à gauche modulo un sous-groupe. Définir le groupe de Klein V_4 des isométries du rectangle comme un sous-groupe de S_4 (par restriction à l'ensemble des sommets) et donner la liste des classes à gauche modulo V_4. Puis lister les classes à droite (*indication :* le morphisme $g \mapsto g^{-1}$ induit une bijection $(G/H)_g \to (G/H)_d$). Conclusion ? Vérifier avec une commande Maple appropriée. Est-ce étonnant, sachant que la conjugaison conserve le type ? Pour finir, déduire de la liste précédente que le groupe quotient S_4/V_4 est isomorphe à S_3 (*indication :* considérer la restriction de l'application de passage au quotient $S_4 \to S_4/V$ au sous-groupe S_3, identifié aux permutations laissant fixe 1).

Remarque. Noter que V_4 est un sous-groupe distingué de A_4. C'est une exception : on a démontré au TR.II.B que A_n est simple pour $n \neq 4$: il ne possède pas de sous-groupe distingué propre.

6. On prend cette fois pour H le sous-groupe engendré par (12) et (34), qui est également isomorphe à V_4, car engendré par deux éléments d'ordre 2 qui

commutent. Est-il distingué dans S_4 ? Lister les classes à gauche et à droite de S_4 modulo H.

Remarque. On a démontré au TR.II.B que A_4 et V_4 sont les seuls sous-groupes distingués propres de S_4.

7. Écrire ses propres procédures `classesg:=proc(G,H)` et `classesd` (*i.e.* n'utilisant pas la commande `cosets`) renvoyant respectivement les ensembles de classes $(G/H)_g$ et $(G/H)_d$ (*indication :* on pourra se contenter de l'algorithme naïf suivant : calculer des classes jusqu'à épuiser les éléments du groupe). Tester sur les exemples précédents. En déduire que `cosets` calcule bien des représentants des classes *à gauche* (et non à droite comme le stipule l'aide de Maple, du moins avec notre définition de classe à gauche).

Systèmes générateurs forts et algorithme de Schreier-Sims

Soit G un groupe de permutations de degré n ; il agit donc sur l'ensemble $\{1,\dots,n\}$. On considère la tour de groupes

$$G = G_0 \supset G_1 \supset \cdots \supset G_{n-1} = \{\mathrm{Id}\}$$

où G_i désigne le sous-groupe constitué des éléments g de G qui laissent fixes (*i.e.* $g(j) = j$) les indices $j \leqslant i$. Une liste $L = (S_1, \dots, S_{n-1})$, où S_i est un système de représentants des classes (à gauche) G_{i-1}/G_i, est appelé *système générateur fort* de G.

8. Construire un système générateur fort pour les sous-groupes de degré 4 suivants : $\{\mathrm{Id}\}$, $<(1234)>$, A_4 et S_4 (on utilisera la commande `classesg`).

Soit $O_i = \{g(i), g \in G_{i-1}\}$ (orbite de i sous G_{i-1}) ; choisissons, pour tout $j \in O_i$, un élément g_j^i de G_{i-1} tel que $g_j^i(i) = j$. Démontrer au papier-crayon que $S_i = \{g_j^i, j \in O_i\}$ représente les classes G_{i-1}/G_i. Il n'était donc pas nécessaire de recourir à la commande `classesg`.

Enfin, calculer le produit $\prod_{i=1}^{n-1} |S_i|$ sur les exemples précédents ; que constate-t-on ?

9. Démontrer la proposition suivante :

Proposition 1. *Soit $L = (S_1, \dots, S_{n-1})$ un système générateur fort de G. Tout élément g de G s'écrit de manière unique comme un produit $g = \sigma_1 \circ \cdots \circ \sigma_{n-1}$, où $\sigma_i \in S_i$ pour $1 \leqslant i \leqslant n-1$.*

En déduire des procédures `card1:=proc(SGF)` et `elements1:=proc(SGF)` renvoyant respectivement le cardinal et la liste des éléments d'un groupe de permutations G donné par un système générateur fort SGF. Tester sur les exemples précédents et vérifier avec les commandes natives de Maple.

10. Écrire rapidement une procédure `image:=proc(g,n,i)` calculant l'image de l'entier i par une permutation g de degré n (donnée comme toujours par une liste de cycles à supports disjoints). On pourra utiliser la conversion en une `permlist` ou, au contraire, s'en passer, ce qui est préférable.

L'algorithme suivant, qui permet de tester si une permutation g appartient au groupe G défini par un système générateur fort $L = (S_1, \dots, S_{n-1})$, résulte directement de la preuve de la proposition 1 :

(a) On pose $g' = g$.

(b) Pour i de 1 à n, on effectue les opérations suivantes : on regarde si $g'(i)$ appartient à $O_i = \{\sigma(i), \sigma \in S_i\}$; si c'est le cas, on note σ_i l'unique élément de S_i tel que $g'(i) = \sigma_i(i)$ et remplace g' par $\sigma_i^{-1} \circ g' \in G_i$; dans le cas contraire, g n'appartient pas à G et c'est terminé.

(c) Si tous les tests ont été positifs, alors g appartient à G et il s'écrit $g = \sigma_1 \circ \cdots \circ \sigma_{n-1}$.

Écrire une procédure `appart:=proc(g,SGF)` réalisant cet algorithme et tester sur les exemples habituels.

11. Afin de compléter le programme d'étude prévu, il reste à expliquer comment, à partir d'un système de générateurs, obtenir un système générateur *fort* de manière efficace.

Tout d'abord, modifier la procédure `appart` pour qu'elle renvoie le couple (i, g') obtenu en sortie de l'algorithme si $g \notin G$ (autrement dit, $g = \sigma_1 \circ \cdots \circ \sigma_{i-1} \circ g'$ avec $\sigma_j \in S_j$ pour $j < i$ et $g' \in G_{i-1}$, mais il n'existe pas $\sigma_i \in S_i$ tel que $g'(i) = \sigma_i(i)$) et (n, Id) si $g \in G$.

La stratégie est la suivante : si $SG = \{g_1, \dots, g_r\}$ engendre le groupe, on part du système générateur fort du groupe trivial $\{\mathrm{Id}\}$ et rajoute progressivement les g_i. Il s'agit donc de construire, à partir d'un système générateur fort $L = (S_1, \dots, S_{n-1})$ d'un groupe G, un système générateur fort $L' = (S'_1, \dots, S'_{n-1})$ du groupe G' engendré par $G \cup \{g\}$. Pour cela :

(a) On applique la procédure `appart` (modifiée) à g : si $i = n$, alors il n'y a rien à faire ; dans le cas contraire, on rajoute g' à S_i puis on applique (a) avec $g = g' \circ h$, pour tout $h \in S_j$, $1 \leqslant j \leqslant i$.

(b) Lorsqu'il n'y a plus rien à faire, on a obtenu un système générateur fort pour G'.

Implémenter cet algorithme (appelé algorithme de Schreier-Sims) et tester sur les exemples habituels. On écrira une procédure récursive `sgf_plus:=proc(g,SGF)`

correspondant à l'ajout de l'élément g, puis une procédure `sgf:=proc(SG,n)` renvoyant le système générateur fort demandé.

Remarque. Le lecteur motivé pourra consulter [16], paragraphe 6, pour une preuve (théorème 6.8) ainsi qu'une discussion de la complexité de cet algorithme.

Enfin, tester l'efficacité du calcul du cardinal et des éléments, *via* celui d'un système générateur fort, en comparant les temps de calcul avec ceux des commandes `grouporder` et `elements` de Maple, ainsi qu'avec la procédure naïve `elements1` du TP.I. Conclusion ? Ces commandes Maple sont, en fait, basées sur des variantes de l'algorithme de Schreier-Sims.

This page intentionally left blank

III

PRÉSENTATION D'UN GROUPE PAR GÉNÉRATEURS ET RELATIONS

Nous avons vu en (I.2.B) que, si S est une partie génératrice d'un groupe G, tout élément x de G s'écrit $x = s_1 \dots s_k$, avec $s_i \in S$ ou $s_i^{-1} \in S$. Mais cette écriture n'est pas unique (remarque I.2.3). Dans ce chapitre, nous allons montrer que pour tout ensemble X, il existe un groupe $L(X)$ dans lequel tout élément s'écrit de *manière unique* en fonction des générateurs $x_i \in X$. C'est le **groupe libre de base** X. Outre l'écriture des éléments, ce groupe est d'une grande importance, car on verra que tout groupe est isomorphe à un quotient d'un tel groupe. De plus, cela conduit à la notion de groupes présentés par générateurs et relations, qui sont des groupes dans lesquels les écritures des éléments en fonction des générateurs peuvent être simplifiées à l'aide des relations entre ces générateurs. Ces groupes sont particulièrement intéressants pour les possibilités qu'ils offrent, de calculs effectifs sur les éléments et de définitions explicites de morphismes, dont on trouvera des illustrations dans le TP.IV.A à la fin du chapitre IV.

III.1. Groupes libres

Définition III.1.1.

a) Soient G un groupe et S une partie de G. Le groupe G est dit ***libre de base*** S si tout élément x de G s'écrit de manière unique

$$x = s_{i_1}^{n_1} \dots s_{i_k}^{n_k}$$

avec $k, i_1, \dots, i_k \in \mathbb{N}$, $n_1, \dots, n_k \in \mathbb{Z}$, $s_{i_1}, \dots, s_{i_k} \in S$, tels que $s_{i_j} \neq s_{i_{j+1}}$. Si $k = 0$, on pose $x = 1$.

On dit alors que S est une famille ***génératrice libre*** de G, ou encore que S est une ***base*** de G.

b) Un groupe G est dit ***libre*** s'il possède une base.

c) Si le groupe G possède une base finie, il est dit ***libre de type fini***.

Théorème III.1.1. *Pour tout ensemble X, il existe un groupe libre $L(X)$ de base X.*

Posons $X = \{x_i\}_{i\in I}$ et considérons X^{-1} un ensemble équipotent à X, dont on notera les éléments $x_i^{-1}, i \in I$.

Il est important de noter qu'il s'agit là seulement d'une notation, qui sera commode dans la suite. Les éléments x_i^{-1} ne sont pas les inverses des x_i puisque, pour l'instant, X et X^{-1} ne sont que des ensembles sans aucune structure algébrique. On aurait pu noter cet ensemble équipotent à X par Y et ses éléments par $y_i, i \in I$, mais, dans la suite, l'écriture des éléments en aurait été compliquée.

Définition III.1.2.

a) On appelle ***mot*** en $X \cup X^{-1}$ toute suite finie d'éléments de $X \cup X^{-1}$

$$x = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}, \text{ où } \epsilon_i = \pm 1.$$

b) Dans l'écriture ci-dessus, l'entier n est la ***longueur*** du mot x, qu'on notera $l(x)$.

c) Deux mots $x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ et $x_{j_1}^{\gamma_1} \dots x_{j_k}^{\gamma_k}$ sont des ***mots égaux*** si $n = k$ et $\forall p,\ 1 \leqslant p \leqslant n,\ i_p = j_p$ et $\epsilon_p = \gamma_p$.

Par convention, il n'existe qu'un seul mot de longueur 0, qu'on notera 1. C'est le mot qui correspond à la suite vide de $X \cup X^{-1}$.

Exemple III.1.1. Si $X = \{x, y, z\}$, xyz, $xyyzz^{-1}xx^{-1}x$ sont des mots en $X \cup X^{-1}$.

On note $\mathcal{M}(\mathcal{X})$ l'ensemble des mots en $X \cup X^{-1}$ et on définit sur $\mathcal{M}(\mathcal{X})$ un **produit** (loi de composition interne) par juxtaposition des mots. Plus précisément, si $x = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ et $y = x_{j_1}^{\gamma_1} \dots x_{j_k}^{\gamma_k}$ sont deux mots, alors

$$xy = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n} x_{j_1}^{\gamma_1} \dots x_{j_k}^{\gamma_k}.$$

Par convention, on pose $1x = x1 = x$. On remarquera que ce produit est associatif, que 1 est élément neutre, mais que $\mathcal{M}(\mathcal{X})$ n'est pas un groupe car tout élément autre que 1 ne peut avoir d'inverse. En effet, pour tout x et y dans

$\mathcal{M}(\mathcal{X})$, on a $l(xy) = l(x) + l(y)$, donc dès que x ou y est différent de 1, $l(xy) > 0$, et $xy \neq 1$. Pour pallier cet inconvénient, on va définir sur $\mathcal{M}(\mathcal{X})$ une relation d'équivalence $\mathcal{R}$ telle que $\mathcal{M}(\mathcal{X})/\mathcal{R}$ soit un groupe pour le produit induit par celui de $\mathcal{M}(\mathcal{X})$.

***Définitions* III.1.3.**

a) Deux mots x et y de $\mathcal{M}(\mathcal{X})$ sont ***adjacents*** s'il existe $t_1, t_2 \in \mathcal{M}(\mathcal{X})$ et $a \in X \cup X^{-1}$ tels que

$$x = t_1 t_2 \text{ et } y = t_1 a a^{-1} t_2$$

ou

$$x = t_1 a a^{-1} t_2 \text{ et } y = t_1 t_2,$$

avec la convention $(a^{-1})^{-1} = a$ pour tout $a \in X \cup X^{-1}$.

Notation. Si x et y sont deux mots adjacents, on écrira $x \mathcal{A} y$.

b) *La relation $\mathcal{R}$ est définie sur $\mathcal{M}(\mathcal{X})$ par*

$$[x\mathcal{R}y] \Leftrightarrow [\exists t_1, \ldots, t_n \in \mathcal{M}(X) \text{ tels que } x = t_1,\ y = t_n \text{ et } t_i \mathcal{A} t_{i+1},\ i = 1, \ldots, n-1].$$

***Lemme* III.1.1.** *La relation $\mathcal{R}$ est une relation d'équivalence.*

Démonstration. Pour tout x de $\mathcal{M}(\mathcal{X})$ on a $x \mathcal{R} x$, en prenant $a = 1$, la relation est donc réflexive. La relation d'adjacence étant symétrique, on en déduit facilement qu'il en est de même pour la relation $\mathcal{R}$. Soient $x \mathcal{R} y$ et $y \mathcal{R} z$; on a

$$(x = t_1)\mathcal{A} \ldots \mathcal{A}(t_n = y = t_{n+1})\mathcal{A} \ldots \mathcal{A} t_{n+p} = z,$$

d'où $x \mathcal{R} z$ et la relation $\mathcal{R}$ est transitive.

Notation. Pour tout x de $\mathcal{M}(\mathcal{X})$, on notera $[x]$ sa classe dans $\mathcal{M}(\mathcal{X})/\mathcal{R}$.

***Lemme* III.1.2.** *La relation $\mathcal{R}$ est compatible avec la loi interne de $\mathcal{M}(\mathcal{X})$.*

Démonstration. Soient x, y, z dans $\mathcal{M}(\mathcal{X})$; remarquons que $x \mathcal{A} y$ implique que $xz \mathcal{A} yz$. En effet, si $x = t_1 t_2$ et $y = t_1 a a^{-1} t_2$, alors $xz = t_1(t_2 z)$ et $yz = t_1 a a^{-1}(t_2 z)$. Par conséquent, si $(x = t_1) \mathcal{A} \ldots \mathcal{A} t_n$, alors $(xz = t_1 z)\mathcal{A} \ldots \mathcal{A} (t_n z = yz)$, ce qui prouve que la relation $\mathcal{R}$ est compatible à droite avec la loi de $\mathcal{M}(\mathcal{X})$. Un raisonnement analogue montre la compatibilité à gauche.

***Lemme* III.1.3.** *L'ensemble $\mathcal{M}(\mathcal{X})/\mathcal{R}$ est un groupe pour la loi induite par celle de $\mathcal{M}(\mathcal{X})$.*

Démonstration. D'après la remarque (II.2.1), on sait que la loi interne de $\mathcal{M}(\mathcal{X})/\mathcal{R}$ induite par celle de $\mathcal{M}(\mathcal{X})$ est associative et possède un élément neutre. Il suffit donc de montrer que tout élément $[x]$ possède un inverse. Considérons d'abord le cas où $x \in X \cup X^{-1}$; il est clair que $xx^{-1}\mathcal{R}\ 1$, car en prenant $t_1 = t_2 = 1$, on a $xx^{-1} = t_1xx^{-1}t_2$ et $1 = t_1t_2$, d'où $xx^{-1}\ \mathcal{A}\ 1$. De la même manière, $x^{-1}x\ \mathcal{R}\ 1$. On en déduit donc que

$$\forall x \in \mathcal{M}(\mathcal{X}),\ [x]^{-1} = [x^{-1}].$$

La projection canonique $\pi : \mathcal{M}(\mathcal{X}) \to \mathcal{M}(\mathcal{X})/\mathcal{R}$ vérifie

$$\pi(xy) = [xy] = [x][y] = \pi(x)\pi(y).$$

Donc, pour tout $x = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$, $\epsilon_i = \pm 1$, $[x]$ est inversible et a pour inverse

$$[x]^{-1} = ([x_{i_1}^{\epsilon_1}] \dots [x_{i_n}^{\epsilon_n}])^{-1} = [x_{i_n}^{\epsilon_n}]^{-1} \dots [x_{i_1}^{\epsilon_1}]^{-1} = [x_{i_n}^{-\epsilon_n}] \dots [x_1^{-\epsilon_1}] = [x_{i_n}^{-\epsilon_n} \dots x_1^{-\epsilon_1}].$$

Démonstration du théorème IV.1.1. Nous allons démontrer que le groupe $\mathcal{M}(\mathcal{X})/\mathcal{R}$ est le groupe $L(X)$ cherché ; pour cela, nous allons construire un groupe L_X qui répond à la définition (III.1.1) et montrer que ce groupe L_X est isomorphe à $\mathcal{M}(\mathcal{X})/\mathcal{R}$. Pour ce faire, nous allons montrer que chaque classe de $\mathcal{M}(\mathcal{X})/\mathcal{R}$ possède un élément privilégié, le groupe L_X sera formé à partir de ces éléments.

Définition III.1.4. Un mot x de $\mathcal{M}(\mathcal{X})$ est ***réduit*** si $x = 1$ ou $x = a_1 \dots a_n$, avec $a_i \in X \cup X^{-1}$ tels que $a_{i+1} \neq a_i^{-1}$, $i = 1, \dots, n-1$.

Proposition III.1.1. *Chaque classe d'équivalence de $\mathcal{M}(\mathcal{X})$ pour la relation $\mathcal{R}$ contient un mot réduit et un seul.*

Démonstration. L'existence est évidente, car si x est non réduit, il existe un mot u tel que $x\mathcal{A}u$ et $l(u) < l(x)$. Comme la fonction l est à valeurs positive ou nulle, en un nombre fini d'étapes on arrive à un mot réduit.

Pour montrer l'unicité, on introduit la construction suivante : pour tout $x = x_1 \dots x_n$ de $\mathcal{M}(\mathcal{X})$ on définit des éléments u_i de la façon suivante :

$u_0 = 1$,
$u_1 = x_1$,
$u_2 = x_1x_2$ si $x_1 \neq x_2^{-1}$
$u_2 = 1$ sinon,

et de façon générale, on pose

$u_{i+1} = u_ix_{i+1}$ si le dernier terme de u_i est différent de x_{i+1}^{-1},
$u_{i+1} = u_{i-1}$ sinon.

Par définition, chaque mot u_i est réduit et $u_i \mathcal{R} (x_1 \dots x_i)$. De plus si x est réduit, alors $x = u_n$.

On appelle u_n la **forme réduite** de x, qu'on note $r(x)$.

L'unicité du mot réduit dans chaque classe d'équivalence de $\mathcal{M}(\mathcal{X})$ pour la relation $\mathcal{R}$ découle des deux lemmes suivants :

Lemme III.1.4. *Si deux mots sont adjacents leurs formes réduites sont égales.*

Démonstration. Soient $x = x_1 \dots x_k x_{k+1} \dots x_n$ et $y = x_1 \dots x_k a a^{-1} x_{k+1} \dots x_n$ deux mots adjacents. Alors les suites u_i et v_i respectivement associées sont telles que $u_0 = v_0, \dots, u_k = v_k$. Montrons que $u_k = v_{k+2}$.

– Si le dernier terme de u_k est différent de a^{-1} alors

$$u_k = v_k,\ v_{k+1} = v_k a,\ v_{k+2} = v_k = u_k.$$

– Si le dernier terme de u_k est a^{-1}, on a $u_k = t a^{-1}$ et, u_k étant réduit, le dernier terme de t est différent de a, donc

$$u_k = v_k,\ v_{k+1} = t,\ v_{k+2} = t a^{-1} = u_k.$$

On en déduit que pour tout $j \geqslant 0$, $u_{k+j} = v_{k+2+j}$ et $u_n = v_{n+2}$, d'où $r(x) = r(y)$.

Lemme III.1.5. *Deux mots équivalents et réduits sont égaux.*

Démonstration. Soient x et y deux mots réduits tels que $x \mathcal{R} y$. Il existe $t_1, \dots, t_n$ tels que $x = t_1,\ y = t_n,\ t_i \mathcal{A} t_{i+1}$, $1 \leqslant i \leqslant n-1$. En considérant la forme réduite de chaque t_i et en appliquant le lemme (III.1.4), on a

$$x = r(t_1) = \dots = r(t_n) = y,$$

d'où le lemme.

En notant L_X l'ensemble des mots réduits correspondants à chaque classe de $\mathcal{M}(\mathcal{X})/\mathcal{R}$ et en considérant la loi interne définie sur L_X par $(r(x), r(y)) \mapsto r(xy)$, on obtient un groupe dans lequel tout élément x s'écrit de manière unique

$$x = x_{i_1}^{n_1} \dots x_{i_k}^{n_k}$$

avec $i_1, \dots, i_k \in \mathbb{N}$, $n_1, \dots, n_k \in \mathbb{Z}$, $x_{i_1}, \dots, x_{i_k} \in X$, tels que $x_{i_j} \neq x_{i_{j+1}}$.

D'autre part, l'application, qui à un élément de $\mathcal{M}(\mathcal{X})/\mathcal{R}$ associe l'unique mot réduit qu'il contient, induit un isomorphisme de groupes de $\mathcal{M}(\mathcal{X})/\mathcal{R}$ sur L_X. Ceci achève la démonstration du théorème (III.1.1). □

Remarques III.1.1.

a) Si $X = \{x\}$, alors $L(X)$ est un monogène infini engendré par x, donc $L(X)$ est isomorphe à $\mathbb{Z}$.

b) Si $card(X) > 1$, alors $L(X)$ est un groupe non abélien.

En effet, soient x et y dans X tels que $x \neq y$. Alors $xyx^{-1}y^{-1}$ est un mot réduit différent de 1, car de longueur 4. Donc xy est différent de yx dans $L(X)$.

***Théorème III.1.2* (propriété universelle du groupe libre).** *Soient G un groupe, S une partie génératrice de G et $i : S \hookrightarrow G$ l'inclusion canonique. Alors le groupe G est libre de base S si et seulement si, pour tout groupe G' et pour toute application $\sigma : S \to G'$, il existe un unique morphisme de groupes $f : G \to G'$ tel que $f \circ i = \sigma$.*

Démonstration. Supposons que $G = L(S)$; tout élément x de $L(S)$ s'écrivant de manière unique $x = s_{i_1}^{n_1} \dots s_{i_k}^{n_k}$, on pose

$$f(x) = \sigma(s_{i_1})^{n_1} \dots \sigma(s_{i_k})^{n_k},$$

et $f(1) = 1_{G'}$. Il est clair qu'on définit ainsi un morphisme de groupes $f : L(S) \to G'$ vérifiant $f \circ i = \sigma$. De plus, si f' est un autre morphisme de groupes vérifiant $f' \circ i = \sigma$, pour tout x de $L(S)$ on a $f(x) = f'(x)$, d'où l'unicité.

Réciproquement, considérons un couple (G, i) vérifiant l'énoncé ci-dessus. On applique alors cet énoncé avec, pour couple (G', σ), le couple $(L(S), j)$, où $j : S \hookrightarrow L(S)$ est l'inclusion canonique. Il existe un unique morphisme $g : G \to L(S)$ tel que $g \circ i = j$. D'autre part, on sait qu'il existe un morphisme de groupes $f : L(S) \to G$ prolongeant l'identité de S. En notant $f_{|S}$ et $g_{|S}$ les restrictions de f et g à S, on déduit de ce qui précède que $g \circ f_{|S} = id_S$ et $f \circ g_{|S} = id_S$, d'où $f \circ g = id_G$ et $g \circ f = id_{L(S)}$. Par conséquent les groupes G et $L(S)$ sont isomorphes et, puisque $f(S) = S$, G est libre de base S. □

Corollaire III.1.1. *Deux groupes libres de base un même ensemble S sont isomorphes par un unique isomorphisme prolongeant l'identité de S.*

Démonstration. Soient G et G' deux groupes libres de bases S. D'après le théorème (III.1.2), il existe un unique morphisme de groupes $f : G \to G'$ tel que $f_{|S} = id_S$ et un unique morphisme de groupes $g : G' \to G$ tel que $g_{|S} = id_S$. On en déduit que $f \circ g = id_{G'}$ et $g \circ f = id_G$. □

Remarque III.1.2. On peut donc parler **du** groupe libre engendré par S.

Théorème III.1.3. *Deux ensembles X et Y sont équipotents si et seulement si les groupes libres $L(X)$ et $L(Y)$ sont isomorphes.*

Démonstration. Supposons que X et Y soient deux ensembles équipotents. Il existe donc une application bijective $\varphi : X \to Y$; le même raisonnement que ci-dessus montre qu'il existe un isomorphisme $L(X) \to L(Y)$ qui prolonge φ.

La réciproque utilise la notion de groupe abélien libre et sera l'objet du TR.VI.A. □

Le théorème III.1.3 justifie la définition suivante :

Définition III.1.5. Si G est un groupe libre, le cardinal d'une partie génératrice libre de G est appelé le ***rang*** de G.

Remarque III.1.3. D'après la proposition III.1.3, deux groupes libres sont **isomorphes** si et seulement s'ils ont **même rang**.

Quelques propriétés des groupes libres seront étudiées au TR.III.C à la fin de ce chapitre. On trouvera au TR.IV.D un exemple de groupe libre de rang 2. Plus généralement, deux symboles distincts engendrent toujours un groupe libre de rang 2.

Théorème III.1.4. *Tout groupe est isomorphe à un quotient d'un groupe libre.*

Démonstration. Soient G un groupe, S une partie génératrice de G et $i : S \hookrightarrow G$ l'injection canonique. D'après le théorème (III.1.2), il existe un morphisme de groupes $f : L(S) \to G$ tel que $f_{|S} = id_S$. On a donc $G = \langle S \rangle = \langle f(S) \rangle$ et f est surjective. On en déduit que G est isomorphe à $L(S)/Ker(f)$. □

Le théorème suivant est fondamental, mais sa démonstration très technique dépasse le cadre de ce livre. Il sera donc admis ; le lecteur désireux d'en voir une démonstration est invité à se reporter à un ouvrage spécialisé en théorie des groupes, par exemple [8].

Théorème III.1.5. *Tout sous-groupe d'un groupe libre est libre.* □

Attention. *Si G est un groupe libre (même de rang fini) et si H est un sous-groupe de G, il n'existe aucune relation* a priori *entre le rang de G et celui de H, comme le prouve l'exercice ci-dessous.*

Exercice III.1. (¶). Soient G un groupe libre de rang 2 et $\{x, y\}$ une base de G.

a) On considère $S = \{y^{-n}xy^n | n \in \mathbb{N}\}$. Montrer que le sous-groupe de G engendré par S est libre de base S.

b) En déduire que le groupe G contient un sous-groupe qui est libre de rang infini dénombrable. Montrer que pour tout $n \in \mathbb{N}$, il existe un sous-groupe de G de rang n.

III.2. Générateurs et relations

Définition III.2.1. Si S est une partie d'un groupe G, le ***sous-groupe normal*** de G ***engendré*** par S, qu'on notera (S), est l'intersection de tous les sous-groupes normaux de G contenant S. Si $S = \emptyset$, on pose $(S) = \{1\}$, où 1 est élément neutre de G.

En général, si G est un groupe engendré par une famille $X = \{x_i\}_{i\in I}$, les générateurs x_i sont liés par des relations.

Exemple III.2.1. Si $G = \langle x\rangle$ est cyclique d'ordre n, le générateur x vérifie la relation $x^n = 1$.

Une relation liant les générateurs x_i, $i \in I$, peut s'écrire sous la forme $r = 1$, où r est un élément du groupe libre $L(X)$.

Définition III.2.2. Soit G un groupe engendré par un ensemble d'éléments $X = \{x_i\}_{i\in I}$, ces éléments vérifiant un ensemble de relations $R = \{r_k = 1_G\}_{k\in K}$. On dit que $\langle X|R\rangle$ est une ***présentation de*** G ***par générateurs et relations*** si G est isomorphe au groupe $L(X)/(R)$, où (R) est le sous-groupe normal du groupe libre $L(X)$, engendré par les $\{r_k\}_{k\in K}$.

Exemples III.2.2.

a) Pour tout ensemble X, $\langle X|\emptyset\rangle$ est une présentation du groupe libre $L(X)$.

b) $\langle x|x^n\rangle$ est une présentation du groupe cyclique d'ordre n.

Exercice III.2. Soient X un ensemble et $Y \subset X$ un sous-ensemble de X. Montrer que $\langle X|Y\rangle$ est une présentation du groupe libre de base $\{X\} \setminus \{Y\}$. (La propriété universelle de groupe libre permet de construire un morphisme de groupes $L(X \setminus Y) \to \langle X|Y\rangle$ et on montre que c'est un isomorphisme.)

Remarque III.2.1. Lorsqu'on donne une présentation d'un groupe G par générateurs et relations, $G = \langle X|R\rangle$, il est utile de supprimer des ensembles X et R les éléments qui sont clairement redondants.

Proposition III.2.1. *Soient $G = \langle X|R\rangle$ et G' un groupe. Pour définir un morphisme de groupes $f : G \to G'$, il suffit de définir $f(x)$ pour $x \in X$ et de vérifier que, pour tout r de R, $f(r) = 1_{G'}$.*

Démonstration. La donnée des $f(x)$ pour $x \in X$ induit, d'après le théorème (III.1.2), un morphisme (qu'on notera encore f) de $L(X)$ dans G'. Si, pour r parcourant R, $f(r) = 1_{G'}$ alors, d'après le théorème de passage au quotient (II.6.2), f induit un morphisme de groupes $L(X)/(R) \to G'$. En composant avec l'isomorphisme $G \simeq L(X)/(R)$, on obtient un morphisme de groupes $G \to G'$. □

Remarque III.2.2. Soit G un groupe présenté par générateurs et relations, $G = \langle X|R\rangle$, et soit $f : G \to G'$ un morphisme de groupes. Montrer que le morphisme f est injectif (*i.e.* $f(x) = 0 \Leftrightarrow x \in (R)$) est équivalent à déterminer **toutes** les relations existantes dans G, liant les générateurs. C'est en général très difficile à faire directement et parfois impossible. Par conséquent, si l'on souhaite montrer que f est un isomorphisme (ce qui est le cas lorsqu'on veut montrer que G est une présentation par générateurs et relations d'un groupe donné G'), il faudra souvent, soit définir un morphisme réciproque, soit montrer, dans le cas où les groupes sont finis, que f est surjectif et que G et G' ont même ordre (*cf.* exercices et TR ci-dessous).

Exercice III.3. Montrer que $\langle\{a, b\}|a^4, b^2, abab\rangle$ est une présentation du groupe diédral D_4 (*cf.* I.1.5.e).

Attention. On prendra garde au fait qu'un groupe peut admettre plusieurs présentations par générateurs et relations.

Exercice III.4. Montrer que $\langle x|x^6\rangle$ et $\langle\{a, b\}|a^2, b^3, aba^{-1}b^{-1}\rangle$, avec $a \neq b$, sont deux présentations du groupe cyclique d'ordre 6.

This page intentionally left blank

THÈMES DE RÉFLEXION

♣ TR.III.A. Présentation du groupe quaternionique $\mathcal{H}$

Le but de cet exercice est de montrer que $\langle\{a,b\}|a^4, a^2b^{-2}, b^{-1}aba\rangle$ est une présentation du groupe quaternionique $\mathcal{H}$ (*cf.* exercice II.2 de la première partie).

La méthode proposée ici n'est pas la plus simple, mais a l'avantage d'utiliser l'intéressant résultat suivant :

Lemme. *Soient G un groupe engendré par une partie S et H un sous-groupe normal de G. Le groupe G/H est engendré par les classes Hs, pour s parcourant S.*

1. *Démontrer ce lemme.*

Notons G le groupe $\langle\{a,b\}|a^4, a^2b^{-2}, b^{-1}aba\rangle$ et posons

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

2. *Montrer que $a \mapsto A$ et $b \mapsto B$ définit un morphisme $\varphi : G \to \mathcal{H}$ et qu'il est surjectif.*

On note H le sous-groupe de G engendré par a, $H = \langle a\rangle$.

3. *Montrer que H est un sous-groupe normal de G.*

4. *Montrer que $|G/H| = 2$.* (Utiliser le lemme.)

5. *En déduire que $|G| = 8$ et que le groupe G est isomorphe au groupe $\mathcal{H}$.*

♠ TR.III.B. Groupes de présentation finie

Le théorème (III.1.4) montre que tout groupe admet une présentation par générateurs et relations. Cependant, si l'ensemble de générateurs est infini, l'étude du groupe n'est pas toujours facilitée par cette présentation.

Beaucoup d'exemples de groupes que nous avons vus dans ce chapitre sont engendrés par un nombre fini d'éléments. Ce sont des groupes de ***type fini***.

Un groupe présenté par générateurs et relations, $G = \langle X|R\rangle$, est dit de ***présentation finie*** si les ensembles X **et** R sont finis.

Pour toute présentation finie d'un groupe G, $G = \langle X|R\rangle$, on introduit le nombre suivant, qui est lié à la présentation donnée,

$$d(X,R) = card(X) - card(R).$$

On remarquera que cet entier, qui appartient à $\mathbb{Z}$, dépend de la présentation donnée de G et on sait qu'elle n'est pas unique. Par exemple, pour les deux présentations du groupe cyclique d'ordre 6 données à l'exercice III.3, on a $d(X,R) = 0$ pour la première et $d(X,R) = -1$ pour la seconde. Ce nombre $d(X,R)$ devient optimal lorsqu'on a éliminé de X et R tous les éléments redondants. Néanmoins, bien que non intrinsèquement lié au groupe G, il permet d'étudier certaines propriétés des groupes de présentation finie.

Soit G un groupe admettant une présentation finie $G = \langle X|R\rangle$ telle que $d(X,R) > 0$. On note $X = \{x_1, \ldots, x_p\}$ et $R = \{r_1, \ldots, r_q\}$, $p > q$.

1. *En posant a_{ij} l'exposant de x_i dans r_j, montrer que le système de q équations à p inconnues*

$$\sum_{i=1}^{p} a_{ij} T_i = O$$

admet une solution non triviale $\{b_1, \ldots, b_p\}$ avec $b_j \in \mathbb{Z}$, $1 \leqslant j \leqslant p$.

2. *Montrer que l'application $X \to \mathbb{Z}$, définie par $x_i \mapsto b_i$, induit un morphisme de groupes $f : G \to \mathbb{Z}$.*

3. *En déduire que si $\langle X|R\rangle$ est une présentation finie d'un groupe G telle que $d(X,R) > 0$, alors le groupe G est infini.*

♠ TR.III.C. Quelques propriétés des groupes libres

Soit $\mathcal{P}$ une propriété. On dit qu'un groupe G est ***résiduellement-$\mathcal{P}$*** si, pour tout élément $x \neq 1$ de G, il existe un sous-groupe normal H_x de G, $x \notin H_x$, tel que le groupe G/H_x possède la propriété $\mathcal{P}$.

Soit G un groupe libre de base $X = \{x_\lambda\}_{\lambda\in\Lambda}$.

Considérons un élément $x \neq 1$ de G, écrit sous la forme $x = x_{\lambda_1}^{\epsilon_1} \ldots x_{\lambda_n}^{\epsilon_n}$, avec $\epsilon_i = 1$, $n \geqslant 1$, les λ_i n'étant pas tous nécessairement distincts.

Pour tout $\lambda_i \in \{\lambda_1, \ldots, \lambda_n\}$, on note σ_{λ_i} la transposition $(i, i+1)$, considérée comme élément de S_{n+1}.

1. *Montrer que l'application $X \to S_{n+1}$ définie par $x_{\lambda_i} \mapsto \sigma_{\lambda_i}$ si $\lambda_i \in \{\lambda_1, \ldots, \lambda_n\}$ et $x_\lambda \mapsto 1$ si $\lambda \notin \{\lambda_1, \ldots, \lambda_n\}$ induit un morphisme de groupes $\varphi : G \to S_{n+1}$.*

2. *On pose $H_x = Ker(\varphi)$. Montrer que $x \notin H_x$ et que le groupe G/H_x est fini.*

3. *En déduire qu'un groupe libre est résiduellement fini.*

4. *Déduire de ce qui précède que si G est un groupe libre, l'intersection de tous ses sous-groupes d'indice fini est réduite à l'élément neutre.*

Un groupe libre étant infini, le sous-groupe réduit à l'élément neutre ne peut être d'indice fini. Comparer alors le résultat ci-dessus et la proposition (II.1.3).

5. *Montrer que si un groupe G est résiduellement-$\mathcal{P}$, il est isomorphe à un sous-groupe d'un produit direct de groupes possédant la propriété $\mathcal{P}$.*

6. *En déduire qu'un groupe libre est isomorphe à un sous-groupe d'un produit direct de groupes finis.*

♠ TR.III.D. Produit libre de groupes

Soit $(G_i)_{i\in I}$ une famille de groupes. Nous allons construire un nouveau groupe, noté $\coprod_{i\in I} G_i$, muni de morphismes naturels de groupes $\lambda_i : G_i \to \coprod_{i\in I} G_i$ et montrer que ce groupe et ces morphismes constituent une solution du problème universel de somme de groupes évoqué à la remarque (I.3.4).

Pour faciliter la compréhension de cette construction, nous allons d'abord étudier le cas où $card(I) = 2$.

Soient G et G' deux groupes. On pose $X = G \cup G'$ et on appelle ***mot*** sur X toute suite finie $g_1 \ldots g_n$, où $n \in \mathbb{N}$ et g_i appartient à G ou à G', pour tout i, $1 \leqslant i \leqslant n$. Le mot correspondant à la partie vide de X sera noté 1 et on note $\mathcal{M}(\mathcal{X})$ l'ensemble des mots sur X.

Deux mots $g_1 \ldots g_n$ et $h_1 \ldots h_p$ sont ***égaux*** si $n = p$ et $g_i = h_i$ pour tout i, $1 \leqslant i \leqslant n$.

Deux mots

$$g_1 \ldots g_{i-1} g_i g_{i+1} \ldots g_n \quad \text{et} \quad g_1 \ldots g_{i-1} g_{i+1} \ldots g_n$$

sont ***élémentairement équivalents*** si g_i est l'élément neutre du groupe auquel il appartient, de même que deux mots

$$g_1 \ldots g_{i-1} g_i g_{i+1} g_{i+2} \ldots g_n \quad \text{et} \quad g_1 \ldots g_{i-1} h_i g_{i+2} \ldots g_n$$

tels que g_i et g_{i+1} sont dans le même groupe et que $g_i g_{i+1} = h_i$.

Deux mots a et b de $\mathcal{M}(\mathcal{X})$ sont ***équivalents*** s'il existe une suite finie de mots $u_1, \dots, u_n$ tels que $a = u_1$ et $b = u_n$, avec u_i élémentairement équivalent à u_{i+1} pour $1 \leqslant i \leqslant n-1$.

1. *Montrer que ceci définit une relation d'équivalence $\mathcal{R}$ sur $\mathcal{M}(\mathcal{X})$.*

Soient $a = g_1 \dots g_n$ et $b = h_1 \dots h_p$ deux mots. On définit leur ***produit*** par

$$ab = g_1 \dots g_n h_1 \dots h_p$$

et pour tout mot c on pose $c1 = 1c = c$.

2. *Montrer que la relation d'équivalence $\mathcal{R}$ définie sur $\mathcal{M}(\mathcal{X})$ est compatible au produit.*

On note $[a]$ la classe d'un mot a de $\mathcal{M}(\mathcal{X})$ dans l'ensemble quotient $\mathcal{M}(\mathcal{X})/\mathcal{R}$.

3. *Montrer que l'ensemble quotient $\mathcal{M}(\mathcal{X})/\mathcal{R}$ muni du produit défini par $[a][b] = [ab]$ est un groupe, dont l'élément neutre est* $[1]$.

On procède maintenant à une « réduction » des mots de la façon suivante : dans un mot $a = g_1 \dots g_n$, si des g_i consécutifs sont dans le même groupe G ou G' on les remplace par leur produit dans ce groupe et on supprime tous les termes égaux aux éléments neutres de G et G'. On note $r(a)$ le mot auquel on arrive ainsi et on l'appelle mot ***réduit***.

On note $G \coprod G'$ l'ensemble des mots réduits.

4. *Montrer que chaque classe d'équivalence de mots de $\mathcal{M}(\mathcal{X})$ contient un et un seul mot réduit.*

5. *Montrer que $G \coprod G'$ muni du produit $r(a)r(b) = r(ab)$ est un groupe.*

On appelle ce groupe le ***produit libre*** des groupes G et G'.

6. *Montrer que dans $G \coprod G'$ tout élément a une écriture unique $g_1 g'_1 g_2 g'_2 \dots g_n g'_n$ avec, pour tout i, $1 \leqslant i \leqslant n$, $g_i \in G$ et $g'_i \in G'$, chacun des termes de cette écriture étant différent des éléments neutres de G et G'.*

Cas général

On pose $X = \cup_{i \in I} G_i$ et on suppose que l'ensemble I est ordonné afin d'éviter les doubles indices. On appelle ***mot*** sur X toute suite finie $g_1 \dots g_n$, où $n \in \mathbb{N}$ et g_i appartient à un certain groupe G_j pour tout i, $1 \leqslant i \leqslant n$. Le mot correspondant à la partie vide de X sera noté 1 et on note $\mathcal{M}(\mathcal{X})$ l'ensemble des mots sur X.

Deux mots $g_1 \dots g_n$ et $h_1 \dots h_p$ sont ***égaux*** si $n = p$ et $g_i = h_i$ pour tout i, $1 \leqslant i \leqslant n$.

Deux mots

$$g_1 \dots g_{i-1} g_i g_{i+1} \dots g_n \quad \text{et} \quad g_1 \dots g_{i-1} g_{i+1} \dots g_n$$

sont ***élémentairement équivalents*** si g_i est l'élément neutre du groupe auquel il appartient, de même que deux mots

$$g_1 \dots g_{i-1} g_i g_{i+1} g_{i+2} \dots g_n \quad \text{et} \quad g_1 \dots g_{i-1} h_i g_{i+2} \dots g_n$$

tels que g_i et g_{i+1} sont dans le même groupe et que $g_i g_{i+1} = h_i$.

Deux mots a et b de $\mathcal{M}(\mathcal{X})$ sont ***équivalents*** s'il existe une suite finie de mots $u_1, \dots, u_n$ tels que $a = u_1$ et $b = u_n$, avec u_i élémentairement équivalent à u_{i+1} pour $1 \leqslant i \leqslant n-1$.

7. *Montrer que ceci définit une relation d'équivalence $\mathcal{R}$ sur $\mathcal{M}(\mathcal{X})$.*

Soient $a = g_1 \dots g_n$ et $b = h_1 \dots h_p$ deux mots. On définit leur ***produit*** par

$$ab = g_1 \dots g_n h_1 \dots h_p$$

et, pour tout mot c, on pose $c1 = 1c = c$.

8. *Montrer que la relation d'équivalence $\mathcal{R}$ définie sur $\mathcal{M}(\mathcal{X})$ est compatible au produit.*

On note $[a]$ la classe d'un mot a de $\mathcal{M}(\mathcal{X})$ dans l'ensemble quotient $\mathcal{M}(\mathcal{X})/\mathcal{R}$.

9. *Montrer que l'ensemble quotient $\mathcal{M}(\mathcal{X})/\mathcal{R}$ muni du produit défini par $[a][b] = [ab]$ est un groupe dont l'élément neutre est $[1]$.*

Un mot a est dit ***réduit*** si $a = 1$ ou si $a = g_1 \dots g_n$ est tel que $\forall i,\ 1 \leqslant i \leqslant n$, g_i n'est pas égal à l'élément neutre du groupe auquel il appartient et g_i et g_{i+1} ne sont pas dans le même groupe G_j, $\forall i,\ 1 \leqslant i \leqslant n-1$.

Comme à la proposition III.1.1, à tout mot a on associe sa forme réduite $r(a)$.

10. *Montrer que chaque classe d'équivalence de mots de $\mathcal{M}(\mathcal{X})$ contient un et un seul mot réduit.*

On note $\coprod_{i\in I} G_i$ l'ensemble des mots réduits.

11. *Montrer que $\coprod_{i\in I} G_i$ muni du produit $r(a)r(b) = r(ab)$ est un groupe.*

On appelle ce groupe le ***produit libre*** des groupes $(G_i)_{i\in I}$.

12. *Montrer que dans $\coprod_{i\in I} G_i$ tout élément a a une écriture unique $a = g_1 \dots g_n$, où $n \in \mathbb{N}$, deux éléments consécutifs dans cette écriture n'appartenant pas au même groupe G_j et aucun d'entre eux n'étant égal à l'élément neutre du groupe auquel il appartient, et $a = 1$ si $n = 0$.*

13. *Montrer que $\forall i \in I$ l'application $\lambda_i : G_i \to \coprod_{i\in I}$ définie par $\lambda_i(g_i) = r(g_i)$ est un morphisme (injectif) de groupes.*

Nous allons maintenant montrer que $(\coprod_{i\in I} G_i,\ \lambda_i)$ est solution du problème universel de somme des groupes $(G_I)_{i\in I}$.

14. *Montrer que pour tout groupe G et toute famille de morphismes de groupes $f_i : G_i \to G$, il existe un* ***unique*** *morphisme de groupes $g : \coprod_{i\in I} \to G$ tel que $g \circ \lambda_i = f_i$, $i \in I$.*

On peut mettre en relation la construction ci-dessus et les groupes libres de la façon suivante :

15. *Soit $X = \{x_i\}_{i\in I}$ un ensemble. Montrer que le groupe libre $L(X)$ est isomorphe au produit libre des groupes monogènes infinis $\langle x_i\rangle$, $i \in I$.*

IV

GROUPES OPÉRANT SUR UN ENSEMBLE

Le groupe D_4 introduit à l'exemple (I.1.2.c) est le groupe des isométries du carré. Notons E l'ensemble des sommets du carré. Pour tout élément f de D_4, il est clair que l'image par f de tout élément x de E est encore un élément de E. Autrement dit, on a une application $D_4 \times E \to E$, définie par $(f, x) \mapsto f(x)$, qui est compatible avec la composition des applications et telle que, si f est l'identité, alors $f(x) = x$. Mais on peut également définir le groupe D_4 abstraitement (par exemple, par sa table) ; son interprétation comme groupe des isométries du carré permet alors, d'après ce qui précède, de considérer le groupe D_4 comme « opérant » sur un ensemble E à quatre éléments. L'objet de ce chapitre est de formaliser ce point de vue et de voir que cette situation permet d'obtenir des renseignements, aussi bien sur l'ensemble sur lequel le groupe opère, que sur le groupe lui-même.

IV.1. Définitions – Exemples

Définition* IV.1.1.** Soit G un groupe (noté multiplicativement, d'élément neutre 1) et soit E un ensemble non vide. Une ***opération à gauche de G ***sur*** E est la donnée d'une application

$$G \times E \longrightarrow E, \qquad (g, x) \longmapsto g.x$$

satisfaisant aux deux conditions suivantes :

(i) $\forall (g_1, g_2) \in G \times G,\ \forall x \in E,\ (g_1 g_2).x = g_1.(g_2.x)$

(ii) $\forall x \in E,\ 1.x = x.$

***Remarque* IV.1.1.** On définit de façon analogue une opération à droite de G sur E.

Dans toute la suite, on ne considérera, sauf mention explicite, que des actions à gauche de G sur E et on ne précisera plus le côté. Au lieu de dire « soient G un groupe, E un ensemble non vide et une action de G sur E », on dira « soit G un ***groupe opérant sur un ensemble*** E ».

***Proposition* IV.1.1.** *Soit G un groupe opérant sur un ensemble E.*

(i) *Pour tout g dans G, l'application*

$$\gamma_g : E \longrightarrow E, \qquad x \longmapsto g.x$$

est une permutation de E.

(ii) *Soit S_E le groupe des permutations de E, l'application*

$$\gamma : G \longrightarrow S_E, \qquad g \longmapsto \gamma_g$$

est un morphisme de groupes.

Démonstration. (i). Il est clair que pour tout élément x de E on a $\gamma_g(g^{-1}.x) = x$, γ_g est donc surjective. D'autre part,

$$[\gamma_g(x) = \gamma_g(y)] \;\Rightarrow\; [g^{-1}.\gamma_g(x) = g^{-1}.\gamma_g(y)] \;\Rightarrow\; [x = y]$$

et γ_g est injective.

(ii). Pour tous éléments g et h dans G et x dans E, on a

$$(\gamma_g \circ \gamma_h)(x) = g.(h.x) = (gh).x = \gamma_{gh}(x),$$

d'où $\gamma_g \circ \gamma_h = \gamma_{gh}$ et γ est un morphisme de groupes. □

***Corollaire* IV.1.1.** *La donnée d'une action d'un groupe G sur un ensemble E est équivalente à la donnée d'un morphisme de groupes de G dans S_E.*

Démonstration. Compte tenu de la proposition (IV.1.1.(ii)), il suffit de prouver que la donnée d'un morphisme de groupes $f : G \to S_E$ définit une action de G sur E. Pour tout $g \in G$ et $x \in E$, on pose $g.x = f(g)(x)$. Alors,

$$\forall (g,h) \in G \times G,\ \forall x \in E,\ g.(h.x) = f(g)(f(h)(x)) =$$

$$(f(g) \circ f(h))(x) = f(gh)(x) = (gh).x.$$

De plus $1.x = id_E(x) = x$, donc $g.x = f(g)(x)$ définit une action de G sur E. □

***Exemples* IV.1.1.**

a) Tout groupe G opère sur lui-même par « translation »

$$G \times G \longrightarrow G, \qquad (g, x) \longmapsto g.x = gx.$$

b) Tout groupe G opère sur lui-même par conjugaison

$$G \times G \longrightarrow G, \qquad (g, x) \longmapsto g.x = gxg^{-1}.$$

c) Tout groupe G opère sur $\mathcal{P}(G)$, ensemble des parties de G, par conjugaison

$$G \times \mathcal{P}(G) \longrightarrow \mathcal{P}(G), \qquad (g, S) \longmapsto g.S = gSg^{-1}, \qquad (g, \emptyset) \longmapsto \emptyset.$$

d) Soit H un sous-groupe d'un groupe G. Alors G opère sur l'ensemble $(G/H)_g$ des classes à gauche modulo H, par

$$G \times (G/H)_g \longrightarrow (G/H)_g, \qquad (g, xH) \longmapsto g.(xH) = gxH.$$

e) Soit E un ensemble non vide. Alors le groupe S_E des permutations de E opère sur E par

$$S_E \times E \longrightarrow E, \qquad (\sigma, x) \longmapsto \sigma.x = \sigma(x).$$

Définition* IV.1.2.** Soit G un groupe opérant sur un ensemble E. Le ***noyau de l'action est le noyau de l'homomorphisme de groupes $\gamma : G \to S_E$ définissant l'action de G sur E.

Ce noyau permet d'obtenir des renseignements sur le groupe G comme, par exemple, les résultats suivants :

***Exercice* IV.1.**

1. Soient G un groupe et H un sous-groupe de G. Montrer que le noyau de l'action de G sur $(G/H)_g$ définie dans l'exemple (IV.1.1.d) est le sous-groupe $\bigcap_{x \in G} xHx^{-1}$. Montrer que c'est le plus grand sous-groupe normal dans G contenu dans H.

2. En déduire que si G est un groupe simple (*cf.* TR.II.B), pour tout sous-groupe $H \neq G$ de G, G est isomorphe à un sous-groupe de $S_{[G:H]}$.

IV.2. Stabilisateurs – Orbites

Il est clair que dans l'action de D_4 sur le carré, l'élément Δ_1 laisse fixe les sommets de la première diagonale. On dit que Δ_1 stabilise ces deux éléments de E.

Proposition - Définition IV.2.1. *Soit G un groupe opérant sur un ensemble E et soit x un élément fixé de E. L'ensemble $Stab_G(x) = \{g \in G : gx = x\}$ est un sous-groupe de G, appelé le stabilisateur de x.*

Démonstration. Soient g et h des éléments de $Stab_G(x)$. On a $g.x = x$ et $h.x = x$, d'où

$$(gh^{-1}).x = (gh^{-1}).(h.x) = g.((h^{-1}h).x) = g.(1.x) = g.x = x,$$

d'où gh^{-1} appartient à $Stab_g(x)$, qui est donc un sous-groupe de G. □

Définition IV.2.1. Soit G un groupe opérant sur un ensemble E et soit x un élément fixé de E. L'ensemble $\Omega_x = \{g.x, g \in G\}$ est appelé l'***orbite*** de x sous l'action de G.

Remarque IV.2.1. Soit G un groupe opérant sur un ensemble E. La relation $\mathcal{R}$ définie sur E par

$$[x\mathcal{R}y] \Longleftrightarrow [\exists\, g \in G, y = g.x]$$

est une relation d'équivalence. L'orbite Ω_x d'un élément x de E sous l'action de G est une classe d'équivalence pour la relation $\mathcal{R}$. Les orbites des éléments de E sous l'action de G forment donc une partition de E.

Exemples IV.2.1. Pour les exemples (IV.1.1), on a respectivement :

a) $Stab_G(x) = \{1_G\}$; $\Omega_x = G$ $(\forall x \in G)$.

b) $Stab_G(x) = Z_G(x)$; $\Omega_x =$ classe de conjugaison de x.

c) $Stab_G(S) = N_G(S)$; $\Omega_S =$ classe de conjugaison de S.

d) $Stab_G(xH) = xHx^{-1}$; $\Omega_{xH} = G/H$.

e) $Stab_{S_E}(x) \simeq S_{E-\{x\}}$; $\Omega_x = E$.

Exercice IV.2. Montrer que si H est un sous-groupe d'indice n de S_n, il est isomorphe au groupe S_{n-1}. (On utilisera le TR.II.B et l'exercice II.1.)

Proposition IV.2.2. *Soient G un groupe opérant sur un ensemble E et x un élément de E. Alors, pour tout élément y de Ω_x, les sous-groupes $Stab_G(x)$ et $Stab_G(y)$ sont conjugués.*

Démonstration. Soit $y \in \Omega_x$; il existe $g \in G$ tel que $y = g.x$. Nous allons montrer que $G_y = gG_xg^{-1}$. Pour tout $h \in G_y$, on a $h.y = y$, d'où $(hg).x = g.x$ *i.e.* $(g^{-1}hg).x = x$, *i.e.* $(g^{-1}hg) \in G_x$, d'où $G_y \subseteq gG_xg^{-1}$. L'inclusion dans l'autre sens est une vérification immédiate. □

Proposition IV.2.3. *Soit G un groupe opérant sur un ensemble E. Alors pour tout élément x de E, on a*

$$card(\Omega_x) = [G : Stab_G(x)].$$

Démonstration. Par définition, $[G : Stab_G(x)]$ est le cardinal de l'ensemble $G/Stab_G(x)$. Nous allons construire une application de Ω_x sur $G/Stab_G(x)$ et montrer qu'elle est bijective. Tout élément de Ω_x s'écrit $g.x$, pour un certain $g \in G$. Posons $\varphi(g.x) = gStab_G(x)$ et montrons que cela définit bien une application de Ω_x sur $G/Stab_G(x)$: si $g.x = h.x$, alors $x = (g^{-1}h).x$ et $g^{-1}h$ appartient à $Stab_G(x)$, d'où $gStab_G(x) = hStab_G(x)$ et φ est bien définie. Il est évident qu'elle est surjective. D'autre part, $gStab_G(x) = hStab_G(x)$ équivaut à $(g^{-1}h) \in Stab_G(x)$, i.e. $(g^{-1}h).x = x$, d'où $g.x = h.x$ et φ est injective. □

Exercice IV.3. Montrer que le cardinal de la classe de conjugaison d'un élément quelconque d'un groupe fini divise l'ordre de ce groupe.

Corollaire IV.2.1. *Soit G un groupe opérant sur un ensemble fini E et soit $\{x_i\}$, $1 \leqslant i \leqslant r$, une famille de représentants des orbites distinctes, alors :*

$$Card(E) = \sum_{i=1}^{r} [G : Stab_G(x_i)].$$

Démonstration. C'est une conséquence immédiate de la proposition (IV.2.3) et du fait que les Ω_x, $x \in E$, forment une partition de E. □

Corollaire IV.2.2 **(équation aux classes).** *Soit G un groupe fini opérant sur lui-même par conjugaison et soit $\{x_i\}$, $1 \leqslant i \leqslant r$, une famille de représentants des orbites distinctes, alors :*

$$Card(G) = \sum_{i=1}^{r} [G : Z_G(x_i)].$$

Démonstration. On a vu dans l'exemple (IV.2.1.b) que, dans ce cas, $Stab_G(x_i) = Z_G(x_i)$. □

Corollaire IV.2.3. *Soit G un groupe fini opérant sur lui-même par conjugaison et soit $\{x_i\}$, $1 \leqslant i \leqslant k$, une famille de représentants des orbites distinctes non ponctuelles (*i.e. *non réduites à un élément), alors :*

$$Card(G) = Card(Z(G)) + \sum_{i=1}^{k} [G : Z_G(x_i)].$$

Démonstration. Si le groupe G est abélien, toutes les orbites sont ponctuelles et $Z(G) = G$, on a donc bien l'égalité.

Si le groupe G est non abélien, l'orbite Ω_x d'un élément x est ponctuelle, $\Omega_x = \{x\}$, si et seulement si x appartient à $Z(G)$. Pour les éléments x de $Z(G)$, on a $Stab_G(x) = G$, d'où $[G : Stab_G(x)] = 1$. Par conséquent, dans l'équation aux classes, la somme des termes qui correspondent aux orbites ponctuelles est égale à $card(Z(G))$. D'où le résultat. □

Exercice IV.4. Dans cet exercice, p est un nombre premier.

1. Montrer que si G est un groupe d'ordre p^n, $n \geqslant 1$, le centre $Z(G)$ de G n'est pas réduit à l'élément neutre.

2. En déduire que :

a) Tout groupe d'ordre p^2 est abélien.

b) Un groupe G d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. (On considérera un sous-groupe H d'ordre p de G et un sous-groupe K engendré par un élément de G n'appartenant pas à H.)

c) Pour tout entier $n \geqslant 1$ et pour tout entier q, $0 \leqslant q \leqslant n$, tout groupe non abélien d'ordre p^n possède un sous-groupe normal d'ordre p^q. (On fera un raisonnement par récurrence sur n et on appliquera l'hypothèse de récurrence au groupe $G/Z(G)$.)

Le cas des groupes abéliens sera traité dans l'exercice (VI.5.3).

3. Soit H un sous-groupe d'un groupe fini G tel que $[G : H] = p$ soit le plus petit nombre premier divisant $|G|$. Montrer que H est un sous-groupe normal de G. (On utilisera l'équation aux classes associée à l'action de H sur $(G/H)_g$ induite par l'action par translation à gauche de G sur $(G/H)_g$.)

IV.3. Produit semi-direct

A - Groupes opérant sur un groupe

Soient G et H deux groupes et

$$G \times H \longrightarrow H, \qquad (g,x) \longmapsto g.x$$

une action de G sur l'ensemble H. On a vu que ceci est équivalent à la donnée d'un homomorphisme de groupes

$$\gamma : G \longrightarrow S_H, \qquad g \longmapsto \gamma_g$$

avec $\gamma_g(x) = g.x$.

Supposons que $Im(\gamma) < Aut(H)$. Alors

$$\forall (x,y) \in H \times H, \ \forall g \in G, \quad g.(xy) = (g.x)(g.y).$$

Réciproquement, si l'action de G sur H satisfait à cette condition supplémentaire, alors pour tout g de G et pour tout (x,y) de $H \times H$, on a $\gamma_g(xy) = \gamma_g(x)\gamma_g(y)$. Autrement dit γ_g est un endomorphisme de H et, puisqu'il est bijectif, c'est un automorphisme. D'où $Im(\gamma) < Aut(H)$.

Définition IV.3.1. Une opération d'un groupe G sur un groupe H satisfaisant à la condition $Im(\gamma) < Aut(H)$ est dite ***opération par automorphismes***.

Attention. Dans toute la suite, lorsqu'un groupe opérera sur un autre groupe, on supposera que l'opération est par automorphismes.

Exemple IV.3.1. L'action d'un groupe sur lui-même par conjugaison est par automorphismes. Ce n'est pas le cas pour l'action par translation.

B - Produit semi-direct de sous-groupes

Définition IV.3.2. Soient G un groupe, H et K deux sous-groupes de G. On dira que G est le ***produit semi-direct de*** K ***par*** H si :

(i) K est un sous-groupe normal de G

(ii) $G = KH$

(iii) $K \cap H = \{1\}$.

Remarque IV.3.1. La condition (i) implique que le groupe G opère par conjugaison sur K. Par restriction, on a donc une action par conjugaison de H sur K et l'homomorphisme $\gamma : H \to S_K$ ainsi déterminé vérifie $Im\gamma < Aut(K)$. De plus, dans $G = KH$, on a

$$\forall (k,k') \in K \times K,\ \forall (h,h') \in H \times H,\quad k\,h\,k'h' = k(h\,k'h^{-1})h\,h'.$$

Si on note l'action de H sur K par $(h,k) \mapsto {}^hk$, on a

$$k\,h\,k'h' = k({}^hk')h\,h',$$

d'où une écriture particulière du produit dans $G = KH$.

Remarque IV.3.2. Les conditions (ii) et (iii) de la définition (IV.3.2) impliquent que le groupe G est en bijection ensembliste avec le produit $K \times H$, mais la loi interne définie est très différente de celle du produit direct de sous-groupes $K \times H$, comme le montre l'écriture ci-dessus.

Exercice IV.5. On sait que $D_4 \simeq \langle \{a,b\} | a^4, b^2, abab \rangle$ (exercice III.4). En considérant les sous-groupes de D_4, $K = \langle a \rangle$, $H = \langle b \rangle$, montrer que le groupe D_4 est le produit semi-direct de K par H.

C - Produit semi-direct de groupes

On généralise l'écriture du produit décrite ci-dessus.

On considère deux groupes G et N et une action de G sur N définie par $\gamma \in Hom(G, Aut(N))$. On notera cette action

$$(g,x) \longmapsto {}^gx,\quad g \in G, x \in N.$$

Proposition - Définition IV.3.1. *Avec les notations ci-dessus, l'ensemble $N \times G$ muni de la loi de composition*

$$(x,g)(y,h) = (x\ {}^gy, gh)$$

où $(x,y) \in N \times N$ et $(g,h) \in G \times G$, est un groupe, en général non abélien, appelé produit semi-direct de N par G relativement à γ et noté $N \underset{\gamma}{\times} G$.

Démonstration. Montrons que la loi ainsi définie est associative. Soient $(x,g),(y,h),(z,k)$ trois éléments de $N \times G$. On a

$$((x,g)(y,h))(z,k) = (x\ {}^gy, gh)(z,k) = (x\ {}^gy\ {}^{gh}z, ghk)$$

et

$$(x,g)((y,h)(z,k)) = (x,g)(y\ {}^{h}z, hk) = (x\ {}^{g}(y^{h}z), ghk)$$

et, l'action de G sur N étant par automorphismes, ce dernier terme est égal à $(x\ {}^{g}y\ {}^{gh}z, ghk)$, d'où l'associativité.

On vérifie aisément que l'élément neutre est $(1_N, 1_G)$ et que

$$(x,g)^{-1} = ({}^{(g^{-1})}x^{-1}, g^{-1}). \qquad \square$$

Proposition IV.3.2.

(i) *Avec les notations ci-dessus, les applications*

$$\alpha : \ G \to N \underset{\gamma}{\times} G, \qquad g \mapsto (1,g)$$

$$\beta : \ N \to N \underset{\gamma}{\times} G, \qquad x \mapsto (x,1)$$

sont des morphismes injectifs de groupes.

(ii) *En posant $K = Im(\beta)$ et $H = Im(\alpha)$, le groupe $N \underset{\gamma}{\times} G$ est le produit semi-direct du sous-groupe K par le sous-groupe H.*

(iii) *En identifiant N à K et G à H par les morphismes β et α, l'action de $g \in G$ sur $x \in N$ s'identifie à $(g,x) \mapsto gxg^{-1}$ dans $N \underset{\gamma}{\times} G$.*

Démonstration. (i). Évident.

(ii). Montrons que K est un sous-groupe normal de $N \underset{\gamma}{\times} G$. Soient $(x,1) \in K$ et $(y,g) \in N \underset{\gamma}{\times} G$, alors $(y,g)(x,1)(y,g)^{-1} = (y\ {}^{g}xy^{-1}, 1) \in K$. On en déduit que KH est un sous-groupe de $N \underset{\gamma}{\times} G$ et, comme $(x,g) = (x,1)(1,g)$, on a $KH = N \underset{\gamma}{\times} G$. De plus, $(x,g) \in K \cap H$ si et seulement si $x = 1$ et $g = 1$, *i.e.* $K \cap H = (1,1)$.

(iii). Les identifications par α et β reviennent à remplacer $(1,g)$ par g, $(x,1)$ par x et $(1,1)$ par 1. Alors (x,g) s'écrit xg et la multiplication dans $N \underset{\gamma}{\times} G$ s'écrit $xgyh = xgyg^{-1}gh = x\ {}^{g}ygh$, avec ${}^{g}y = gyg^{-1}$. $\square$

Remarque IV.3.3. Si $\gamma \in Hom(G, Aut(N))$ est tel que $\gamma(g) = id_N$ pour tout $g \in G$, alors $N \underset{\gamma}{\times} G$ est le produit direct $N \times G$.

Exemple IV.3.2. On considère C_4 et C_2 deux groupes cycliques d'ordre respectif 4 et 2. On pose $C_4 = \langle a \rangle$ avec $a^4 = 1$, $C_2 = \langle b \rangle$ avec $b^2 = 1$ et on considère $\gamma : C_2 \to Aut(C_4)$ le morphisme de groupes défini par

$$\gamma(1) = id_{C_4}, \gamma(b)(x) = x^{-1}, x \in C_4.$$

Alors, d'après l'exercice IV.5 et la proposition (IV.3.2.(iii)), le produit semi-direct $C_4 \underset{\gamma}{\times} C_2$ est isomorphe au groupe diédral D_4.

On peut se demander si deux éléments distincts γ et δ de $Hom(G, Aut(N))$ peuvent donner deux produits semi-directs $N \underset{\gamma}{\times} G$ et $N \underset{\delta}{\times} G$ isomorphes. L'exercice ci-dessous donne une réponse partielle à cette question.

Exercice IV.6.

1. Soient $\gamma \in Hom(G, Aut(N))$ et $\varphi \in Aut(G)$. Montrer que γ et $\gamma \circ \varphi$ définissent deux produits semi-directs $N \underset{\gamma}{\times} G$ et $N \underset{\gamma\circ\varphi}{\times} G$ isomorphes.

2. Soient γ et δ deux éléments distincts de $Hom(G, Aut(N))$. Montrer que s'il existe un élément $\psi \in Aut(N)$ tel que

$$\forall g \in G, \gamma(g) = \psi \circ \delta(g) \circ \psi^{-1}$$

les produits semi-directs $N \underset{\gamma}{\times} G$ et $N \underset{\delta}{\times} G$ sont isomorphes.

IV.4. Opérations transitives, fidèles

Définition IV.4.1. On dit qu'un groupe G opère ***transitivement*** sur un ensemble E si

$$\forall (x, y) \in E \times E, \exists g \in G, \ y = g.x.$$

C'est équivalent à dire qu'il n'y a qu'une seule orbite.

Exemples IV.4.1.

a) Un groupe G opère transitivement sur lui-même par translation.

b) Un groupe $G \neq \{1\}$ n'opère pas transitivement sur lui-même par conjugaison.

Proposition IV.4.1.

(i) *Soient G un groupe et H un sous-groupe de G. Alors G opère transitivement par translation à gauche sur l'ensemble $(G/H)_g$ des classes à gauche modulo H.*

(ii) *Si G opère transitivement sur un ensemble E, il existe un sous-groupe H de G et une bijection équivariante $E \simeq (G/H)_g$* (i.e. *l'action de G sur E se transporte via cette bijection en l'action de G par translation à gauche sur $(G/H)_g$).*

Démonstration. (i). Pour l'opération de G sur $(G/H)_g$ par translation définie par $(g, xH) \mapsto gxH$, on a $\Omega_H = (G/H)_g$.

(ii). Si G opère transitivement sur E, on a $E = \Omega_x$, qui est équipotent à $(G/Stab_G(x))_g$, et la bijection $g.x \mapsto gStab_G(x)$ vérifie la propriété énoncée. □

Dans l'action de D_4 sur le carré, il est clair que le seul élément de D_4 qui laisse invariant chaque sommet est l'identité. On formalise cette propriété de la façon suivante :

Définition IV.4.2. On dit qu'un groupe G opère ***fidèlement*** sur un ensemble E si

$$(g \in G,\ g.x = x,\ \forall x \in E) \Longrightarrow (g = 1).$$

C'est équivalent à dire que l'homomorphisme $\gamma : G \to S(E)$, associé à l'action de G sur E, est injectif.

Exemples IV.4.2.

a) L'action d'un groupe G sur lui-même par translation est fidèle.

b) En général, l'action d'un groupe $G \neq \{1\}$ sur lui-même par conjugaison n'est pas fidèle, puisque le noyau de cette action est le centre $Z(G)$ de G.

IV.5. Points fixes

Définition IV.5.1. Soit G un groupe opérant sur un ensemble E. Le sous-ensemble de E

$$E_G = \{x \in E \,|\, g.x = x, \forall g \in G\}$$

est appelé sous-ensemble des ***points fixes*** de E sous l'action de G.

Remarques IV.5.1.

a) On a

$$E_G = \{x \in E \,|\, Stab_G(x) = G\} = \{x \in E \,|\, \Omega_x = \{x\}\}.$$

b) E_G peut être vide (par exemple dans le cas où G opère transitivement sur E).

Exemples IV.5.1.

a) Si un groupe G opère par conjugaison sur lui-même, l'ensemble des points fixes est le centre $Z(G)$ de G.

b) Si un groupe $G \neq \{1\}$ opère par translation sur lui-même, l'ensemble des points fixes est vide.

Proposition IV.5.1. *Soient p un nombre premier, n un entier non nul et G un groupe fini d'ordre p^n opérant sur un ensemble fini E. Alors*

$$Card(E_G) \equiv Card(E) \pmod{p}.$$

Démonstration. Un élément x appartient à E_G si et seulement si $\Omega_x = \{x\}$, donc $Card(E_G)$ est le nombre d'orbites ponctuelles. Soient $(x_i)_{i\in I}$ une famille de représentants des orbites non ponctuelles. Alors

$$Card(E) = Card(E_G) + \sum_{i\in I} Card(\Omega_{x_i}).$$

Or, $Card(\Omega_{x_i}) = [G : Stab_G(x_i)]$ est différent de 1 et divise p^n, il est donc de la forme p^{α_i}, avec $\alpha_i \geqslant 1$. Donc $(Card(E) - Card(E_G))$ est divisible par p. □

THÈMES DE RÉFLEXION

♣ TR.IV.A. Groupes diédraux D_n

Nous avons introduit au chapitre I le groupe D_4 des isométries du carré et avons indiqué dans l'exemple (IV.3.2) que ce groupe est un produit semi-direct du groupe cyclique $\mathbb{Z}/4\mathbb{Z}$ par le groupe cyclique $\mathbb{Z}/2\mathbb{Z}$. Nous allons ici introduire le groupe diédral général D_n comme groupe d'isométries du polygône régulier à n côtés et montrer que c'est un produit semi-direct du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ par le groupe cyclique $\mathbb{Z}/2\mathbb{Z}$.

Soient $n \in \mathbb{N}$, $n \geqslant 3$, et P_n le polygône plan régulier convexe à n sommets $A_0, \ldots, A_{n-1}$ inscrit dans le cercle unité, dont on notera O le centre. On note D_n le groupe des isométries du plan qui laissent P_n invariant.

1. *Vérifier que la symétrie orthogonale s d'axe OA_0 et la rotation r de centre O et d'angle $2\pi/n$ appartiennent à D_n.*

2. *Montrer que le cardinal de D_n est $2n$.*

3. *Montrer que $srs = r^{-1}$ et en déduire que pour tout $m \in \mathbb{N}$, on a $sr^m s = r^{-m}$.*

4. *En déduire que $\langle \{a, b\} |\ a^n, b^2, abab \rangle$ est une présentation par générateurs et relations du groupe D_n.*

On pose $G = \langle r \rangle$ et $H = \langle s \rangle$ et on considère l'action de H sur G donnée par le morphisme de groupes $\gamma : H \to Aut(G)$ défini par $\gamma(s)(r^m) = r^{-m}$.

5. *Montrer que $D_n \simeq G \underset{\gamma}{\times} H$.*

Puisque $G \simeq \mathbb{Z}/n\mathbb{Z}$ et $H \simeq \mathbb{Z}/2\mathbb{Z}$, on a le résultat annoncé.

Étude du groupe $Aut(D_n)$

On pose $H = \{\gamma \in Aut(D_n) | \gamma(a) = a\}$ et $K = \{\gamma \in Aut(D_n) | \gamma(b) = b\}$, où a et b sont les générateurs de D_n dans la présentation donnée à la question 4.

6. *Montrer que H et K sont des sous-groupes de $Aut(D_n)$.*

7. *Montrer que $|H| = n$ et $|K| = \varphi(n)$, où φ est la fonction d'Euler.*

8. *Montrer que $Aut(D_n)$ est le produit semi-direct du sous-groupe H par le sous-groupe K.*

♣ TR.IV.B. Groupe des isométries du cube

On considère un cube dans $\mathbb{R}^3$ dont les sommets sont numérotés de 1 à 8, où [1,2,3,4] détermine la face supérieure, [5,6,7,8] la face inférieure, ces deux faces étant reliées par les arêtes [1,5], [2,6], [3,7], [4,8].

On note G le groupe des isométries directes de ce cube (dans $\mathbb{R}^3$). Tout élément r de G induit une permutation σ_r de l'ensemble des sommets, donc un élément de S_8. Comme r est entièrement déterminé par σ_r (en d'autres termes, l'action de G sur l'ensemble des sommets du cube est fidèle), on peut identifier r et σ_r, donc décrire un élément de G par la permutation de S_8 correspondante.

1. *Démontrer que les éléments*

$$\alpha = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 2&3&4&1&6&7&8&5 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 2&6&7&3&1&5&8&4 \end{pmatrix}$$

appartiennent à G.

2. *Soit $H = \langle \alpha, \beta \rangle$ le sous-groupe de G engendré par α et β. Déterminer l'orbite de 1 sous l'action de H.*

3. *En déduire que G opère transitivement sur l'ensemble des sommets du cube.*

4. *Déterminer le stabilisateur de 1 sous l'action de G. En déduire l'ordre de G.*

On veut démontrer que G est isomorphe au groupe S_4. Une façon de faire serait de caractériser S_4 par des générateurs et des relations et vérifier que G admet un système de générateurs de ce type. Une autre façon, plus naturelle, est de trouver un ensemble de quatre éléments sur lequel agit G. Il est raisonnable de penser que cet ensemble est à trouver dans la géométrie du cube.

5. *Démontrer que l'ensemble $\{[1,7],[2,8],[3,5],[4,6]\}$ des diagonales (non orientées, donc $[1,7] = [7,1]$ par exemple) du cube est permuté par G. En déduire que G est isomorphe à S_4.*

♠ TR.IV.C. Produits et extensions de groupes

Soient G un groupe, N un sous-groupe normal de G et G/N le groupe quotient. On cherche à étudier la structure de G et ses propriétés à partir de celles de N

et G/N. Plus généralement, deux groupes N et H étant donnés, on cherche tous les groupes G tels que N soit isomorphe à un sous-groupe normal de G et H isomorphe au quotient par ce sous-groupe.

Plus précisément, étant donnés trois groupes N, G, H et des morphismes de groupes $N \xrightarrow{i} G$ et $G \xrightarrow{p} H$, on dit que

$$N \xrightarrow{i} G \xrightarrow{p} H$$

est une ***suite exacte*** si $Im(i) = Ker(p)$. Une suite de plusieurs morphismes est exacte si toutes les suites formées de deux morphismes consécutifs sont exactes.

Avec ces notations, le problème posé ci-dessus consiste à trouver tous les groupes G tels que la suite

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

soit exacte, les groupes N et H étant fixés. En effet, l'exactitude de la suite $1 \longrightarrow N \xrightarrow{i} G$ est équivalente au fait que le morphisme i est injectif et donc que N est isomorphe à un sous-groupe de G. De plus, l'exactitude de la suite $N \xrightarrow{i} G \xrightarrow{p} H$ indique que $i(N) = Ker(p)$, d'où $i(N)$ est un sous-groupe normal de G. L'exactitude de la suite $G \xrightarrow{p} H \longrightarrow 1$ indique que le morphisme p est surjectif. On en déduit que le groupe H est isomorphe au groupe $G/Ker(p)$, qui est égal au groupe $G/Im(i)$.

Dans la situation ci-dessus, on dit que G est une ***extension*** de H par N.

Les groupes N et H étant donnés, le problème de déterminer tous les groupes G qui sont extension de H par N est très difficile et n'a pas de réponse en général. Nous allons ici interpréter, dans ce cadre, les notions de produit semi-direct et direct.

Soient N et H deux groupes et un morphisme $\gamma : H \to Aut(N)$ définissant une opération par automorphismes de H sur N. On pose $G = N \underset{\gamma}{\times} H$.

1. *Montrer que les morphismes canoniques*

$$i : N \to N \underset{\gamma}{\times} H, \qquad n \mapsto (n, 1)$$
$$p : N \underset{\gamma}{\times} H \to H, \qquad (n, h) \mapsto h$$

sont tels que la suite

$$1 \longrightarrow N \xrightarrow{i} N \underset{\gamma}{\times} H \xrightarrow{p} H \longrightarrow 1$$

est exacte.

2. *Montrer que l'application* $s : H \to N \underset{\gamma}{\times} H$, *définie par* $s(h) = (1, h)$, *est un morphisme de groupes vérifiant* $p \circ s = id_H$.

On dit que s est une ***section*** de p. La condition $p \circ s = id_H$ impliquant que s est un morphisme injectif, on remarquera que $s(H)$ est isomorphe à H.

Réciproquement, on considère une suite exacte

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

et on suppose qu'il existe une section s de p.

3. *En identifiant* N *à* $i(N)$ *et* H *à* $s(H)$, *montrer que* G *est isomorphe au produit semi-direct* $N \underset{\gamma}{\times} H$, *où* γ *définit l'action de* $s(H)$ *sur* $i(N)$ *par conjugaison.*

Conclusion. Ce qui précède montre que, deux groupes N et H étant donnés, un groupe G est isomorphe à un produit semi-direct de N par H si et seulement s'il existe une suite exacte

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

tel que le morphisme p admette une section.

D'après la remarque (IV.3.3), un groupe G est produit direct $N \times H$ de deux groupes N et H si et seulement si c'est le produit semi-direct $N \underset{\gamma}{\times} H$, où γ est l'identité.

4. *Soient* N *et* H *deux groupes. Montrer qu'un groupe* G *est isomorphe au produit direct* $N \times H$ *si et seulement s'il existe une suite exacte*

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

telle que le morphisme p *admette une section* s *vérifiant* $s(H) \subseteq Z_G(i(N))$.

5. *Appliquer ce qui précède pour montrer que :*

a) *Le groupe* S_n *est un produit semi-direct de* A_n *par* $\mathbb{Z}/2\mathbb{Z}$. (Considérer la signature.)

b) *Le groupe quaternionique* $\mathcal{H}$ *ne peut être obtenu comme produit semi-direct de deux de ses sous-groupes.*

♣ TR.IV.D. Groupes libres de rang 2

L'objectif de ce TR est de donner des exemples de groupes libres de rang 2. Cette étude est basée sur le résultat suivant :

Lemme du ping-pong

Soit un groupe G opérant sur un ensemble E. On suppose que E_1 et E_2 sont des sous-ensembles de E, $E_2 \not\subset E_1$, et que G_1 et G_2 sont des sous-groupes de G tels que G_1 ait au moins trois éléments et que les propriétés suivantes soient satisfaites :

$$\forall g \in G_1 \setminus \{1_G\}, g(E_2) \subset E_1 \quad \text{et} \quad \forall h \in G_2 \setminus \{1_G\}, h(E_1) \subset E_2.$$

Alors le sous-groupe de G engendré par G_1 et G_2 est isomorphe au produit libre de G_1 et G_2.

1. *Soit $g = g_1 h_1 \dots g_r$ un mot, avec, pour tous i, $g_i \in G_1 \setminus \{1_G\}$ et $h_i \in G_2 \setminus \{1_G\}$. Montrer que ce mot ne peut être trivial.* (Faire opérer ce mot sur E_2.)

2. *Soit $h_0 \in G_2 \setminus \{1_G\}$ et supposons que $h_0 g = 1$. Montrer que l'opération de g sur E_2 induit une application bijective de E_2 sur E_1. En déduire alors que $E_2 \subset E_1$.*

3. *En déduire que tous les mots réduits construits à partir de G_1 et G_2 sont non triviaux et en déduire le lemme.*

On considère maintenant le groupe $SL_2(\mathbb{R})$ formé des matrices $(2,2)$ inversibles à coefficients dans $\mathbb{R}$, de déterminant $+1$ (*groupe spécial linéraire*). Pour toute matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ et tout élément $x \in E = \mathbb{R} \cup \{\infty\}$, on considère l'homographie

$$h_M : x \mapsto \frac{ax+b}{cx+d}$$

avec $h_M(-\frac{d}{c}) = \infty$ et $h_M(\infty) = \frac{a}{c}$, si $c \neq 0$.

4. *Montrer que h_M, pour $M \in SL_2(\mathbb{R})$, définit une action de $SL_2(\mathbb{R})$ sur E.*

On considère les matrices

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

et on pose $E_1 =]-1,1[$ et E_2 le complémentaire de $[-1,1]$ dans E.

5. *Montrer que pour tout entier $n \neq 0$, $h_A^n(E_1) \subset E_2$ et $h_B^n(E_2) \subset E_1$.*

6. *En déduire que tout mot réduit w construit à partir de A et B, commençant par une puissance de B et se terminant par une puissance de A, est tel que $h_w \neq id$ et donc que $w \neq 1$.*

7. *Montrer qu'il en est de même pour tout mot réduit construit à partir de A et B.*

8. *En déduire que le sous-groupe de* $SL_2(\mathbb{R})$ *engendré par* A *et* B *est libre de rang* 2.

9. *Plus généralement, montrer que deux symboles abstraits distincts engendrent un groupe libre de rang* 2.

TRAVAUX PRATIQUES

TP.IV.A. Générateurs et relations, autour de l'algorithme de Todd-Coxeter

Les groupes définis par générateurs et relations constituent, avec les groupes de permutations, les deux principaux types de groupes pour lesquels MAPLE offre des commandes avancées dédiées à leur manipulation.

Si les groupes de permutations sont définis par des générateurs, les relations sont entièrement régies par la multiplication des cycles ; de plus, l'unicité de la décomposition en cycles définit un élément de façon univoque. Dans le cas des groupes présentés par générateurs et relations, se posent des problèmes de « combinatoire des mots » : à supposer que le groupe soit fini, comment savoir si l'on a écrit tous les mots (et être sûr que ces mots correspondent à des éléments distincts modulo les relations) ?

Un des principaux algorithmes est dû à Todd et Coxeter : il permet, disposant d'une présentation de G et d'un sous-groupe H *d'indice fini* n (défini par des générateurs exprimés comme des mots en les générateurs de G), de donner un système de représentants des classes modulo H.

Dans le cas où G est un groupe fini, en prenant $H = \{\mathrm{Id}\}$, on obtient en particulier les éléments de G.

De plus, l'algorithme nous fournit un morphisme $\rho : G \to \mathrm{Aut}(G/H) \simeq S_n$ qui traduit l'action de G par translation sur les classes G/H. C'est d'ailleurs cette action qui est à la base de l'algorithme, d'où le choix de différer ce TP en fin de chapitre IV. On obtient ainsi, si ρ est injectif, une réalisation de G comme un groupe de permutations.

Les objectifs de ce TP sont multiples : d'une part, on apprend à manipuler les groupes définis par générateurs et relations (calcul du cardinal, du moins si ce

dernier est fini, etc.) et fournit des présentations de quelques groupes usuels intéressants (par exemple le groupe des isométries directes du carré et celui du tétraèdre, isomorphes à S_4 et A_4 respectivement). On utilise Maple pour vérifier que l'on a bien obtenu toutes les relations, point difficile qu'il est fastidieux de réaliser à la main. D'autre part, c'est l'occasion, *via* l'algorithme de Todd-Coxeter, d'étudier l'opération de G sur G/H par translation. Apparaissent également, parmi les exemples choisis, plusieurs produits semi-directs.

☞ *Ne pas oublier de charger la librairie* Maple *dédiée à la manipulation des groupes :* `with(group);`.

Familiarisation avec les commandes Maple : premiers exemples

1. La définition d'un groupe par générateurs et relations se fait avec la commande `grelgroup`. Écrire deux fonctions `Cyclique` et `Diedral` définissant, par une présentation et en fonction de n, le groupe cyclique $C_n \simeq \mathbb{Z}/n\mathbb{Z}$ et le groupe diédral D_n des isométries du polygone régulier à n côtés (*indication* : on rappelle que ce second groupe est engendré par la rotation d'angle $\frac{2\pi}{n}$ et une symétrie axiale ; autrement dit, $D_n = \langle\{a,b\}|a^n, b^2, abab\rangle$. On renvoie au besoin à TR.IV.A pour plus de détails). Vérifier, avec la commande `grouporder`, que l'on obtient bien le nombre d'éléments escompté. Définir également le groupe libre $Z \simeq \mathbb{Z}$ à 1 élément et lui appliquer la commande `grouporder`.

2. Soit G un groupe engendré par un ensemble d'éléments $X = \{a_i\}_{i\in I}$ vérifiant un ensemble de relations $R = \{r_k = 1_G\}_{k\in K}$. Pour démontrer que $\langle X|R\rangle$ est une présentation de G, *i.e.* que G est isomorphe au quotient $G' = L(X)/(R)$, on montre en pratique que $\mathrm{Card}(G') = \mathrm{Card}(G)$ (en fait l'inégalité $\leqslant$ suffit) : on a une application $G' \to G$ en vertu de la propriété universelle et du théorème de factorisation (*cf.* chapitre III, proposition III.2.1), qui est surjective puisque X engendre G. La difficulté consiste à montrer l'injectivité, autrement dit, que ce sont bien là toutes les relations. On peut utiliser Maple pour cela.

Démontrer, en utilisant cette stratégie, que $S_4 \simeq \langle\{a,b\}|a^4, b^2, (ab)^3\rangle$ et donner également une présentation de A_4. Pour finir, remarquer que l'algorithme de Maple est tellement gourmand en terme d'espace disque utilisé qu'il est difficile de statuer avec l'ordinateur si $A_5 \simeq \langle\{a,b\}|a^3, b^3, (ab)^5\rangle$ ou non (suggéré par le choix des générateurs $a = (123)$ et $b = (345)$ de A_5).

3. Si $G = \langle X|R\rangle$, on définit un sous-groupe H de G par l'ensemble de ses générateurs, exprimés comme des mots en les éléments de X. On utilise pour cela la commande `subgrel`.

Tester cette commande avec $G = D_5$ et les sous-groupes $K = \langle a \rangle$ et $L = \langle b \rangle$. Sont-ils distingués dans D_5 ? Vérifier avec la commande `isnormal`. Calculer leurs ordres (noter que pour appliquer la commande `grouporder` à un sous-groupe, il faut d'abord en calculer une présentation *via* la commande `pres`).

Sachant que l'ordre de $x \in X$ est égal à l'ordre du sous-groupe qu'il engendre, écrire une procédure `ordre:=proc(x,G)` renvoyant l'ordre d'un mot x en les générateurs du groupe G. Tester en calculant les ordres des éléments de C_{10}. Conclusion ?

Il semble que la commande `pres` de Maple soit buguée (à moins que le problème n'ait été corrigé depuis...) : `pres(subgrel({x=[a,a]},Cyclique(10))` donne un résultat aberrant. On évitera, autant que possible, d'utiliser par la suite cette commande (dont on ne connaît d'ailleurs pas les algorithmes sous-jacents, à la différence de `grouporder`, bâtie sur l'algorithme de Todd-Coxeter que nous détaillerons plus loin).

4. La commande `cosets` renvoit une liste de représentants des classes modulo un sous-groupe défini avec une commande `subgrel` (qui fait donc référence au groupe dont il est issu). Tester avec $L \subset D_5$: s'agit-il des classes à droite ou à gauche ? Tester également avec $\langle a \rangle \subset S_4$. C'est *a priori* un choix arbitraire historique dans la littérature sur le sujet.

Comment obtenir les éléments de G en utilisant la commande `cosets` ? Écrire une fonction `elements1` renvoyant, en fonction du groupe G (défini comme toujours par une commande `grelgroup`), la liste de ses éléments. Tester sur les exemples précédents (C_{10}, D_5, S_4).

L'algorithme de Todd-Coxeter

On se donne un groupe G défini par un ensemble $X = \{g_1, \ldots, g_m\}$ de générateurs vérifiant un ensemble $R = \{r_j = 1_G\}_{1 \leqslant j \leqslant k}$ de relations. D'autre part, soit H un sous-groupe de G engendré par $Y = \{h_1, \ldots, h_s\}$. Les r_j et h_j sont exprimés comme des mots en les éléments de $X \cup X^{-1}$.

L'algorithme de Todd et Coxeter permet d'énumérer les différentes classes à droite, *i.e.* les éléments de $(G/H)_d$, en faisant agir G sur $(G/H)_d$ par translation à doite : $Hx \cdot g = H(xg)$. Au final, on obtient l'indice n de H dans G, des éléments $g_i \in G$ tels que $(G/H)_d = \{Hg_1, \ldots, Hg_n\}$ (*i.e.* des représentants des classes) et la description explicite du morphisme $\rho : G \to S((G/H)_d) = S_n$ (après numérotation des classes), c'est-à-dire l'expression des $\rho(g_i)$ en tant qu'éléments de S_n.

L'énumération de Todd-Coxeter est basée sur les trois observations suivantes, où les classes sont affectées de numéros en commençant par $1 = H$:

TC-1 : $1 \cdot h = 1$ pour tout $h \in H$;

TC-2 : $i \cdot r = i$ pour toute classe i et tout « relateur » $r \in R$;

TC-3 : $i \cdot g = j \Leftrightarrow j \cdot g^{-1} = i$ pour toutes classes i, j et tout $g \in G$.

On définit trois types de tables ; pour faciliter la compréhension, nous prendrons l'exemple suivant : $G = \langle \{a, b\} | a^4, b^3, abab \rangle$ et $H = \langle a \rangle$.

– *Les tables du sous-groupe* : À chaque $h = g_{i_1}^{\pm 1} \dots g_{i_l}^{\pm 1} \in Y$, on associe une table à une ligne et $l+1$ colonnes (l est la longueur du mot). On mettra en position j le numéro de classe de $1 \cdot g_{i_1}^{\pm 1} \dots g_{i_j}^{\pm 1} = (1 \cdot g_{i_1}^{\pm 1} \dots g_{i_{j-1}}^{\pm 1}) \cdot g_{i_j}^{\pm 1}$. Sur notre exemple, la table est donc initialisée (compte-tenu de **TC-1**) avec :

	a
1	1

C'est un cas particulier où la table du sous-groupe est déjà complète.

– *Les tables des relateurs* : Sur le même principe, à chaque $r = g_{i_1}^{\pm 1} \dots g_{i_l}^{\pm 1} \in R$, on associe une table à $l+1$ colonnes et un nombre de lignes indéterminé pour l'instant. On peut même présenter ces tables en les mettant bout à bout. Sur notre exemple, en tenant compte de **TC-2** pour l'initialisation, on trouve :

	a	a	a	a	b	b	b	a	b	a	b
1				1			1				1

On passe donc du numéro en position (i, j) à celui en position $(i, j+1)$ en faisant agir l'élément de $X \cup X^{-1}$ figurant en première ligne entre les deux colonnes j et $j+1$. Les barres verticales matérialisent le début et la fin de chaque table.

– *La table de l'action sur les classes* : On met en colonne les éléments de X et en ligne les numéros des classes. En position (i, g) se trouve le numéro de classe de $i \cdot g$. Pour notre exemple :

	a	b
1		

On construit ces tables progressivement : dès que l'on obtient une nouvelle classe, donc un nouveau numéro, en posant $i \cdot g = j$ par exemple, on rajoute une ligne aux tables des relateurs et à celle de l'action sur les classes, et on reporte ce numéro partout où apparaît $i \cdot g = j$. On utilise aussi **TC-3** pour compléter où l'on peut.

Traitons notre exemple :

– Compte tenu de **TC-1**, la table des relateurs s'écrit :

	a	a	a	a	b	b	b	a	b	a	b
1	1	1	1	1			1	1			1

– On pose ensuite $2 = 1 \cdot b$; les tables deviennent :

	a	a	a	a	b	b	b	a	b	a	b
1	1	1	1	1	2		1	1	2		1
2				2		1	2		1	1	2

	a	b
1	1	2
2		

– On continue et on pose $3 = 2 \cdot b$:

	a	a	a	a	b	b	b	a	b	a	b
1	1	1	1	1	2	3	1	1	2		1
2				2		1	2		1	1	2
3				3	1	2	3			2	3

	a	b
1	1	2
2		3
3		

Au cours de ce processus de remplissage, on peut découvrir dans les tables du sous-groupe ou des relateurs une nouvelle égalité $i' \cdot g' = j'$ entre deux numéros déjà existants ; on remplace alors partout où l'on peut.

– Dans notre exemple, on trouve $3 \cdot b = 1$. Les tables deviennent :

	a	a	a	a	b	b	b	a	b	a	b
1	1	1	1	1	2	3	1	1	2		1
2				2	3	1	2		1	1	2
3				3	1	2	3			2	3

	a	b
1	1	2
2		3
3		1

– On continue et on pose $2 \cdot a = 4$:

a	a	a	a	b	b	b	a	b	a	b
1	1	1	1	1	2	3	1	1	2	4	1
2	4			2	3	1	2	4	1	1	2
3				3	1	2	3			2	3
4			2	4			4				4

	a	b
1	1	2
2	4	3
3		1
4		

Arrivé à ce stade apparaît un nouveau phénomène : dans notre exemple, on déduit $4 \cdot b = 1$. Or $3 \cdot b = 1$ se lit dans la table de l'action sur les classes. Par conséquent $4 = 3$. On supprime donc la dernière ligne des tables des relateurs et de la table de l'action, et on remplace partout 4 par 3.

– On obtient :

a	a	a	a	b	b	b	a	b	a	b
1	1	1	1	1	2	3	1	1	2	3	1
2	3			2	3	1	2	3	1	1	2
3				3	1	2	3			2	3

	a	b
1	1	2
2	3	3
3		1

– On continue et on pose $3 \cdot a = 4$, puis $4 \cdot a = 5$:

a	a	a	a	b	b	b	a	b	a	b
1	1	1	1	1	2	3	1	1	2	3	1
2	3	4	5	2	3	1	2	3	1	1	2
3	4	5	2	3	1	2	3	4	5	2	3
4	5	2	3	4	5		4	5			4
5	2	3	4	5		4	5	2	3	4	5

	a	b
1	1	2
2	3	3
3	4	1
4	5	5
5	2	

– On pose $5 \cdot b = 6$:

	a	a	a	a	b	b	b	a	b	a	b
1	1	1	1	1	2	3	1	1	2	3	1
2	3	4	5	2	3	1	2	3	1	1	2
3	4	5	2	3	1	2	3	4	5	2	3
4	5	2	3	4	5	6	4	5	6	6	4
5	2	3	4	5	6	4	5	2	3	4	5
6	6	6	6	6	4	5	6	6	4	5	6

	a	b
1	1	2
2	3	3
3	4	1
4	5	5
5	2	6
6	6	4

L'algorithme est terminé. Comme on le voit, il y a une certaine flexibilité dans l'ordre où l'on fait les déductions successives. En général, cet algorithme se termine lorsque l'indice de H dans G est fini (voir [16], chapitre 8, Théorème 3.4 pour un énoncé précis).

Expliquons pourquoi, lorsque cet algorithme se termine, il donne bien le résultat escompté. Notant $I = \{1, \dots, n\}$ l'ensemble des numéros obtenus, on va justifier que la table de l'action sur les classes définit bien une action de G sur I. Puis, on va mettre en bijection I et $(G/H)_d$, de sorte que les actions de G sur les deux ensembles se correspondent (on parle de bijection G-équivariante). On suit le raisonnement de [2], chapitre 6, Théorème 9.10 :

– Par construction, les colonnes de la table de l'action sur les classes correspondent bien à des bijections de I. En vertu de **TC-2**, on obtient donc un morphisme $\rho : G \to S(I) = S_n$ (par propriété universelle et passage au quotient). En d'autre termes, G agit sur I.

– L'application $G \to I$ définie par $g \mapsto 1 \cdot g$, qui est surjective par construction de I (G y agit transitivement), factorise en vertu de **TC-1** en une application $\psi : (G/H)_d \twoheadrightarrow I$.

– On construit d'autre part, par récurrence, une application $\phi : I \to (G/H)_d$. On part de $\phi(1) = H$; au cours du processus de remplissage, lorsque l'on rajoute $j = i \cdot g$, on pose $\phi(j) = \phi(i) \cdot g$. Si par contre on tombe sur une égalité $j = i$, alors $\phi(j) = \phi(i)$ également, puisque la première égalité résulte des propriétés **TC-i** qui sont vérifiées par les éléments de $(G/H)_d$.

– L'application $\phi \circ \psi : (G/H)_d \to (G/H)_d$ est G-équivariante et vérifie $\phi \circ \psi(H) = H$. Il s'agit donc de l'identité : $\phi \circ \psi(H \cdot g) = \phi \circ \psi(H) \cdot g = H \cdot g$. On en déduit que ψ est également injective : c'est donc une bijection.

– En définitive, on peut identifier les indices et les classes et le morphisme $\rho : G \to S(I) = S_n$ décrit bien l'action de G sur $(G/H)_d$ (après identification).

5. Confronter sur l'exemple précédent les résultats des calculs à la main avec ceux de Maple. On calculera les classes à droite $(G/H)_d$ avec la commande `cosets` et le morphisme $\rho : G \to S((G/H)_d) = S_n$ *via* la commande `permrep(H)`.

En utilisant l'ordre des permutations correspondant aux générateurs a et b, démontrer que ces derniers sont respectivement d'ordres 4 et 3 (*a priori*, les relations $a^4 = b^3 = 1$ ne permettent que de majorer ces ordres). En déduire le cardinal de G.

Enfin, démontrer que G constitue une présentation du groupe O des isométries directes du cube (*indication* : on pourra utiliser les résutats démontrés dans le TR.IV.B).

6. Soit T le groupe des isométries directes du tétraèdre. Justifier que T permute transitivement les quatre sommets, que cette action est fidèle et que le stabilisateur d'un sommet est une rotation d'angle $\frac{2\pi}{3}$. En déduire que T est de cardinal 12 et isomorphe à A_4. Quel est l'ordre du produit ab de deux telles rotations (d'angle $\frac{2\pi}{3}$ et d'axes distincts) ?

Cela amène à définir $G = \langle \{a, b\} | a^3, b^3, abab \rangle$, groupe dont on désire connaître le cardinal. Effectuer à la main l'algorithme de Todd-Coxeter en prenant $H = \langle a \rangle$ (noter que ce choix est plus judicieux que $H = \{\mathrm{Id}\}$ pour

l'objectif en question) ; on trouve la table suivante :

	a	a	a	b	b	b	a	b	a	b
1	1	1	1	2	3	1	1	2	3	1
2	3	4	2	3	1	2	3	1	1	2
3	4	2	3	1	2	3	4	4	2	3
4	2	3	4	4	4	4	2	3	4	4

Vérifier avec Maple, puis conclure qu'il s'agit bien d'une présentation du groupe T.

On modifie maintenant légèrement les relations : on considère $G_1 = \langle\{a,b\}|a^3, b^3, aba^2b\rangle$. Prenant toujours $H_1 = \langle a\rangle$, effectuer de nouveau l'algorithme à la main et avec Maple. Démontrer enfin que $G_1 \simeq \mathbb{Z}/3\mathbb{Z}$: l'ordre du groupe est bien moindre.

Encore des exemples

7. Soit $G = \langle\{a,b\}|a^2, b^2, abab^{-1}a^{-1}b^{-1}\rangle$. Calculer son ordre avec la commande `grouporder`, puis l'ordre de $H = \langle a\rangle$ et $K = \langle b\rangle$ *via* la commande `cosets`. Enfin, à l'aide de la commande `permrep` appliquée au sous-groupe H, retrouver les ordres de a et b, et démontrer que G est isomorphe à S_3.

8. Soient $G = \langle\{a,b,c\}|a^2, b^3, c^5, abc\rangle$ et H le sous-groupe de G engendré par a et cbc^{-1}. A l'aide du morphisme $G \to (G/H)_d$ et des commandes Maple, montrer que G est isomorphe à A_5. Autrement dit, nous avons obtenu une présentation de A_5.

En utilisant le sous-groupe $K = \langle a\rangle$, réaliser également G comme un sous-groupe de A_{30}.

9. Soit $G = \langle\{a,b\}|a^7, b^3, bab^{-1}a^{-2}\rangle$. Démontrer que G est le produit semi-direct de $H = \langle a\rangle$ par $K = \langle b\rangle$ (consulter si nécessaire le chapitre IV, paragraphes 3.B et 3.C pour des rappels sur la notion de produit semi-direct). De quel produit semi-direct $\mathbb{Z}/7\mathbb{Z} \times_\gamma \mathbb{Z}/3\mathbb{Z}$ s'agit-il (à isomorphisme près) ? On explicitera le morphisme $\gamma : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$: notant encore par les lettres a et b les générateurs $\bar{1}$ des deux groupes respectivement, il s'agit de donner $\gamma(b)a$.

10. Soit $G = \langle\{a,b\}|a^4, b^4, a^2b^2\rangle$. Calculer son ordre *via* la commande `grouporder` (au besoin, réinitialiser Maple à l'aide de la commande `restart`). Ce groupe est-il abélien ? Pour le savoir, définir le groupe G_1

obtenu en rajoutant la relation de commutativité $aba^{-1}b^{-1} = 1_G$ de a et b. Déterminer la structure de groupe de G_1 (on montrera qu'il s'agit d'un produit direct de deux groupes cycliques dont on déterminera les ordres).

Soit H le sous-groupe de G engendré par le produit ab. Démontrer avec Maple que H est d'indice 4 et isomorphe à $\mathbb{Z}$.

De façon générale, quel est le noyau du morphisme $\rho : G \to S((G/H)_d)$? Que se passe-t-il si H est distingué ? Revenant à notre exemple, démontrer que le quotient G/H est un groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Pour finir, soit K le sous-groupe engendré par a. Démontrer que G est le produit semi-direct de H par K. Existe-t-il plusieurs produits semi-directs $\mathbb{Z} \times_\gamma \mathbb{Z}/4\mathbb{Z}$ possibles ? Que vaut $a(ab)a^{-1}$?

TP.IV.B. Actions k-transitives, formule de Burnside et énumérations de Polya

Ce TP fait suite au TP.II et termine l'étude des groupes de permutations. Un tel groupe de permutations G, de degré n, agit naturellement sur $X_n = \{1, \dots, n\}$. On en détermine les orbites et teste la transitivité de l'action pour différents groupes. Puis on généralise à l'action diagonale sur X_n^k afin de discuter la k-transitivité. Des limitations dues aux temps de calcul apparaissent rapidement et sont contournées par l'usage de la formule de Burnside. Cela permet de regarder des groupes de plus haut degré et, en particulier, de mentionner les fameux groupes de Mathieu. Pour finir, on procède à quelques dénombrements dits « de Polya », la formule d'énumération de Polya étant basée sur une généralisation de la formule de Burnside.

Calcul de l'orbite

☞ *Quelques commandes* Maple *utiles* : `minus`, `time`.

1. Écrire une procédure `orbite:=proc(G,X,action)` renvoyant la liste des orbites pour l'action d'un groupe G (défini avec la commande `permgroup`) sur un ensemble X : l'élément $g \cdot x$, pour $g \in G$ et $x \in X$, est donc `action(g,x)`. On partira de la liste des éléments de G, obtenue *via* la commande `elements`, et on soustraira progressivement les classes, jusqu'à épuisement des éléments (algorithme naïf).

   Tester cette procédure avec S_3 et A_3 agissant sur $\{1, 2, 3\}$; ainsi `action` correspond à la fonction `(g,x)->image(g,3,x)`, où `image` désigne la procédure déjà écrite au cours du TP.II.

2. Écrire des fonctions `OrbiteSn` et `OrbiteAn` renvoyant respectivement, en fonction de n, les orbites pour l'action naturelle de S_n et A_n sur $X_n = \{1, \dots, n\}$. Vérifier que l'action est transitive pour $3 \leqslant n \leqslant 8$.

Quel est le temps de calcul pour S_8 ? Comparer en calculant l'orbite de 1 avec la commande Maple `orbit`.

3. La lenteur de la procédure `orbite` provient du fait que l'on calcule au préalable tous les éléments du groupe. On peut s'en passer, en travaillant intelligemment avec le système S de générateurs du groupe G. Ainsi, pour calculer l'orbite de i, on procède comme suit :

(a) Initialisation : $O := \{i\}$.
(b) On fait agir les éléments de S : s'il n'en résulte aucun nouvel élément, c'est terminé ; sinon, soit N l'ensemble de ces nouveaux éléments.
(c) On met à jour $O := O \cup N$.
(d) On fait agir les éléments de S sur N (plutôt que sur O tout entier) : s'il n'en résulte aucun nouvel élément, c'est terminé. Sinon, on met à jour N comme l'ensemble de ces nouveaux éléments qui ne sont pas déjà dans O, puis on applique (c).

Implémenter cet algorithme au sein d'une procédure

```
orbite_i:=proc(G,i,action)
```

renvoyant l'orbite de i pour l'action de G définie par `action`, puis modifier la procédure `orbite` afin qu'elle utilise `orbite_i`. Enfin, récolter les fruits en testant, sur S_8 par exemple, l'amélioration du temps de calcul.

4. Écrire une fonction `OrbiteG` renvoyant, en fonction du groupe de permutations G (qui sera toujours introduit comme un `permgroup`), la liste des orbites pour l'action naturelle de G. Comme application, déterminer tous les groupes de permutations transitifs de degré 3 (*i.e.* les sous-groupes de S_3 agissant transitivement sur X_3). Vérifier également la transitivité de l'action pour les groupes suivants :

```
L[1]:=permgroup(4,{[[1,2,3,4]]}):
L[2]:=permgroup(4,{[[1,2,3,4]],[[1,2]]}):
L[3]:=permgroup(4,{[[1,2,3,4]],[[1,3]]}):
L[4]:=permgroup(4,{[[1,2],[3,4]],[[1,3],[2,4]]}):
L[5]:=permgroup(4,{[[1,2,3]],[[1,2],[3,4]]}):\vspace*{-1mm}
```

On peut démontrer qu'il s'agit là de tous les groupes transitifs de degré 4 (à conjugaison près).

Étude de la k-transitivité

On dit qu'un groupe G opère *k-transitivement* sur un ensemble X (de cardinal supérieur ou égal à k) s'il opère transitivement (pour l'action diagonale) sur l'ensemble des k-uplets de points *tous distincts* : pour tout $x = (x_1, \dots, x_k)$ et $x' = (x'_1, \dots, x'_k)$ dans X^k tels que $x_i \neq x_j$ et $x'_i \neq x'_j$ $(j \neq i)$, il existe $g \in G$ tel que, pour tout i, $g \cdot x_i = x'_i$. En particulier, un groupe agissant k-transitivement agit transitivement et l-transitivement pour $l \leqslant k$.

☞ *Quelques commandes* Maple *utiles* : `irem` ; on peut définir le produit cartésien X_n^2 par deux commandes `seq` successives :

```
X2:=n->{seq(seq([i,j],i=1..n),j=1..n)}:
```

5. Écrire une fonction `orbite2` renvoyant, en fonction de n, la liste des orbites pour l'action diagonale de S_n sur X_n^2. Tester avec $n = 3$: quel est le nombre d'orbites ? Vérifier que ces actions sont 2-transitives, pour $3 \leqslant n \leqslant 7$.

6. Écrire une fonction `Orbite2` renvoyant, en fonction du groupe de permutations G, la liste des orbites pour l'action diagonale sur X_n^2 (n sera donc le degré de G). En déduire que les seuls groupes 2-transitifs de degré 4 sont S_4 et A_4.

Déterminer également le cas du degré 5, *i.e.* les groupes de permutations agissant 2-transitivement parmi les groupes transitifs de degré 5 dont voici la liste :

```
L[6]:=permgroup(5,{[[1,2,3,4,5]]}):
L[7]:=permgroup(5,{[[1,2,3,4,5]],[[1,2]]}):
L[8]:=permgroup(5,{[[1,2,3,4,5]],[[2,5],[3,4]]}):
L[9]:=permgroup(5,{[[1,2,3,4,5]],[[1,2,3]]}):
L[10]:=permgroup(5,{[[1,2,3,4,5]],[[2,3,5,4]]}):
```

Reconnaître S_5 et A_5 et vérifier que L_{10} est un produit semi-direct.

7. Pour définir X_n^k sous Maple, une solution est d'indexer ses éléments à l'aide de la bijection $\Phi_k : \{1, \dots, n^k\} \to X_n^k$ dont la réciproque est la fonction

$$(x_1, \dots, x_k) \mapsto 1 + \sum_{i=1}^{k} (x_i - 1) k^{i-1}$$

(à un décalage près, cela correspond à l'écriture d'un nombre en base k).

Écrire une procédure `Phik:=proc(i,n,k)` calculant $\Phi_k(i)$ et définir X_n^k sous Maple comme une fonction `Xk` de n et k.

8. Écrire une fonction `orbitesG` renvoyant, en fonction de l'entier k et du groupe de permutations G, la liste des orbites pour l'action diagonale sur X_n^k. En testant sur la liste des L_i, quel nombre minimal d'orbites trouve-t-on pour l'action sur X_n^3 ? Justifier qu'une action 3-transitive donne lieu à 5-orbites, puis donner la liste des groupes de permutations 3-transitifs de degré inférieur ou égal à 5.

Parmi ces derniers, lesquels opèrent 4-transitivement ? Démontrer au papier-crayon que S_n agit n-transitivement et que A_n agit $(n-2)$-transitivement pour tout n.

9. Soit $\Pi(k)$ l'ensemble des partitions de $\{1,\dots,k\}$ et $\pi : X_n^k \to \Pi(k)$ l'application définie par $x \mapsto \pi_x$, où π_x désigne la partition correspond à la relation d'équivalence $i \sim j \Leftrightarrow x_i = x_j$. Démontrer que $o \mapsto \pi_o := \pi_x$ $(x \in o)$, définit une application surjective de l'ensemble O des orbites pour l'action diagonale sur X_n^k vers $\Pi(k)$, et que cette application est injective lorsque l'action est k-transitive. En déduire que le nombre d'orbites distinctes pour une action k-transitive sur X_n^k est égal au nombre $p(k)$ de partitions de $\{1,\dots,k\}$.

Il existe différentes façons de calculer $p(k)$:

(a) Soit $p(k,j)$ le nombre de partitions de l'ensemble $\{1,\dots,k\}$ en j sous-ensembles (disjoints) ; on a $p(k,k) = p(k,1) = 1$ et

$$p(k,j) = jp(k-1,j) + p(k-1,j-1)$$

(on distingue selon que k est tout seul ou appartient à l'un des j ensembles de la partition de $\{1,\dots,k-1\}$). Cette relation permet de calculer $p(k,j)$ par récurrence, puis $p(k) = \sum_{j=1}^{k} p(k,j)$.

(b) Soit on utilise la formule

$$p(k) = \sum_{j=1}^{k} \sum_{r=0}^{k-j} (-1)^r \frac{j^k}{r!j!}.$$

Calculer $p(k)$ jusqu'à $k = 10$, par les deux méthodes. Pour la première, on n'oubliera pas d'ajouter `option remember` au début de la procédure récursive que l'on écrira, ce qui diminue les temps de calcul.

Formule de Burnside

Soit G un groupe fini opérant sur un ensemble fini X et soit N le nombre d'orbites. Pour $g \in G$, on note $r(g)$ le nombre de points fixes de g dans X, *i.e.* le

nombre d'éléments $x \in X$ tels que $g \cdot x = x$. La formule de Burnside dit que

$$N = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} r(g).$$

☞ *Quelques commandes* Maple *utiles* : `add`.

10. Démontrer la formule de Burnside (*indication :* on pourra poser $\delta(x, g) = 1$ si $g \cdot x = x$ et 0 sinon, puis calculer $\sum_{g \in G} r(g)$ en introduisant la fonction δ).

Écrire une fonction `nbPtFix` renvoyant, en fonction de g et de n, le nombre de points fixes de la permutation g de degré n agissant sur X_n. Quel est le nombre de points fixes pour l'action sur X_n^k par rapport à celle sur X_n ? En déduire une procédure `nbOrb:=proc(k,G)` calculant, à l'aide de la formule de Burnside, le nombre d'orbites pour l'action diagonale d'un groupe de permutations G sur X_n^k. Comparer les temps de calcul entre `OrbitesG` et `nbOrb`, par exemple pour S_5 agissant sur X_5^5. Conclusion ?

11. Le gain obtenu nous permet d'investiguer de nouveaux exemples. Parmi la liste suivante des groupes de permutations transitifs de degré 6, lesquels sont 4-transitifs (ou plus) ? On écrira une procédure `OrdreTrans:=proc(G)` renvoyant l'ordre de transitivité du groupe de permutations G.

```
L[11]:=permgroup(6,{[[1,2,3,4,5,6]]}):
L[12]:=permgroup(6,{[[1,5],[2,4],[3,6]],[[1,6],[2,5],[3,4]]}):
L[13]:=permgroup(6,{[[1,2,3,4,5,6]],[[2,6],[3,5]]}):
L[14]:=permgroup(6,{[[1,3,5],[2,4,6]],[[1,2],[5,6]]}):
L[15]:=permgroup(6,{[[1,2,3]],[[1,4],[2,5],[3,6]]}):
L[16]:=permgroup(6,{[[1,3,5],[2,4,6]],[[1,2]]}):
L[17]:=permgroup(6,{[[1,3,5],[2,4,6]],[[1,6],[2,5]]}):
L[18]:=permgroup(6,{[[1,2],[3,4],[5,6]],[[1,2,3],[4,5,6]]}):
L[19]:=permgroup(6,{[[1,2,3,4,5,6]],[[1,3],[2,4]]}):
L[20]:=permgroup(6,{[[1,2,3]],[[1,5,2,4],[3,6]]}):
L[21]:=permgroup(6,{[[1,2,3,4]],[[1,5],[3,6]]}):
L[22]:=permgroup(6,{[[1,2,3,4,5]],[[1,6],[2,5]]}):
L[23]:=permgroup(6,{[[1,2,3,4,5,6]],[[1,3]]}):
L[24]:=permgroup(6,{[[1,2,3,4,5]],[[1,6],[2,3],[4,5]]}):
L[25]:=permgroup(6,{[[1,2,3,4,5,6]],[[4,5,6]]}):
L[26]:=permgroup(6,{[[1,2,3,4,5,6]],[[1,2]]}):
```

Même question pour le degré 7 :

```
L[27]:=permgroup(7,{[[1,2,3,4,5,6,7]]}):
L[28]:=permgroup(7,{[[1,2,3,4,5,6,7]],[[2,7],[3,6],[4,5]]}):
L[29]:=permgroup(7,{[[1,2,3,4,5,6,7]],[[2,3,5],[4,7,6]]}):
L[30]:=permgroup(7,{[[1,2,3,4,5,6,7]],[[2,4,3,7,5,6]]}):
L[31]:=permgroup(7,{[[1,2,3,4,5,6,7]],[[2,3],[4,7]]}):
L[32]:=permgroup(7,{[[1,2,3,4,5,6,7]],[[1,2,3]]}):
L[33]:=permgroup(7,{[[1,2,3,4,5,6,7]],[[1,2]]}):
```

Voyez-vous d'autres groupes que A_n et S_n ? Tester sur les deux derniers exemples suivants :

```
L[34]:=permgroup(11,{[[1,2,3,4,5,6,7,8,9,10,11]],[[3,7,11,8],
[4,10,5,6]]}):
L[35]:=permgroup(12,{[[1,2,3,4,5,6,7,8,9,10,11]],
[[3,7,11,8],[4,10,5,6]],[[1,12],[2,11],[3,6],[4,8],[5,9],
[7,10]]}):
```

C'est un fait assez surprenant : les seuls groupes finis qui sont au moins 4-transitifs sont, à part les groupes A_n et S_n, les quatre groupes de Mathieu M_{11}, M_{12}, M_{23} et M_{24}. Les deux premiers ont été notés L_{34} et L_{35} dans la liste précédente ; les deux autres sont d'ordre 23 et 24, d'où des temps de calcul très longs.

Énumérations de Polya

Soient A, B deux ensembles finis et G un groupe de permutations agissant sur A. On considère l'action suivante de G sur l'ensemble B^A des fonctions $f : A \to B$: un élément g agit par $(g \cdot f)(a) = f(g \cdot a)$. La formule d'énumération de Polya nous dit que l'ensemble O des orbites sous G de B^A est de cardinal

$$N = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \mathrm{Card}(B)^{c_g},$$

où c_g désigne le nombre de cycles dans la décomposition de g en produits de cycles à supports disjoints. C'est un corollaire immédiat de la formule de Burnside (remarquer que f est laissée fixe par g si et seulement si f est constante sur le support de chaque cycle de g).

Afin de répondre à des problèmes classiques de dénombrement, on introduit une version *à poids* de cette formule. La fonction de poids est une application

$\omega : B \to R$, à valeurs dans un anneau commutatif quelconque contenant $\mathbb{Q}$. Le poids de la fonction f est par définition $\omega(f) = \prod_{a\in A} \omega(f(a))$; en particulier, le poids est constant sur les orbites sous G de B^A. La formule d'énumération de Polya, avec poids, nous dit que :

$$\sum_{o\in O} \omega(o) = \frac{1}{\mathrm{Card}(G)} \sum_{g\in G} \left(\sum_{b\in B} \omega(b)\right)^{c_1(g)} \dots \left(\sum_{b\in B} \omega(b)^n\right)^{c_n(g)} \qquad (1)$$

où $c_i(g)$ désigne le nombre de cycles de longueur i dans la décomposition canonique de g. Le type de g nous renseigne donc sur les coefficients c_i.

La démonstration de cette formule utilise une version avec poids du lemme de Burnside :

$$\sum_{o\in O} \omega(o) = \frac{1}{\mathrm{Card}(G)} \sum_{g\in G} \sum_{g\cdot f=f} \omega(f)$$

(on retrouve la formule de Burnside classique en prenant pour ω la fonction constante de valeur 1). De plus, si $g = \alpha_1 \dots \alpha_r$ est la décomposition en cycles, les fonctions fixes par g sont en bijection avec les r-uplets $(b_1, \dots, b_r) \in B^r$ (b_i désigne la valeur de f sur le cycle α_i). Le poids d'une telle fonction est $\omega(f) = \prod \omega(a_i)^{l_i}$, où l_i désigne la longueur du cycle α_i. On termine la preuve en injectant cette égalité dans la formule de Burnside (en exercice).

☞ *Quelques commandes* Maple *utiles* : `mul` ; on peut simplifier et ordonner une expression polynômiale $P(x_1, \dots, x_n)$ par la succession de commandes `sort(normal(P))`.

12. La formule d'énumération de Polya permet de dénombrer des objets considérés modulo certaines symétries. Par exemple, on s'intéresse aux colliers de n perles différents que l'on peut réaliser avec des perles rouges ou bleues. Par définition, deux tels objets sont considérés comme différents s'il ne sont pas égaux modulo une permutation circulaire (le fermoir est invisible).

Dénombrer à la main les colliers à 5 perles. Combien y en a-t-il à 3 boules rouges et 2 boules bleues ? Pour $n = 10$ par exemple, il est impossible de dénombrer à la main : on utilise le formalisme de Polya exposé ci-dessus.

Définir une fonction `Z` renvoyant, en fonction du groupe de permutations G et de la liste W des poids des éléments de B, le résultat de la formule de Polya (1). On pourra utiliser la procédure `typ` écrite au cours du TP.I.

Un collier réalisé à partir de perles rouges ou bleues est une fonction de $\{1, \dots, n\}$ dans l'ensemble $\{rouge, bleu\}$. En prenant comme poids la fonction constante de valeur 1, puis en attribuant à *rouge* un poids « formel »

r (ainsi $R = \mathbb{Q}[r]$), retrouver les résultats précédents. Dénombrer ensuite les colliers à 10 perles ; combien y en a-t-il à exactement 6 perles rouges ?

Remarque. Maple dispose d'une bibliothèque de combinatoire assez riche (charger la librairie `combstruct`) qui permet de construire de tels objets (encore faut-il comprendre la syntaxe). Par exemple, on peut définir un type « collier à 10 perles rouges ou bleues modulo permutations circulaires », en afficher un exemple choisi aléatoirement, et même dénombrer :

```
>collier2:={N=Cycle(Union(rouge,bleu)),rouge=Atom,bleu=Atom}:
>draw([N,collier2,unlabeled], size=10);
>count([N,collier2,unlabeled], size=10);
```

13. On considère, de plus, comme identiques deux colliers qui sont égaux à un « retournement de collier » près (cela correspond aux deux façons d'enfiler le collier autour du cou). Dénombrer les colliers différents de 5 perles, avec cette définition. Combien y en a-t-il à exactement 3 boules rouges ? Mêmes questions avec 10 perles.

This page intentionally left blank

V

LES THÉORÈMES DE SYLOW

On sait, d'après le théorème de Lagrange (II.1.1), que l'ordre de tout sous-groupe d'un groupe fini G divise l'ordre de G. Mais on a vu (par exemple au TR.II.B) que si G est un groupe d'ordre n et si d est un diviseur de n, il n'existe pas nécessairement de sous-groupe de G qui soit d'ordre d. On peut donc se poser la question :

Étant donné un groupe fini G d'ordre n, existe-t-il des diviseurs de n pour lesquels il existe des sous-groupes de G d'ordre ces diviseurs ?

L'objet de ce chapitre est d'apporter une réponse à cette question lorsque le diviseur d est de la forme une puissance d'un nombre premier.

De plus, la connaissance des sous-groupes correspondants permettra de préciser la structure du groupe G.

V.1. Le premier théorème de Sylow

Lemme V.1.1. *Soient p un nombre premier et n un nombre entier non nul. Pour tous nombres entiers r, n, s tels que $1 \leqslant r \leqslant n$ et s non divisible par p, on a $C_{sp^n}^{p^r} = \lambda p^{n-r}$, où λ est un nombre entier non divisible par p (C_m^q désigne le nombre de parties à q élements dans un ensemble à m éléments).*

Démonstration. On a

$$C_{sp^n}^{p^r} = \frac{(sp^n)!}{p^r!(sp^n-p^r)!} = \frac{sp^n(sp^n-1)\dots(sp^n-p^r+1)}{p^r(p^r-1)\dots 1}$$

$$= sp^{n-r}\frac{sp^n-1}{1}\dots\frac{sp^n-(p^r-k)}{p^r-k}\dots\frac{sp^n-(p^r-1)}{p^r-1}.$$

Posons

$$\lambda = s\frac{sp^n-1}{1}\dots\frac{sp^n-(p^r-k)}{p^r-k}\dots\frac{sp^n-(p^r-1)}{p^r-1}.$$

Puisque p ne divise pas s et que $C_{sp^n}^{p^r}$ est un nombre entier, pour établir le résultat il suffit de montrer que pour tout nombre k, $1 \leqslant k \leqslant (p^r-1)$, la fraction $\frac{sp^n-k}{k}$ est égale à une fraction irréductible dont p ne divise ni le numérateur ni le dénominateur. Écrivons k sous la forme $k = qp^t$, avec $t \geqslant 0$ et p ne divisant pas q. On a alors

$$\frac{sp^n-k}{k} = \frac{sp^{n-t}-q}{q}$$

et p ne divise pas $sp^{n-t}-q$, d'où le résultat. □

Théorème V.1.1 **(premier théorème de Sylow).** *Soit G un groupe fini. Pour tout nombre premier p et tout nombre entier r tels que p^r divise l'ordre de G, il existe un sous-groupe de G d'ordre p^r.*

Démonstration. Notons $|G| = qp^n$, avec p ne divisant pas q. Soit r un nombre entier fixé, $1 \leqslant r \leqslant n$. On note $E(r)$ l'ensemble des parties de G à p^r éléments. D'après le lemme (V.1.1), on a

$$card(E(r)) = C_{qp^n}^{p^r} = \lambda p^{n-r}.$$

Pour tout élément g de G, l'opération par translation à gauche de g sur G est une bijection. Par conséquent, pour tout élément X de $E(r)$, on a $card(g.X) = card(X)$ et le groupe G opère donc sur l'ensemble $E(r)$. Soient $\{X_i\}$, $1 \leqslant i \leqslant s$, l'ensemble des orbites distinctes et $\{x_i\}$, $1 \leqslant i \leqslant s$, une famille de représentants de ces orbites. D'après le corollaire (IV.2.1), on a

$$\lambda p^{n-r} = card(E(r)) = \sum_{i=1}^{s} [G : Stab_G(x_i)].$$

Si p^{n-r+1} divisait tous les termes $[G : Stab_G(x_i)]$, alors p^{n-r+1} serait en facteur dans la somme et il diviserait λ. Par conséquent, puisque p ne divise pas λ,

il existe un indice k, $1 \leqslant k \leqslant s$, tel que p^{n-r+1} ne divise pas $[G : Stab_G(x_k)]$. Posons $H = Stab_G(x_k)$.

Nous allons montrer que le sous-groupe H de G est d'ordre p^r.

Puisque G est un groupe, on a

$$\forall h \in G,\ \forall g \neq g' \in G,\ gh \neq g'h.$$

C'est en particulier vrai pour $h \in X_k$ et $g, g' \in H$, auquel cas gh et $g'h$ sont dans X_k, car $H = Stab_G(x_k)$. On en déduit donc une injection de H dans X_k, d'où $|H| \leqslant card(X_k) = p^r$.

D'autre part, on a $qp^n = |H|[G : H]$. Par conséquent, $[G : H]$ divise qp^n et p^{n-r+1} ne divise pas $[G : H]$. D'où $[G : H] = q'p^t$ avec q' divise q et $0 \leqslant t \leqslant n-r$. On en déduit que $|H| = \frac{q}{q'}p^{n-t}$. Mais, on a $r \leqslant n - t \leqslant n$, d'où p^r divise $|H|$ et $p^r \leqslant |H|$.

On a donc $p^r \leqslant |H| \leqslant p^r$, d'où l'égalité. □

Exercice V.1. Soient G un groupe fini et p un nombre premier divisant l'ordre de G. Montrer qu'il existe un élément d'ordre p dans G.

Définition V.1.1.

a) Un groupe fini d'ordre p^r, où p est un nombre premier, est appelé un ***p-groupe***.

b) Soient G un groupe et p un nombre premier divisant l'ordre de G. Un sous-groupe de G d'ordre p^r, où r est maximal tel que p^r divise l'ordre de G, est appelé un ***p-sous-groupe de Sylow*** de G.

Remarque V.1.1. Soient G un groupe fini et H un sous-groupe de G. Alors tout p-sous-groupe (resp. p-sous-groupe de Sylow) de G contenu dans H est un p-sous-groupe (resp. p-sous-groupe de Sylow) de H. (C'est une conséquence du théorème de Lagrange.)

V.2. Le second théorème de Sylow

Lemme V.2.1. *Soient G un groupe et $(p, n, r) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^*$, p premier ne divisant pas r. Soient H un sous-groupe de G d'indice r et K un sous-groupe de G d'ordre p^n. Alors K est contenu dans un conjugué de H.*

Démonstration. Posons $E = (G/H)_g$ et considérons l'opération de K par translation à gauche sur E. Alors, puisque $Card(E) = r$, d'après la proposition (IV.5.1),

on a $|E_K| \equiv r\,(mod\ p)$. Comme p ne divise pas r, $|E_K|$ n'est pas nul, donc E_K n'est pas vide. Mais, $xH \in E_K$ si et seulement si K est un sous-groupe de $Stab_G(xH) = xHx^{-1}$, donc K est un sous-groupe de xHx^{-1}. □

Lemme V.2.2. *Soit G un groupe fini et H un p-sous-groupe de Sylow de G. Alors H est l'unique p-sous-groupe de Sylow de son normalisateur $N_G(H)$.*

Démonstration. D'après la remarque (V.1.1), H est un p-sous-groupe de Sylow de $N_G(H)$. Donc $|N_G(H)| = qp^n$ avec p ne divisant pas q. Soit K un p-sous-groupe de Sylow de $N_G(H)$ (on a donc $|K| = |H|$). Alors, $[N_G(H) : K] = q$ et, d'après le lemme (V.2.1), K est un sous-groupe de xHx^{-1} pour $x \in N_G(H)$. Mais, si $x \in N_G(H)$, alors $xHx^{-1} = H$. Par conséquent, K est un sous-groupe de H et, puisque $|K| = |H|$, on a $H = K$. □

***Théorème V.2.1* (deuxième théorème de Sylow).** *Soient G un groupe fini et p un nombre premier divisant l'ordre de G.*

(i) *Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G.*

(ii) *Tous les p-sous-groupes de Sylow de G sont conjugués entre eux.*

(iii) *Le nombre de p-sous-groupes de Sylow de G est congru à 1 modulo p et divise l'ordre de G.*

Démonstration. Posons $|G| = qp^n$, avec p ne divisant pas q.

(i). Soient H un p-sous-groupe de G et S un p-sous-groupe de Sylow de G. On a $|H| = p^r$, $[G : S] = q$ et p ne divise pas q. D'après le lemme (V.2.1), H est un sous-groupe de xSx^{-1} pour un élément x de G. Mais $|xSx^{-1}| = |S|$, donc xSx^{-1} est un p-sous-groupe de Sylow de G.

(ii). Comme on l'a remarqué ci-dessus, le conjugué d'un p-sous-groupe de Sylow est un p-sous-groupe de Sylow. Soient S et S' deux p-sous-groupes de Sylow de G. Le raisonnement ci-dessus, appliqué à $H = S'$, montre que S' est un sous-groupe de xSx^{-1} pour un certain élément x de G. Puisque $|S'| = |S| = |xSx^{-1}|$, on en déduit que $S' = xSx^{-1}$.

(iii). Soit $\mathcal{S}$ l'ensemble des p-sous-groupes de Sylow de G. Le groupe G opère transitivement par conjugaison sur $\mathcal{S}$. Soit $H \in \mathcal{S}$

$$card(\mathcal{S}) = card(\Omega_H) = [G : Stab_G(H)].$$

Mais $Stab_G(H) = N_G(H)$ et $q = [G : H] = [G : N_G(H)][N_G(H) : H]$. Par conséquent, $card(\mathcal{S})$ divise q, donc $card(\mathcal{S})$ divise $qp^n = |G|$.

On considère l'action de H sur $\mathcal{S}$ par conjugaison et $\mathcal{S}_H$ l'ensemble des points fixes pour cette action. D'après la proposition (IV.5.1), on a

$$card(\mathcal{S}_H) \equiv card(\mathcal{S}) \quad mod(p).$$

Mais, un p-sous-groupe de Sylow H' appartient à $\mathcal{S}_H$ si et seulement si $H' = yH'y^{-1}$ pour tout élément y de H, *i.e.* si et seulement si H est un sous-groupe de $N_G(H')$. D'après le lemme (V.2.2), $N_G(H')$ ne contient qu'un seul p-sous-groupe de Sylow qui est H'. D'où $H = H'$ et $card(\mathcal{S}_H) = 1$. On en conclut que $card(\mathcal{S}) \equiv 1 \ (mod\, p)$. □

***Remarque* V.2.1.** La démonstration ci-dessus montre plus précisément que, si $|G| = qp^n$ avec p ne divisant pas q, le nombre de p-sous-groupes de Sylow de G divise q.

***Corollaire* V.2.1.**

(i) *Un groupe fini G admet un seul p-sous-groupe de Sylow S si et seulement si S est un sous-groupe normal de G.*

(ii) *Si G est un groupe abélien, pour tout nombre premier p divisant l'ordre de G, il n'y a qu'un seul p-sous-groupe de Sylow.*

Démonstration. (i). C'est une conséquence évidente du fait que les p-sous-groupes de Sylow d'un groupe G sont conjugués entre eux et qu'un sous-groupe de G est normal dans G si et seulement s'il est égal à tous ses conjugués dans G.

(ii). C'est une conséquence du point précédent et du fait que, dans un groupe abélien, tous les sous-groupes sont normaux. □

***Exercice* V.2.** Soit G un groupe d'ordre pqr, où $p > q > r$ sont des nombres premiers. On note, respectivement, n_p, n_q, n_r le nombre des p-sous-groupes, q-sous-groupes, r-sous-groupes de Sylow de G.

a) Montrer que $pqr \geqslant n_p(p-1) + n_q(q-1) + n_r(r-1) + 1$.

b) Montrer que

$$(n_p > 1,\ n_q > 1,\ n_r > 1) \Rightarrow (n_p = qr,\ n_q \geqslant p,\ n_r \geqslant q).$$

c) En déduire que G n'est pas simple.

V.3. Applications

Proposition V.3.1. *Soit G un groupe fini d'ordre pq, où p et q sont deux nombres premiers distincts et q n'est pas congru à 1 modulo p. Alors G n'a qu'un seul p-sous-groupe de Sylow.*

Démonstration. Le nombre de p-sous-groupes de Sylow de G est congru à 1 modulo p et divise q. Puisque q est premier et non congru à 1 modulo p, le nombre de p-sous-groupes de Sylow de G est égal à 1. □

Proposition V.3.2. *Soit G un groupe fini d'ordre pq, où p et q sont des nombres premiers distincts, alors G n'est pas simple.*

Démonstration. Puisque p et q sont distincts, on peut supposer que $p > q$ et, par conséquent, q n'est pas congru à 1 modulo p. Donc, d'après ce qui précède, G n'a qu'un seul p-sous-groupe de Sylow, qui est donc un sous-groupe normal non trivial de G. Donc G n'est pas un groupe simple. □

Proposition V.3.3. *Soient p et q deux nombres premiers distincts tels que*

$$p \not\equiv 1 \ (mod\ q) \ \text{ et } \ q \not\equiv 1 \ (mod\ p).$$

Alors, tout groupe d'ordre pq est cyclique.

Démonstration. D'après la proposition (V.3.1), il existe dans G un seul p-sous-groupe de Sylow S et un seul q-sous-groupe de Sylow T, qui sont donc des sous-groupes normaux de G, d'après le corollaire (V.2.1.(ii)). Puisque $|S| = p$ et $|T| = q$ qui sont premiers, S et T sont des groupes cycliques et leur intersection est réduite à $\{1\}$. Posons $S = \langle x\rangle$ et $T = \langle y\rangle$. Considérons $z = xyx^{-1}y^{-1}$; on a $x \in S$ et $yx^{-1}y^{-1} \in S$ puisque S est un sous-groupe normal de G, donc $z \in S$. Pour des raisons analogues $z \in T$, d'où $z = 1$ et $xy = yx$. Par conséquent xy est un élément d'ordre pq dans le groupe G, qui est lui-même d'ordre pq, donc $G = \langle xy\rangle$. □

Proposition V.3.4. *Soit G un groupe fini non trivial et soit $p_1^{n_1} \dots p_k^{n_k}$ la décomposition en facteurs premiers de l'ordre de G. Si pour tout i, $1 \leqslant i \leqslant k$, G a un unique p_i-sous-groupe de Sylow S_i, alors G est isomorphe au groupe $\prod_{1\leqslant i\leqslant k} S_i$, produit direct des groupes S_i, $1 \leqslant i \leqslant k$.*

Démonstration. D'après l'hypothèse, chacun des S_i est normal dans G et, par conséquent, $H = S_1 \dots S_k$ est un sous-groupe de G, dont on vérifie aisément qu'il est isomorphe au produit direct des (S_i), $1 \leqslant i \leqslant k$ (*cf.* exercice I.8). De plus, $|G| = |H|$, d'où le résultat. □

Corollaire V.3.1. *Soit G un groupe abélien fini non trivial et soit $p_1^{n_1} \dots p_k^{n_k}$ la décomposition en facteurs premiers de l'ordre de G. Alors G est isomorphe au produit direct de ses p_i-sous-groupes de Sylow, $1 \leqslant i \leqslant k$.* □

This page intentionally left blank

THÈMES DE RÉFLEXION

♠ TR.V.A. $Int(S_6) \neq Aut(S_6)$

Nous allons ici compléter l'étude du groupe des automorphismes du groupe S_n commencée au TR.II.C.

Pour tout $n \in \mathbb{N}^*$, on identifie S_n à S_E avec $E = \{1, \ldots, n\}$, (*cf.* TR.I.A), et on considère l'opération naturelle de S_n sur E (exemple IV.1.1.e). Pour tout élément i de E, on note $S(i)$ le stabilisateur de i pour cette action. On a vu à l'exemple (IV.2.1.e) que $S(i)$ est isomorphe à S_{n-1}, donc d'indice n dans S_n.

1. *Montrer que les sous-groupes $S(i)$ sont conjugués entre eux dans S_n.* (On utilisera la proposition (IV.2.2).)

2. *Montrer que pour $n \neq 4$, les assertions suivantes sont équivalentes :*

(i) $Int(S_n) = Aut(S_n)$.

(ii) *Les sous-groupes d'indices n de S_n sont conjugués entre eux dans S_n.* (On considérera un sous-groupe H d'indice n de S_n et l'isomorphisme $S_n \to S_{S_n/H}$ obtenu à partir de l'action par translation de S_n sur S_n/H).

Ce qui précède montre que si l'assertion (ii) ci-dessus est vérifiée, les sous-groupes d'indice n de S_n sont les $S(i)$. Pour montrer le résultat annoncé, il suffit donc de montrer que, lorsque $n = 6$, il existe un sous-groupe de S_6 qui n'est pas conjugué à un $S(i)$.

Soit P un 5-sous-groupe de Sylow de S_5 et soit N le normalisateur de P dans S_5.

3. *Montrer que $|N| = 20$.*

On a donc $card(S_5/N) = 6$.

4. *Montrer que S_5 opère transitivement et fidèlement sur S_5/N et en déduire un morphisme injectif de groupes $f : S_5 \to S_6$.*

5. *Montrer que $f(S_5)$ est un sous-groupe d'indice 6 de S_6 qui opère transitivement sur un ensemble à six éléments. Il n'est donc pas conjugué à un $S(i)$.*

♣ TR.V.B. Détermination des groupes d'ordre n, $n \leqslant 15$

On a étudié ce problème pour $n \leqslant 9$ au TR.I.C, et on connaît déjà la réponse pour les nombres 11 et 13, puisqu'ils sont premiers. D'autre part, la proposition (V.3.3) donne la réponse pour les groupes d'ordre 15.

Soit p un nombre premier impair. On considère un groupe G d'ordre $2p$ et on note n_2 le nombre de ses 2-sous-groupes de Sylow. D'après le théorème (V.2.1), on sait que $n_2 = 1$ ou $n_2 = p$.

1. *Montrer que si $n_2 = 1$, alors G est isomorphe au groupe $\mathbb{Z}/2p\mathbb{Z}$, et que si $n_2 = p$, alors G est isomorphe au groupe diédral D_p.*

Ceci détermine donc, en particulier, les groupes d'ordre n pour $n = 10$ et $n = 14$.

Il reste donc à examiner le cas où G est un groupe d'ordre 12. On note n_2 (resp. n_3) le nombre de 2-sous-groupes (resp. 3-sous-groupes) de Sylow de G, qui sont alors d'ordre 4 (resp. d'ordre 3). On sait que $n_2 = 1$ ou $n_2 = 3$ et que $n_3 = 1$ ou $n_3 = 4$.

2. *Montrer qu'on ne peut avoir simultanément $n_2 = 3$ et $n_3 = 4$.* (Considérer le nombre d'éléments d'ordre 3).

Cas $n_2 = 1$ et $n_3 = 1$

3. *Montrer qu'alors G est isomorphe au groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, et qu'il n'y a pas d'autre groupe abélien d'ordre 12 (à isomorphisme près).*

Cas $n_2 = 1$ et $n_3 = 4$

On note H_2 le 2-sous-groupe de Sylow de G et H_3 un 3-sous-groupe de Sylow de G.

4. *Montrer que H_2 est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et que G est le produit semi-direct de H_2 par H_3. En déduire que G est isomorphe au groupe A_4.*

Cas $n_2 = 3$ et $n_3 = 1$

On note H_3 le 3-sous-groupe de Sylow de G : on a $H_3 = \langle a \rangle$ avec $a^3 = 1$. On note H_2 un 2-sous-groupe de Sylow de G : on a $H_2 = \langle b \rangle$ avec $b^4 = 1$, ou $H_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, auquel cas on pose $H_2 = \{1, b, c, bc\}$.

On suppose que $H_2 = \langle b \rangle$ avec $b^4 = 1$.

5. *Montrer que* $G = \{1, a, a^2, b, b^2, b^3, ba, b^2a, b^3a, ba^2, b^2a^2, b^3a^2\}$. *En posant* $x = b^2a$, *montrer que* $\langle \{x, b\} | x^6, b^4, x^3b^{-2}, xbxb^{-1} \rangle$ *est une présentation du groupe* G *par générateurs et relations (groupe dicyclique d'ordre 12, noté* Q_{12}*).*

On suppose que $H_2 = \{1, b, c, bc\}$.

6. *Montrer qu'il existe un élément* x *dans* H_2 *tel que* $xax^{-1} \neq a$.

7. *On suppose que* $x = b$ *et on pose* $K = \langle b \rangle H_3$. *Montrer que* K *est le produit semi-direct de* H_3 *par* $\langle b \rangle$. *En déduire que* K *est isomorphe au groupe diédral* D_3.

8. *Montrer qu'il existe un élément* y *dans* H_2 *et non dans* K, *tel que* $yay^{-1} = a$. *Montrer que* y *commute avec tous les éléments de* H *et en déduire que le groupe* G *est isomorphe au groupe* $\mathbb{Z}/2\mathbb{Z} \times D_3$, *qui est lui-même isomorphe au groupe diédral* D_6.

En résumé, un groupe d'ordre 12 est isomorphe à l'un des groupes suivants :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},\ A_4,\ Q_{12},\ D_6.$$

♣ TR.V.C. Détermination des groupes d'ordre *pq*

Le but ici est de déterminer, à isomorphismes près, les groupes d'ordre pq, où p et q sont des nombres premiers.

Nous avons traité le cas $p = q$ dans l'exercice (IV.4). Pour mémoire, tout groupe d'ordre p^2, p premier, est abélien et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

On suppose maintenant que p et q sont deux nombres premiers, $p < q$, et que G est un groupe d'ordre pq.

1. *Montrer que* G *ne possède qu'un seul* q*-sous-groupe de Sylow.*

2. *En déduire que* G *est isomorphe à un produit semi-direct de* $\mathbb{Z}/q\mathbb{Z}$ *par* $\mathbb{Z}/p\mathbb{Z}$.

Nous avons vu au TR.I.B.10 que $Aut(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

3. *Montrer que :*

- *Si* p *ne divise pas* $(q-1)$, *il n'existe pas de morphisme non trivial de* $\mathbb{Z}/p\mathbb{Z}$ *dans* $Aut(\mathbb{Z}/q\mathbb{Z})$.
- *Si* p *divise* $(q-1)$, *il existe* $(p-1)$ *morphismes non triviaux, distincts deux à deux, de* $\mathbb{Z}/p\mathbb{Z}$ *dans* $Aut(\mathbb{Z}/q\mathbb{Z})$, *qu'on notera* φ_i, $1 \leqslant i \leqslant (p-1)$.

4. *Montrer que pour tout* $i \neq j$, $1 \leqslant i \leqslant (p-1)$, $1 \leqslant j \leqslant (p-1)$, *les groupes* $\mathbb{Z}/q\mathbb{Z} \underset{\varphi_i}{\times} \mathbb{Z}/p\mathbb{Z}$ *et* $\mathbb{Z}/q\mathbb{Z} \underset{\varphi_j}{\times} \mathbb{Z}/p\mathbb{Z}$ *sont isomorphes.* (On appliquera l'exercice (IV.6.2).)

On en déduit donc qu'il n'existe, à isomorphisme près, qu'un seul produit semi-direct non trivial de $\mathbb{Z}/q\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$, qu'on notera $\mathbb{Z}/q\mathbb{Z} \underset{\varphi}{\times} \mathbb{Z}/p\mathbb{Z}$.

5. *En déduire que tout groupe d'ordre pq, p et q premiers, $p < q$, est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$ ou à $\mathbb{Z}/q\mathbb{Z} \underset{\varphi}{\times} \mathbb{Z}/p\mathbb{Z}$.*

On remarquera qu'on retrouve ici, comme cas particulier, le résultat de la proposition (V.3.3).

VI

GROUPES ABÉLIENS

Nous allons montrer dans ce chapitre que le fait, pour un groupe, d'être abélien permet de décrire plus précisément sa structure, en particulier lorsqu'il est engendré par un nombre fini d'éléments.

Les groupes considérés dans ce chapitre étant tous abéliens, leurs lois seront notées additivement, l'élément neutre sera noté 0, le symétrique de tout élément x sera noté $-x$.

On trouvera dans le second volume de cet ouvrage une étude de la structure de ***module***. C'est une structure analogue à celle d'espace vectoriel, dans laquelle le corps de base est remplacé par un anneau. Ce changement modifie substantiellement les propriétés de la structure, mais le formalisme linéaire (*i.e.* l'utilisation des combinaisons linéaires) est le même que dans le cadre des espaces vectoriels. Un groupe abélien est un module sur l'anneau $\mathbb{Z}$, ce qui se traduira dans ce qui suit par l'utilisation de combinaisons linéaires à coefficients dans $\mathbb{Z}$.

VI.1. Somme directe de groupes abéliens

A - Somme directe de sous-groupes d'un groupe abélien

Nous avons déjà remarqué qu'une réunion de sous-groupes d'un groupe n'est pas, en général, un sous-groupe. Nous allons nous intéresser ici au sous-groupe *engendré* par une réunion de sous-groupes.

Définition* VI.1.1.** Soient G un groupe abélien et $(H_i)_{i\in I}$ une famille non vide de sous-groupes de G. On appelle ***somme des sous-groupes $H_i, i \in I$, qu'on note $\sum_{i\in I} H_i$, le sous-groupe de G engendré par $\bigcup_{i\in I} H_i$.

***Proposition* VI.1.1.** *Soient G un groupe abélien et $(H_i)_{i\in I}$ une famille non vide de sous-groupes de G. Alors un élément x de G appartient à $\sum_{i\in I} H_i$ si et seulement si x s'écrit comme une somme finie*

$$x = x_{i_1} + \ldots + x_{i_k}$$

avec $x_{i_j} \in H_{i_j}$, $1 \leqslant j \leqslant k$, et $i_1, \ldots, i_k \in I$.

Démonstration. On a $\sum_{i\in I} H_i = \langle S\rangle$, avec $S = \bigcup_{i\in I} H_i$, et la proposition est une conséquence de la remarque (I.2.2). □

Dans l'écriture ci-dessus, pour un x donné, les éléments x_{i_j} ne sont pas uniques. Pour obtenir l'unicité de l'écriture de x en fonction des x_{i_j}, on est amené à considérer la définition suivante :

Définition* VI.1.2.** Soient G un groupe abélien et $(H_i)_{i\in I}$ une famille non vide de sous-groupes de G. Le sous-groupe $\sum_{i\in I} H_i$ est ***somme directe des sous-groupes H_i si

$$\forall j \in I,\ H_j \cap \sum_{\substack{i\in I\\ i\neq j}} H_i = \{0\}.$$

Dans ce cas, le sous-groupe $\sum_{i\in I} H_i$ est noté $\bigoplus_{i\in I} H_i$.

***Proposition* VI.1.2.** *Soient G un groupe abélien et $(H_i)_{i\in I}$ une famille non vide de sous-groupes de G. Le sous-groupe $H = \sum_{i\in I} H_i$ est somme directe des H_i si et seulement si tout $x \in H$ s'écrit de manière <u>unique</u> $x = \sum_{1\leqslant j\leqslant k} x_{i_j}$ avec $k \in \mathbb{N}^*$, $\{i_1, \ldots, i_k\} \subset I$, $x_{i_j} \in H_{i_j}$, $1 \leqslant j \leqslant k$.*

Démonstration. Cette démonstration est la même que celle de la proposition analogue dans le cas des espaces vectoriels et laissée au lecteur à titre d'exercice. □

B - Somme directe de groupes abéliens

Proposition - Définition VI.1.3. *Soient I un ensemble non vide et $(G_i)_{i\in I}$ une famille de groupes abéliens. Le sous-ensemble du groupe $\prod_{i\in I} G_i$, (*cf. *proposition I.3.5), formé par les éléments qui n'ont qu'un nombre fini de composantes non nulles, est un sous-groupe de $\prod_{i\in I} G_i$, appelé somme directe des groupes abéliens G_i, $i \in I$, et noté $\bigoplus_{i\in I} G_i$.* □

Remarques VI.1.1.

a) Pour tout $i \in I$, l'application $\lambda_i : G_i \to \bigoplus_{i\in I} G_i$, qui à x_i associe la suite dont tous les termes sont nuls sauf celui d'indice i qui est égal à x_i, est un morphisme (injectif) de groupes.

b) Les groupes $\bigoplus_{i\in I} G_i$ et $\prod_{i\in I} G_i$ sont égaux si et seulement si l'ensemble I est fini.

c) Si pour tout $i \in I$, on a $G_i = G$, on pose $G^I = \prod_{i\in I} G_i$ et $G^{(I)} = \bigoplus_{i\in I} G_i$.

d) Si I et J sont deux ensembles non vides,

$$[card(I) = card(J)] \Longrightarrow [G^I = G^J \quad \text{et} \quad G^{(I)} = G^{(J)}].$$

Nous avons déjà vu au chapitre I que le produit direct de groupes est solution du problème universel de produit de groupes et que cette solution est la même, que l'on considère des groupes abéliens ou non abéliens. Nous avons posé et résolu le problème universel de somme de groupes non abéliens (*cf.* TR.III.D). Nous allons maintenant montrer que ce problème de somme de groupes admet une réponse très différente de celle vue au TR.III.D, dès lors qu'il s'agit de groupes abéliens.

Théorème VI.1.1 **(propriété universelle de la somme directe de groupes abéliens).** *Soient I un ensemble non vide et $(G_i)_{i\in I}$ une famille de groupes abéliens. Avec les notations ci-dessus, pour tout groupe abélien G et toute famille de morphismes de groupes $f_i : G_i \to G$, $i \in I$, il existe un unique morphisme de groupes $g : \bigoplus_{i\in I} G_i \to G$ tel que, pour tout $i \in I$, $g \circ \lambda_i = f_i$.*

Démonstration. Existence de g : Soit $(x_i)_{i\in I}$ un élément de $\bigoplus_{i\in I} G_i$. Posons

$$g((x_i)_{i\in I}) = \sum_{i\in I} f_i(x_i).$$

Seul un nombre fini de termes x_i étant non nuls, cette somme est bien définie. D'autre part, le groupe G étant abélien, on vérifie aisément que g est un homomorphisme de groupes. De plus, soit $x \in G_i$: pour tous $i, j \in I$, $j \neq i$, on a $(\lambda_i(x))_j = 0$, d'où $g(\lambda_i(x)) = f_i(x)$ et $g \circ \lambda_i = f_i$, pour tout $i \in I$.

Unicité de g : Tout élément x de $\bigoplus_{i\in I} G_i$ s'écrit de manière unique $\lambda_{i_1}(x_{i_1}) + \ldots + \lambda_{i_n}(x_{i_n})$. Par conséquent, quel que soit le morphisme g vérifiant $g \circ \lambda_i = f_i$ pour tout $i \in I$, on a $g(x) = f_{i_1}(x_{i_1}) + \ldots + f_{i_n}(x_{i_n})$, ce qui prouve l'unicité de g. □

Nous allons donner deux propositions qui sont des corollaires immédiats du théorème ci-dessus.

Corollaire VI.1.1. *Soient I un ensemble non vide et $(G_i)_{i\in I}$ une famille de groupes abéliens. Un groupe G est isomorphe au groupe $\bigoplus_{i\in I} G_i$ si et seulement s'il existe une famille $(H_i)_{i\in I}$ de sous-groupes de G tels que*

(i) $H_i \simeq G_i$, $\forall i \in I$.

(ii) $G = \bigoplus_{i\in I} H_i$. □

Corollaire VI.1.2. *Soient I un ensemble non vide, $(G_i)_{i\in I}$ et $(G'_i)_{i\in I}$ deux familles de groupes abéliens telles que, pour tout $i \in I$, les groupes G_i et G'_i soient isomorphes. Alors les groupes $\bigoplus_{i\in I} G_i$ et $\bigoplus_{i\in I} G'_i$ sont isomorphes.* □

C - Facteur direct d'un groupe abélien

Définition VI.1.3. Soient G un groupe abélien et H un sous-groupe de G. On dit que H est un ***facteur direct*** de G s'il existe un sous-groupe K de G tel que $G = H \oplus K$.

Attention. *Un sous-groupe d'un groupe abélien n'est pas toujours un facteur direct de ce groupe. C'est l'une des différences entre espaces vectoriels et modules.*

Exercice VI.1. Montrer que le groupe abélien $(\mathbb{Z}, +)$ n'est pas un facteur direct du groupe abélien $(\mathbb{Q}, +)$.

Proposition VI.1.4. *Soient G un groupe abélien, H un sous-groupe de G et $i : H \hookrightarrow G$ l'injection canonique. Alors H est un facteur direct de G si et seulement s'il existe $p \in Hom(G, H)$ tel que $p \circ i = id_H$.*

Démonstration. Supposons que $G = H \oplus K$. Tout élément g de G s'écrit de manière unique $g = h + k$, avec $h \in H$ et $k \in K$. On définit p par $p(g) = h$ et on vérifie aisément que c'est un morphisme de groupes répondant à la question.

Supposons qu'il existe un morphisme de groupes $p : G \to H$ tel que $p \circ i = id_H$. Pour tout élément g de G on pose $h = p(g)$: on a alors $h = p \circ i(h) = p(h)$, *i.e.* $(g - h) \in Ker(p)$. On a $g = h + (g - h)$ et, si $x \in H \cap Ker(p)$, alors on a $x = p(x) = 0$, d'où $G = H \oplus Ker(p)$. □

VI.2. Groupes abéliens libres

A - Définition - Propriété universelle

Définition* VI.2.1.** On dit qu'un groupe abélien est ***libre s'il est somme directe de groupes monogènes infinis.

Autrement dit, un groupe abélien G est libre s'il existe un ensemble I et une famille d'éléments de G, $X = \{x_i\}_{i\in I}$, tels que

$$G = \bigoplus_{i\in I} \langle x_i\rangle \quad \text{et} \quad \langle x_i\rangle \simeq \mathbb{Z}, \quad \forall\, i \in I.$$

La famille X est ***une base*** de G.

L'écriture ci-dessus montre que, à isomorphisme près, il n'existe qu'un seul groupe abélien libre de base donnée X.

***Remarques* VI.2.1.**

a) D'après le corollaire (VI.1.1), en identifiant $\langle x_i\rangle$ à $\mathbb{Z}$, on peut aussi écrire $G \simeq \mathbb{Z}^{(I)}$, ou, en appliquant la remarque (VI.1.1.d), $G \simeq \mathbb{Z}^{(X)}$.

Autrement dit, si l'on écrit le groupe G sous la forme $\mathbb{Z}^{(I)}$, cela signifie qu'on considère que G est libre de base un ensemble non précisé de cardinal égal au cardinal de I ; si on écrit G sous la forme $\mathbb{Z}^{(X)}$, cela signifie que l'on précise une base $X = \{x_i\}_{i\in I}$ de G.

b) Il est clair, d'après la définition, qu'une somme directe de groupes abéliens libres est un groupe abélien libre. Précisément, $\mathbb{Z}^{(X)} \bigoplus \mathbb{Z}^{(Y)} = \mathbb{Z}^{(X\cup Y)}$.

***Théorème* VI.2.1.** *Soient G un groupe abélien non nul et $X = \{x_i\}_{i\in I}$ une famille non vide d'éléments de G. Les assertions suivantes sont équivalentes :*

(i) *G est un groupe abélien libre de base X*

(ii) *Tout élément x de G s'écrit de manière unique sous la forme*

$$x = \sum_{1\leqslant j\leqslant k} n_j\, x_{i_j}$$

où $k \in \mathbb{N}^*$, $\{i_1, \ldots, i_k\} \subseteq I$, et $n_j \in \mathbb{Z}$ pour tout j, $1 \leqslant j \leqslant k$

(iii) *La famille X est une partie génératrice de G telle que, quelle que soit la partie finie non vide $\{i_1, \ldots, i_k\}$ de I, la relation*

$$\sum_{1\leqslant j\leqslant k} n_j\, x_{i_j} = 0, \quad \text{où} \quad n_j \in \mathbb{Z} \quad \forall j \quad (1 \leqslant j \leqslant k)$$

implique $n_j = 0$ pour tout j, $1 \leqslant j \leqslant k$.

Démonstration. (i) $\Leftrightarrow$ (ii). Le groupe G est égal à $\bigoplus_{i\in I}\langle x_i\rangle$ si et seulement si tout élément x de G s'écrit de manière unique $x=\sum_{1\leqslant j\leqslant k} y_{i_j}$, avec $y_{i_j}\in\langle x_{i_j}\rangle$. Mais y_{i_j} s'écrit de manière unique $y_{i_j}=n_j x_{i_j}$ avec $n_j\in\mathbb{Z}$, d'où le résultat.

(ii) $\Rightarrow$(iii). L'écriture de tout élément x de G donnée par (ii) montre que X est une partie génératrice. De plus l'élément 0 s'écrit $0=\sum_{1\leqslant j\leqslant k} n_{i_j}x_{i_j}$ avec $n_{i_j}=0$, $1\leqslant j\leqslant k$. Cette écriture étant unique par hypothèse, on en déduit le résultat.

(iii) $\Rightarrow$ (ii). La partie X étant génératrice, pour tout élément x de G, il existe un ensemble fini J tel que $x=\sum_{j\in J} n_j x_{i_j}$. S'il existe un autre ensemble fini L tel que $x=\sum_{l\in L} m_l x_{i_l}$, on a

$$0=\left(\sum_{j\in J} n_j x_{i_j}\right)-\left(\sum_{l\in L} m_l x_{i_l}\right)$$

$$0=\left(\sum_{p\in J\cap L}(n_p-m_p)x_{i_p}\right)+\left(\sum_{j\in J, j\notin L} n_j x_{i_j}\right)-\left(\sum_{l\in L, l\notin J} m_l x_{i_l}\right).$$

La condition (iii) implique que chacun des coefficients de cette somme est nul. On en déduit que $J=L$ et $n_j=m_j$ pour tout $j\in J$. □

Terminologie. Une famille $X=\{x_i\}_{i\in I}$ satisfaisant à la condition (iii) ci-dessus est dite ***libre*** sur $\mathbb{Z}$. On dit aussi que les éléments x_i, $i\in I$, sont ***linéairement indépendants*** sur $\mathbb{Z}$. Autrement dit, X est une ***base*** de G si et seulement si c'est une ***partie libre et génératrice***.

On remarquera qu'une sous-famille non vide d'une famille libre sur $\mathbb{Z}$ est libre sur $\mathbb{Z}$.

Théorème VI.2.2 **(propriété universelle d'un groupe abélien libre).** *Soient G un groupe abélien, X une partie de G, j_X l'inclusion canonique de X dans G. Alors G est abélien libre de base X si et seulement si, pour tout groupe abélien A et toute application $\sigma: X\to A$, il existe un unique morphisme de groupes $f: G\to A$ tel que $f\circ j_X=\sigma$.*

Démonstration. Supposons que le groupe abélien G soit libre de base X.

Existence de f : Notons $X=\{x_i\}_{i\in I}$ la base donnée de G. Tout élément x de G s'écrit de manière unique $x=\sum_{i\in I} n_i x_i$, où les n_i sont des entiers nuls sauf pour un nombre fini de $i\in I$. Par conséquent, si on pose $f(x)=\sum_{i\in I} n_i\sigma(x_i)$, cette somme est bien définie. On vérifie aisément que l'application f ainsi définie est un morphisme de groupes vérifiant $f\circ j_X=\sigma$.

Unicité de f : Soit $f' : G \to A$ un autre morphisme de groupes vérifiant $f' \circ j_X = \sigma$. Alors, pour tout élément x_i de X, on a $f(x_i) = f'(x_i)$, d'où $f(x) = f'(x)$ pour tout élément x de G.

On suppose maintenant que le groupe abélien G est tel que pour tout groupe abélien A et toute application $\sigma : X \to A$, il existe un unique morphisme de groupes $f : G \to A$ tel que $f \circ j_X = \sigma$. C'est en particulier vérifié si $A = \mathbb{Z}^{(X)}$ est libre de base X et $\sigma = i_X$ est l'injection de X dans $\mathbb{Z}^{(X)}$. Le début de la démonstration montre qu'il existe un morphisme de groupes $g : A \longrightarrow G$ tel que $g \circ i_X = j_X$. On vérifie que les morphismes f et g sont réciproques l'un de l'autre. Ce sont donc des isomorphismes. □

Corollaire VI.2.1. *Tout groupe abélien est isomorphe à un quotient d'un groupe abélien libre.*

Démonstration. Soit X une partie génératrice d'un groupe abélien G et σ l'inclusion de X dans G. On considère le groupe libre de base X, $\mathbb{Z}^{(X)}$, et j_X l'inclusion de X dans $\mathbb{Z}^{(X)}$. D'après le théorème (VI.2.2), il existe un morphisme de groupes $f : \mathbb{Z}^{(X)} \to G$ tel que $f \circ j_X = \sigma$. Montrons que f est surjectif. En effet, tout élément x de G s'écrit

$$x = \sum_{1 \leqslant l \leqslant k} n_l \sigma(x_{i_l}) = \sum_{1 \leqslant l \leqslant k} n_l f(j_X(x_{i_l})) = f\left(\sum_{1 \leqslant l \leqslant k} n_l j_X(x_{i_l}) \right).$$

On en déduit que le groupe G est isomorphe au groupe $\mathbb{Z}^{(X)}/Ker(f)$. □

Corollaire VI.2.2. *Si $p : G \longrightarrow G'$ est un homomorphisme surjectif de groupes abéliens et si G' est libre, alors il existe un homomorphisme de groupes abéliens $s : G' \longrightarrow G$ tel que $p \circ s = id_{G'}$. En particulier, $s(G')$ est un facteur direct de G.*

Démonstration. Soit X une base de G'. Puisque p est surjectif, il existe une application $j : X \to G$ telle que $p \circ j = id_X$. D'après le théorème (VI.2.2), il existe un morphisme de groupes $s : G' \to G$ tel que $p \circ s = id_{G'}$. On déduit de la proposition (VI.1.4) que $s(G')$ est facteur direct dans G. □

Remarque VI.2.2. L'égalité $p \circ s = id_{G'}$ implique que le morphisme s est injectif et donc que le groupe G' est isomorphe au sous-groupe $s(G')$ de G. Par conséquent, on peut dire que, sous les hypothèses du corollaire (VI.2.1), le groupe G' est isomorphe à un facteur direct du groupe G.

Exercice VI.2. Montrer que sous les hypothèses ci-dessus, on a

$$G = Ker(p) \oplus s(G').$$

Terminologie. Avec les notations ci-dessus, on dit que s est une ***section*** de p.

B - Rang d'un groupe abélien libre

Soient X et Y deux ensembles équipotents et $\varphi : X \to Y$ une application bijective. On considère les groupes abéliens libres $\mathbb{Z}^{(X)}$ et $\mathbb{Z}^{(Y)}$ ainsi que les inclusions canoniques $j_X : X \to \mathbb{Z}^{(X)}$ et $j_Y : Y \to \mathbb{Z}^{(Y)}$. En appliquant le théorème (VI.2.2) à

$$j_Y \circ \varphi : X \to \mathbb{Z}^{(Y)} \quad \text{et} \quad j_X \circ \varphi^{-1} : Y \to \mathbb{Z}^{(X)},$$

on obtient deux morphismes de groupes

$$\mathbb{Z}^{(X)} \to \mathbb{Z}^{(Y)} \quad \text{et} \quad \mathbb{Z}^{(Y)} \to \mathbb{Z}^{(X)}$$

qui sont des isomorphismes réciproques l'un de l'autre. On en déduit donc la proposition suivante :

Proposition VI.2.1. *Si deux ensembles X et Y sont tels que que $card(X) = card(Y)$, alors les groupes abéliens libres de bases X et Y sont isomorphes.* □

Ceci nous conduit à nous demander si le cardinal d'une base caractérise, à isomorphisme près, un groupe abélien libre. Nous allons d'abord étudier le cas où le groupe est engendré par une partie finie, puis étudier ensuite le cas général.

Définition VI.2.2. Un groupe (non nécessairement abélien) est dit de **type fini** s'il est engendré par une partie finie.

Exemple VI.2.1. Pour tout entier n, $\mathbb{Z}^n$ est un groupe abélien libre de type fini.

Exercice VI.3. Montrer que le groupe abélien $(\mathbb{Q}, +)$ n'est pas libre, n'est pas de type fini.

Théorème VI.2.3.

(i) *Un groupe abélien libre G est de type fini si et seulement s'il a une base finie.*

(ii) *Dans ce cas, toutes les bases de G ont le même nombre d'éléments.*

Démonstration. (i). Il est clair que si le groupe G admet une base finie, il est de type fini.

Supposons que le groupe G est libre de type fini. Cela signifie que, d'une part, il admet une base $X = \{x_i\}_{i \in I}$ et que, d'autre part, il admet une partie génératrice finie $Y = \{y_1, \ldots, y_k\}$. Pour tout j, $1 \leqslant j \leqslant k$, il existe une partie finie I_j contenue dans I telle que $y_j \in \sum_{i \in I_j} \langle x_i \rangle$. Mais comme tout élément x de G

s'écrit $x = \sum_{j=1}^{k} n_j y_j$, alors $x \in \sum_{j\in L}\langle x_j\rangle$, avec $L = \bigcup_{1\leqslant j\leqslant k} I_j$. On en déduit que $\{x_i\}_{i\in L}$ est une partie finie, génératrice, libre comme sous-famille d'une famille libre.

(ii). Démontrons que $I = L$, ce qui prouvera que toutes les bases sont finies. On a $L \subseteq I$: supposons qu'il existe p contenu dans I et non contenu dans L. On peut donc écrire $x_p = \sum_{j\in L} n_j x_j$, puisque $\{x_j\}_{j\in L}$ est une base de G. Par conséquent, l'intersection

$$\langle x_p\rangle \cap \sum_{j\in I, j\neq p} \langle x_j\rangle$$

est non vide, ce qui est en contradiction avec l'hypothèse $G = \bigoplus_{j\in I}\langle x_j\rangle$.

Montrons maintenant que toutes les bases de G ont le même nombre d'éléments. Soit $\{x_1, \ldots, x_n\}$ une base de G. On considère le sous-groupe $2G$ de G. Un élément x appartient à $2G$ si et seulement si $x = \sum_{i=1}^{n} n_i x_i$ avec $n_i \in 2\mathbb{Z}$, d'où

$$2G = \bigoplus_{i=1}^{n} 2\langle x_i\rangle.$$

On a donc

$$G/2G \simeq \left(\bigoplus_{i=1}^{n}\langle x_i\rangle\right) / \left(\bigoplus_{i=1}^{n} 2\langle x_i\rangle\right) \simeq \bigoplus_{i=1}^{n}(\langle x_i\rangle/2\langle x_i\rangle)$$

(pour ce dernier isomorphisme, *cf.* exercice II.6.1). Mais, $\langle x_i\rangle/2\langle x_i\rangle \simeq \mathbb{Z}/2\mathbb{Z}$ pour tout i et, par conséquent, $G/2G \simeq (\mathbb{Z}/2\mathbb{Z})^n$.

Si nous considérons un autre base $\{y_1, \ldots, y_p\}$ de G, le même raisonnement conduit à l'isomorphisme $G/2G \simeq (\mathbb{Z}/2\mathbb{Z})^p$. On a donc $n = p$ et toutes les bases de G sont finies et ont même nombre d'éléments. □

Plus généralement, on a :

Théorème VI.2.4. *Quels que soient les ensembles X et Y,*

$$[\mathbb{Z}^{(X)} \simeq \mathbb{Z}^{(Y)}] \Longleftrightarrow [card(X) = card(Y)].$$

Démonstration. On a déjà vu à la proposition (VI.2.1) que si $card(X) = card(Y)$, alors le groupe libre $\mathbb{Z}^{(X)}$ est isomorphe au groupe libre $\mathbb{Z}^{(Y)}$, par un isomorphisme prolongeant une bijection donnée entre les deux ensembles équipotents X et Y. Précisons alors le cardinal de $\mathbb{Z}^{(X)}$. □

Lemme VI.2.1. *Si X est un ensemble fini, alors $\mathbb{Z}^{(X)}$ est un ensemble dénombrable.*

Démonstration. Si $card(X) = n$, le groupe $\mathbb{Z}^{(X)}$ est isomorphe au groupe $\mathbb{Z}^n$ et on sait qu'un produit fini d'ensembles dénombrables est dénombrable (*cf.* appendice). □

Supposons que X et Y soient deux ensembles tels que les groupes $\mathbb{Z}^{(X)}$ et $\mathbb{Z}^{(Y)}$ soient isomorphes. Si X est un ensemble fini, le résultat est un corollaire évident du théorème (VI.2.3.(ii)). Supposons X infini, nous allons alors démontrer le lemme suivant :

***Lemme* VI.2.2.** *Si X est un ensemble infini, alors $card(\mathbb{Z}^{(X)}) = card(X)$.*

Démonstration. Posons $X = \{x_i\}_{i\in I}$ et notons $\mathcal{F}(X)$ l'ensemble des parties finies de X. On considère l'application $f : \mathbb{Z}^{(X)} \to \mathcal{F}(X)$ qui à x associe la partie A_x définie de la façon suivante :

- Si $x = 0$, on pose $A_x = \emptyset$.
- Si x est non nul, il s'écrit de manière unique $x = \sum_{1\leqslant j\leqslant k} n_j x_{i_j}$ et on pose $A_x = \{x_{i_1}, \ldots, x_{i_k}\}$.

Il est clair que f est une application surjective. D'autre part, pour toute partie A de $\mathcal{F}(X)$, $f^{-1}(A)$ est contenu dans $\mathbb{Z}^{(A)}$ qui, d'après le lemme (VI.2.1), est dénombrable puisque A est finie.

Mais, si f est une application surjective d'un ensemble E sur un ensemble infini F telle que, pour tout élément x de F, $f^{-1}(x)$ soit dénombrable, alors les ensembles E et F sont équipotents (*cf.* appendice).

On en déduit donc que $card(\mathbb{Z}^{(X)}) = card(\mathcal{F}(X))$. Mais, lorsque l'ensemble X est infini, les ensembles X et $\mathcal{F}(X)$ sont équipotents (*cf.* appendice). D'où le lemme. Par conséquent, si les groupes $\mathbb{Z}^{(X)}$ et $\mathbb{Z}^{(Y)}$ sont isomorphes, on a

$$card(X) = card(\mathbb{Z}^{(X)}) = card(\mathbb{Z}^{(Y)}) = card(Y).$$ □

***Remarque* VI.2.3.** La démonstration ci-dessus et le TR.I.B montrent que pour tout ensemble X, il existe un groupe abélien équipotent à X. Autrement dit, sur tout ensemble on peut définir une structure de groupe, comme cela a été précisé à la remarque (I.1.1.d).

Les considérations précédentes conduisent à la définition suivante :

Définition* VI.2.3.** Si G est un groupe abélien libre, le cardinal d'une base de G est appelé le ***rang de G.

On remarquera que si G et H sont des groupes libres de rangs finis respectifs p et q, alors $G \bigoplus H$ est un groupe libre de rang $p+q$.

C - Sous-groupes d'un groupe abélien libre

Nous avons admis au chapitre III qu'un sous-groupe d'un groupe libre est un groupe libre. Nous allons ici montrer que ce résultat est également vrai dans le cadre des groupes abéliens.

Attention. *Notons $\mathcal{A}$ la classe des groupes abéliens et $\mathcal{G}$ celle des groupes. Il est évident que $\mathcal{A}$ est contenue dans $\mathcal{G}$. Cependant, un groupe abélien libre G n'est pas un groupe libre lorsqu'on le considère dans $\mathcal{G}$. Il suffit pour s'en convaincre de remarquer que si X est un ensemble ayant au moins deux éléments distincts, le groupe abélien libre de base X est abélien par définition, alors que le groupe libre de base X n'est pas abélien* (cf. *remarque III.1.1.b). Par conséquent, le fait qu'un sous-groupe d'un groupe libre soit un groupe libre n'implique pas qu'il en soit de même pour les groupes abéliens.*

Théorème VI.2.5. *Tout sous-groupe d'un groupe abélien libre est un groupe abélien libre.*

Démonstration. Nous allons donner d'abord une démonstration élémentaire dans le cas du rang fini, qui permet de préciser que le rang du sous-groupe est inférieur ou égal au rang du groupe ; le cas infini nécessite une démonstration plus élaborée.

Le groupe réduit à l'élément neutre étant libre de base l'ensemble vide, dans la suite on ne considérera que des sous-groupes non triviaux.

(VI.2.5.1). Supposons que G soit un groupe abélien libre de rang fini n ; nous allons faire un raisonnement par récurrence sur n.

Si $n = 1$, le groupe G est isomorphe à $\mathbb{Z}$. Tout sous-groupe de G est donc isomorphe à un $k\mathbb{Z}$, donc à $\mathbb{Z}$ et, par conséquent, est un groupe abélien libre de rang 1.

Supposons le résultat vrai pour les groupes abéliens libres de rang $r \leqslant n-1$ et soit G un groupe libre de rang n. Alors G est isomorphe à $\mathbb{Z}^n$; considérons le morphisme de groupes $p : \mathbb{Z}^n \to \mathbb{Z}$ défini par $p((x_1, \ldots, x_n)) = x_n$. Il est clair que $Ker(p) = \{(x_1, \ldots, x_{n-1}, 0) | x_i \in \mathbb{Z}\}$ est un groupe isomorphe à $\mathbb{Z}^{n-1}$, donc libre de rang $n-1$. Tout sous-groupe de G est isomorphe à un sous-groupe H de $\mathbb{Z}^n$. On a $p(H) = a\mathbb{Z}$; si $a = 0$, alors H est contenu dans $Ker(p)$ et le résultat découle de l'hypothèse de récurrence. Si $a \neq 0$, $p(H)$ est un sous-groupe de $\mathbb{Z}$, donc libre, et le morphisme $H \to p(H)$ est surjectif et a pour noyau $H \cap \mathbb{Z}^{n-1}$,

qui est libre par hypothèse de récurrence. On déduit de l'exercice (VI.2) que $H \simeq (H \cap \mathbb{Z}^{n-1}) \oplus p(H)$, et H est un groupe abélien libre comme somme directe de groupes abéliens libres. De plus, $p(H)$ est de rang inférieur ou égal à 1 et $(H \cap \mathbb{Z}^{n-1})$ est, par hypothèse, de rang inférieur ou égal à $n-1$. D'où le résultat.

(VI.2.5.2). Considérons maintenant un groupe abélien libre $G \neq \{0\}$ de base $X = \{x_i\}_{i\in I}$ **quelconque** et H un sous-groupe propre de G.

Pour tout $k \in I$, on note $\pi_k : G \to \mathbb{Z}$ le morphisme $k^{\text{ième}}$ coordonnée, *i.e.* $\pi_k(g) = n_k$ avec $g = \sum_{i\in I} n_i x_i$.

On peut toujours supposer que I est muni d'une structure d'ensemble ***bien ordonné*** (*cf.* appendice). Pour tout $t \in I$, on note G_t le sous-groupe de G engendré par les éléments x_i pour $i \leqslant t$, et on pose $H_t = H \cap G_t$. L'image de H_t par π_t est un sous-groupe de $\mathbb{Z}$, $\pi_t(H_t) = \mathbb{Z}a_t$. On note y_t un élément de H_t tel que $\pi_t(y_t) = a_t$. Si $a_t = 0$, on prend $y_t = 0$.

Pour tout $s \in I$, on considère K_s le sous-groupe de G engendré par les éléments y_t pour $t \leqslant s$. Donc K_t est contenu dans H_t, pour tout t. Nous allons montrer que, pour tout $s \in I$, $K_s = H_s$, ce qui prouvera que le sous-groupe H lui-même est engendré par les éléments $(y_s)_{s\in I}$.

Supposons que, par hypothèse de récurrence, on ait : pour tout $t < s$, $K_t = H_t$. Cette hypothèse est bien vérifiée pour le plus petit élément de I. Pour tout élément $x \in H_s$, on a $\pi_s(x) = qa_s$, $q \in \mathbb{Z}$, donc $x - qy_s$ s'écrit comme combinaison linéaire d'un nombre fini de x_i, avec $i < s$. On a donc $x - qy_s \in H_t$, avec $t < s$. D'où, d'après l'hypothèse de récurrence, $x - qy_s \in K_t$. Mais, $K_t \subset K_s$ et, par conséquent, l'élément x appartient à K_s, d'où $K_s = H_s$.

Ce qui précède prouve que la famille $(y_s)_{s\in I}$ est génératrice de H. Montrons maintenant que la sous-famille des y_s qui ne sont pas nuls est libre sur $\mathbb{Z}$. Supposons qu'il existe une relation $S = \sum_{finie} n_i y_i = 0$, dans laquelle il existe des termes non nuls. On note k le plus grand indice i tel que $n_i y_i \neq 0$. Puisque $\pi_k(y_i) = 0$ pour $i < k$, on a $\pi_k(n_k y_k) = \pi_k(S) = 0$. Mais, $\pi_k(n_k y_k) = n_k a_k$ et, puisque $a_k \neq 0$, on doit avoir $n_k = 0$, ce qui est contraire à l'hypothèse.

On en déduit que la famille des $(y_s)_{s\in I}$ qui sont non nuls est une base de H, qui est donc un groupe abélien libre. □

Corollaire VI.2.3. *Si H est un sous-groupe d'un groupe libre G, alors $rang(H) \leqslant rang(G)$.*

Démonstration. Si le groupe G est de rang fini, le résultat a été démontré en (VI.2.5.1). Supposons G de rang infini. Si H est de rang fini, le résultat est bien clair. Si H est de rang infini, d'après le lemme (VI.2.2), on a $rang(H) = card(H)$ et $rang(G) = card(G)$. Comme $H \subseteq G$, on en déduit que $rang(H) \leqslant rang(G)$. □

Attention. *Comme cela a été mentionné au chapitre III, ce résultat de comparaison entre le rang d'un groupe libre et le rang de ses sous-groupes est faux pour les groupes non abéliens.*

Corollaire VI.2.4. *Si G est un groupe abélien engendré par n éléments, tout sous-groupe H de G admet une partie génératrice ayant au plus n éléments.*

Démonstration. D'après la démonstration du corollaire (VI.2.1), il existe un morphisme surjectif de groupe $f : \mathbb{Z}^n \to G$. L'image réciproque de H par f est un sous-groupe K de $\mathbb{Z}^n$, donc libre de rang $p \leqslant n$. L'image par f d'une base de K est une partie génératrice de H. □

Remarque VI.2.4. Si G est un groupe libre de rang fini, si H et K sont deux sous-groupes tels que $G = H \oplus K$, alors $rang(G) = rang(H) + rang(K)$.

VI.3. Groupes abéliens de torsion

Définition VI.3.1. Un groupe abélien G est dit ***de torsion*** si tout élément de G est d'ordre fini (*i.e.* $\forall x \in G, \exists n \in \mathbb{Z}$ tel que $nx = 0$). Il est dit ***sans torsion*** si tout élément, différent de l'élément neutre, est d'ordre infini (*i.e.* $\forall x \in G, x \neq 0, nx = 0$ implique $n = 0$).

Exemples VI.3.1.

a) $(\mathbb{Z}, +)$ est sans torsion. Plus généralement, un groupe abélien libre est sans torsion.

b) $(\mathbb{Q}, +)$ est sans torsion.

c) Tout groupe fini est de torsion.

d) $(\mathbb{Q}/\mathbb{Z}, +)$ est de torsion.

e) $(\mathbb{C}^*, \times)$ possède des éléments d'ordre infini et des éléments, différents de l'élément neutre, d'ordre fini.

Proposition - Définition VI.3.1. *Soit G un groupe abélien. L'ensemble formé des éléments d'ordre fini de G, est un sous-groupe $T(G)$ de G. C'est le sous-groupe de torsion de G. Si $T(G) \neq G$, le groupe $G/T(G)$ est sans torsion.*

Démonstration. Si G est un groupe sans torsion alors $T(G) = 0$, si G est un groupe de torsion alors $T(G) = G$; dans ces deux cas le résultat est trivial.

Supposons que G soit un groupe tel que $T(G)$ soit distinct de G et de $\{0\}$. Soient x et y deux éléments de $T(G)$; notons p (resp. q) l'ordre de x (resp. y). On a $pq(x-y) = 0$, donc $(x-y) \in T(G)$ et $T(G)$ est un sous-groupe de G. Soit $\overline{x}$ un élément du groupe $G/T(G)$. S'il existe $p \in \mathbb{N}^*$ tel que $p\overline{x} = 0$, on a $px \in T(G)$, *i.e.* il existe $q \in \mathbb{N}^*$ tel que $qpx = 0$, d'où $x \in T(G)$ et $\overline{x} = 0$, d'où $G/T(G)$ est un groupe sans torsion. □

Exercice VI.4. Soient G un groupe abélien et H un sous-groupe de G. Montrer que

a) $T(H) = H \cap T(G)$.

b) $T(G)/T(H)$ *est un sous-groupe de* $T(G/H)$.

Proposition - Définition VI.3.2. *Soient G un groupe abélien et p un nombre premier. L'ensemble $G(p)$, formé des éléments de G dont l'ordre est une puissance de p, est un sous-groupe de G, appelé composante p-primaire de G.* □

Théorème VI.3.1. *Soient G un groupe abélien de torsion et $\mathcal{P}$ l'ensemble des nombres premiers. Alors G est égal à $\bigoplus_{p\in\mathcal{P}} G(p)$.*

Démonstration. Soit x un élément d'ordre n de G. On considère $n = p_1^{r_1} \dots p_k^{r_k}$ la décomposition en facteurs premiers de n et on pose $n_i = n/p_i^{r_i}$, $1 \leqslant i \leqslant k$. Les nombres entiers n_i sont premiers entre eux dans leur ensemble donc, d'après le théorème de Bezout, il existe des nombres entiers $a_1, \dots, a_k$ tels que $\sum_{1\leqslant i\leqslant k} a_i n_i = 1$. On en déduit que

$$x = 1x = a_1(n_1x) + \dots + a_k(n_kx),$$

où, pour $1 \leqslant i \leqslant k$, n_ix est d'ordre $p_i^{r_i}$. Par conséquent,

$$x \in \sum_{1\leqslant i\leqslant k} G(p_i) \subseteq \sum_{\mathcal{P}} G(p),$$

d'où $G \subseteq \sum_{\mathcal{P}} G(p)$. Comme l'inclusion dans l'autre sens est évidente, on a

$$G = \sum_{\mathcal{P}} G(p).$$

Montrons que cette somme est directe. Soit p_0 un élément de $\mathcal{P}$ et soit

$$x \in G(p_0) \cap \sum_{p\neq p_0, p\in\mathcal{P}} G(p).$$

Il existe $\{p_1, \ldots, p_n\} \subset (\mathcal{P} \setminus \{p_0\})$ tel que $x = x_1 + \ldots + x_n$, avec $x_i \in G(p_i)$. Chaque x_i, $1 \leqslant i \leqslant n$, est d'ordre $p_i^{s_i}$ et, puisque les p_i sont premiers et que le groupe G est abélien, x est d'ordre $p_1^{s_1} \ldots p_n^{s_n}$. Mais, puisque $x \in G(p_0)$, il est aussi d'ordre $p_0^{s_0}$, d'où $x = 0$. On a donc

$$G = \bigoplus_{p \in \mathcal{P}} G(p). \qquad \square$$

Exercice VI.5.

1. Montrer que si G est un groupe abélien fini et si p est un nombre premier divisant l'ordre de G, alors $G(p)$ est le p-sous-groupe de Sylow de G.

2. Soit G un groupe abélien fini d'ordre n et soit $n = p_1^{r_1} \ldots p_k^{r_k}$ la décomposition de n en facteurs premiers. Montrer que $G = \bigoplus_{1 \leqslant i \leqslant k} G(p_i)$.

3. En déduire que si G un groupe abélien fini d'ordre n, pour tout diviseur d de n, le groupe G possède un sous-groupe d'ordre d. (On rappelle que ceci est faux pour les groupes non abéliens.)

Proposition VI.3.3. *Soit G un groupe abélien de type fini. Alors,*

(i) *G est de torsion si et seulement si G est fini*

(ii) *G est sans torsion si et seulement si G est libre.*

Démonstration. (i). Il est clair que tout groupe fini est de torsion.

Soit G un groupe abélien de type fini de torsion et soit $\{x_1, \ldots, x_n\}$ une famille génératrice de G. Chaque élément x_i, $1 \leqslant i \leqslant n$, est d'ordre fini p_i. Par conséquent, dans toute écriture d'un élément x quelconque de G, $x = \sum_{1 \leqslant i \leqslant n} n_i x_i$, on peut supposer que $0 \leqslant n_i \leqslant p_i - 1$. On a donc

$$G = \left\{ \sum_{1 \leqslant i \leqslant n} n_i x_i \right\}$$

où les n_i ne prennent qu'un nombre fini de valeurs, par conséquent le groupe G est fini.

(ii). Il est clair qu'un groupe abélien libre est sans torsion.

Soit G un groupe abélien de type fini sans torsion et soit $\{x_1, \ldots, x_s\}$ une famille génératrice de G. On va faire un raisonnement par récurrence sur s.

Si $s = 1$, G est isomorphe à $\mathbb{Z}$ et donc libre de rang 1.

Supposons le résultat vrai pour les groupes engendrés par $r \leqslant s-1$ éléments. Si la famille $\{x_1, \ldots, x_s\}$ est libre, c'est une base et le groupe G est libre. Sinon, considérons une combinaison linéaire nulle liant les générateurs de G,

$$\sum_{1 \leqslant i \leqslant s} n_i x_i = 0.$$

Les coefficients n_i étant dans $\mathbb{Z}$ et le groupe G étant sans torsion, on peut supposer que les n_i sont premiers entre eux dans leur ensemble (sinon, on met en facteur le *pgcd* des n_i et on utilise l'hypothèse que le groupe est sans torsion).

Si l'un des coefficients, par exemple n_k, est égal à 1, on a

$$x_k = \sum_{1 \leqslant i \leqslant s, i \neq k} n_i x_i$$

et le groupe G est engendré par les $s-1$ éléments $(x_i)_{1 \leqslant i \leqslant s, i \neq k}$. Il est donc libre par hypothèse de récurrence.

Si tous les coefficients n_i sont distincts de 1, il existe au moins deux coefficients n_j et n_k tels que $|n_j| > |n_k| > 0$. En faisant la division euclidienne de n_j par n_k, on a $|n_j - qn_k| < |n_k|$. On pose $x'_k = x_k + qx_j$; il est clair que $\{x_1, \ldots, x_j, \ldots, x'_k, \ldots, x_s\}$ est une partie génératrice de G. D'autre part, on a

$$n_1 x_1 + \ldots + (n_j - qn_k)x_j + \ldots + n_k x'_k + \ldots + n_s x_s = 0$$

où les coefficients sont premiers entre eux dans leur ensemble et $|n_j - qn_k| < |n_j|$.

Alors, ou bien $|n_j - qn_k| = 1$ et on est ramené au cas précédent, ou bien $|n_j - qn_k| > 1$ et on réitère le procédé. Comme ce procédé converge vers le *pgcd* des n_i, on arrivera, en un nombre fini d'étapes, à ce que l'un des coefficients soit égal à 1.

Dans tous les cas, on se ramène à une famille génératrice constituée de $(s-1)$ éléments au plus et, par hypothèse de récurrence, le groupe G est libre. □

Attention. *Cette proposition est fausse, en général, pour les groupes non abéliens et pour les groupes abéliens qui ne sont pas de type fini (contre-exemple : $(\mathbb{Q}, +)$).*

VI.4. Structure des groupes abéliens de type fini

Proposition VI.4.1. *Tout groupe abélien G de type fini est somme directe d'un groupe libre de rang fini et d'un groupe fini (qui est son sous-groupe de torsion $T(G)$).*

Démonstration. Il est clair que l'image dans $G/T(G)$ d'une partie génératrice de G est une partie génératrice de $G/T(G)$, il est donc de type fini. On sait, d'après la proposition-définition (VI.3.1), que le groupe $G/T(G)$ est sans torsion, donc, d'après la proposition (VI.3.3), $G/T(G)$ est libre, de rang fini.

D'autre part, la projection canonique $\pi : G \to G/T(G)$ a pour noyau $T(G)$ et, d'après le corollaire (VI.2.1), la remarque (VI.2.2) et l'exercice (VI.2), on a $G \simeq T(G) \oplus G/T(G)$. Il existe donc un sous-groupe libre de rang fini F de G, isomorphe à $G/T(G)$, tel que $G = T(G) \oplus F$.

Supposons qu'on ait $G = H \oplus K$, avec H groupe fini et K groupe libre de rang fini. Puisque H est un sous-groupe fini de G, on a $H \subseteq T(G)$. D'autre part, tout élément $x \neq 0$ de $T(G)$ s'écrit de manière unique $x = h + k$ avec $h \in H$ et $k \in K$. En notant p l'ordre de x, on a $ph + pk = 0$, *i.e.* $ph = -pk$. Mais $H \cap K = \{0\}$, d'où $pk = 0$ et, puisque K est libre, $k = 0$. Par conséquent $H = T(G)$; on en déduit que $K \simeq G/T(G)$. □

La décomposition ci-dessus étant unique, à isomorphisme près, le rang du groupe libre F est parfaitement déterminé, et donc le groupe F aussi (à isomorphisme près). Nous allons maintenant donner une description précise de la partie de torsion comme somme directe de groupes cycliques.

Pour cela, nous allons d'abord établir le résultat fondamental suivant :

Théorème VI.4.1. *Soient G un groupe abélien libre de rang fini n et H un sous-groupe de G. Alors*

(i) *Il existe une base $(e_1, \dots, e_n)$ de G, un entier $q \leqslant n$, une famille d'entiers positifs $a_1, \dots, a_q$ tels que*

a) *a_i divise a_{i+1}, $1 \leqslant i \leqslant q-1$*

b) *$(a_1 e_1, \dots, a_q e_q)$ soit une base de H*

(ii) *Les entiers q, $a_1, \dots, a_q$ vérifiant ces conditions sont uniquement déterminés par la donnée de G et H.*

Démonstration. (i). Si $H = \{0\}$ le résultat est trivial ; on suppose donc $H \neq \{0\}$. Nous allons faire un raisonnement par récurrence sur n.

Si $n = 1$, le groupe G est isomorphe à $\mathbb{Z}$ et le résultat concernant les sous-groupes de $\mathbb{Z}$ est déjà connu.

On suppose le théorème vrai pour les groupes libres de rang inférieur ou égal à $(n-1)$.

Soit $(x_i)_{1 \leqslant i \leqslant n}$ une base de G et $(\pi_i)_{1 \leqslant i \leqslant n}$ les fonctions coordonnées associées à cette base. Rappelons qu'elles sont définies de la manière suivante : tout élément x de G s'écrivant de manière unique $x = \sum_{1 \leqslant i \leqslant n} n_i x_i$, on pose $\pi_i(x) = n_i$.

Pour tout $u \in Hom(G,\mathbb{Z})$, $u(H)$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $\mathbb{Z}\alpha_u$. On a donc un ensemble de nombres entiers positifs ou nuls (α_u). Puisque H est non nul, il existe au moins une fonction coordonnée qui ne s'annule pas sur H, il existe donc des α_u non nuls. On pose

$$a = inf_{\substack{u\in Hom(G,\mathbb{Z})\\ \alpha_u\neq 0}}(\alpha_u)$$

et on note f un élément de $Hom(G,\mathbb{Z})$ correspondant à a, *i.e.* $f(H) = \mathbb{Z}a$. Soit $h \in H$ tel que $f(h) = a$; écrivons $h = \sum_{1\leqslant i\leqslant n} h_i x_i$.

***Lemme* VI.4.1.** *Pour tout i, $1 \leqslant i \leqslant n$, a divise h_i.*

Démonstration. Soit d le *pgcd* de a et h_i ; il existe des entiers r et s tels que

$$d = rh_i + sa = r\pi_i(h) + sf(h) = (r\pi_i + sf)(h).$$

Comme $(r\pi_i + sf) \in Hom(G,\mathbb{Z})$, il existe un α tel que $(r\pi_i + sf)(H) = \mathbb{Z}\alpha$. On a donc $\mathbb{Z}d \subseteq \mathbb{Z}\alpha$. Puisque d divise a, on a $\mathbb{Z}a \subseteq \mathbb{Z}d$. On a donc $\mathbb{Z}a \subseteq \mathbb{Z}\alpha$. On en déduit que α divise a et, par minimalité de a, $\alpha = a$. On a donc $\mathbb{Z}d = \mathbb{Z}a$, d'où a divise d, donc a divise h_i.

Par conséquent, pour tout i, $1 \leqslant i < n$, il existe $g_i \in \mathbb{Z}$ tel que $h_i = ag_i$. On pose $g = \sum_{1\leqslant i\leqslant n} g_i x_i$. On a $h = ag$, donc $f(h) = f(ag) = af(g)$, mais comme $f(h) = a$, on a $f(g) = 1$. Le morphisme $f : G \to \mathbb{Z}$ admet donc une section λ définie par $\lambda(1) = g$. Le groupe $\lambda(\mathbb{Z})$ est isomorphe à $\mathbb{Z}$, donc libre de rang 1. Il s'identifie au sous groupe de G engendré par g, que nous noterons $\langle g\rangle$, qui est donc lui aussi libre de rang 1. On déduit du corollaire (VI.2.1), de la remarque (VI.2.2) et de l'exercice (VI.2) que $G = \langle g\rangle \oplus Ker(f)$. Par conséquent, $Ker(f)$ est un groupe libre de rang $n-1$ et

$$H = (\langle g\rangle \cap H) \oplus (Ker(f) \cap H).$$

De plus, pour tout élément y de H, on a $f(y) = ba$ avec $b \in \mathbb{Z}$, d'où $y = bh + (y - bag)$, et $(y - bag) \in (Ker(f) \cap H)$, puisque $f(g) = 1$. Ceci, et l'unicité de l'écriture de tout élément de H en fonction de la décomposition en somme directe donnée ci-dessus, impliquent que $\langle g\rangle \cap H = \langle h\rangle$. On a donc

$$H = \langle h\rangle \oplus (H \cap Ker(f)).$$

Par hypothèse de récurrence appliquée au groupe $Ker(f)$ et son sous-groupe $Ker(f) \cap H$, il existe

– une base $(e_2, \ldots, e_n)$ de $Ker(f)$,

– un entier $q \geqslant 2$,

– des entiers positifs $a_2, \ldots, a_q$, avec $a_2 \mid a_3 \mid \ldots \mid a_q$,

tels que $(a_2e_2, \ldots, a_qe_q)$ soit une base de $Ker(f) \cap H$.

Posons $a_1 = a$ et $e_1 = g$ (*i.e.* $a_1e_1 = h$). On déduit de ce qui précède que $(a_1e_1, a_2e_2, \ldots, a_qe_q)$ est une base de H.

Montrons que a_1 divise a_2. On considère le morphisme $v : G \to \mathbb{Z}$ défini par $v(e_1) = v(e_2) = 1$ et $v(e_i) = 0$ pour $i \geqslant 3$. Alors, $a = a_1 = v(a_1e_1) = v(h)$ et, puisque $v(H) = \mathbb{Z}\beta$, on a $\mathbb{Z}a \subseteq \mathbb{Z}\beta$. D'où, par minimalité de a, $\mathbb{Z}\beta = \mathbb{Z}a = \mathbb{Z}a_1$. D'autre part, $a_2 = v(a_2e_2) \in v(H) = \mathbb{Z}\beta$, donc $a_2 \in \mathbb{Z}a_1$, *i.e.* a_1 divise a_2.

(ii). Pour démontrer l'unicité des entiers $q, a_1, \ldots, a_q$, nous allons d'abord déduire de (i) un théorème de structure des groupes abéliens de type fini. La démonstration du théorème (VI.4.1.(ii)) sera faite pages 150 et 151. □

Théorème VI.4.2 **(de structure des groupes abéliens de type fini).** *Soit G un groupe abélien de type fini. Il existe un unique entier p et une unique famille $(a_1, \ldots, a_r)$ d'entiers supérieurs ou égaux à 2, avec a_i divise a_{i+1} pour $1 \leqslant i \leqslant r-1$, tels que*

$$G \simeq \mathbb{Z}^p \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_r\mathbb{Z}.$$

Démonstration. Existence : Soit $(x_1, \ldots, x_n)$ une famille génératrice de G. Il existe un morphisme surjectif $f : \mathbb{Z}^n \to G$ tel que $G \simeq \mathbb{Z}^n/ker(f)$. D'après le théorème (VI.4.1), il existe une base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$, un entier q, $1 \leqslant q \leqslant n$, des entiers positifs $a_1, \ldots, a_q$, avec a_i divise a_{i+1} pour $1 \leqslant i \leqslant (q-1)$, tels que $(a_1e_1, \ldots, a_qe_q)$ soit une base de $Ker(f)$. On pose $a_{q+1} = \ldots = a_n = 0$, alors

$$\mathbb{Z}^n/Ker(f) \simeq \bigoplus_{1 \leqslant i \leqslant n} (\mathbb{Z}e_i/\mathbb{Z}a_ie_i).$$

Mais, pour tout i, on a $\mathbb{Z}e_i/\mathbb{Z}a_ie_i \simeq \mathbb{Z}/a_i\mathbb{Z}$ et, si $a_i = 0$, $\mathbb{Z}/a_i\mathbb{Z} = \mathbb{Z}$. D'où, en posant $p = (n-q)$, et en éliminant les a_i éventuellement égaux à 1,

$$G \simeq \mathbb{Z}^p \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_r\mathbb{Z}.$$

Unicité : Supposons qu'il existe deux familles de nombres entiers $(p, a_1, \ldots, a_r)$ et $(q, b_1, \ldots, b_s)$ telles que

$$G \simeq \mathbb{Z}^p \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_r\mathbb{Z}$$

et

$$G \simeq \mathbb{Z}^q \oplus \mathbb{Z}/b_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/b_s\mathbb{Z}.$$

Chacune de ces deux sommes est une décomposition de G en la somme directe d'un groupe libre de rang fini et d'un groupe fini. D'après la proposition (VI.4.1), cette décomposition est unique ; on en déduit que $\mathbb{Z}^p \simeq \mathbb{Z}^q$, *i.e.* $p = q$, et que

$$\bigoplus_{1\leqslant i\leqslant r} \mathbb{Z}/a_i\mathbb{Z} \simeq T(G) \simeq \bigoplus_{1\leqslant i\leqslant s} \mathbb{Z}/b_i\mathbb{Z}.$$

D'après le théorème (VI.3.1) ou l'exercice (VI.5.2), si $|T(G)| = p_1^{t_1} \dots p_k^{t_k}$, on a

$$T(G) = \bigoplus_{1\leqslant i\leqslant k} G(p_i).$$

Supposons que l'unicité de la décomposition en somme directe du théorème (VI.4.2) soit vérifiée pour les groupes $G(p_i)$, $1 \leqslant i \leqslant k$. Montrons que cela entraîne l'unicité de la décomposition pour le groupe $T(G)$.

On a donc

$$\bigoplus_{1\leqslant i\leqslant r} \mathbb{Z}/a_i\mathbb{Z} \simeq T(G) \simeq \bigoplus_{1\leqslant i\leqslant s} \mathbb{Z}/b_i\mathbb{Z}$$

avec $a_1|a_2|\dots|a_r$ et $b_1|b_2|\dots|b_s$.

Notons x_i un générateur de $\mathbb{Z}/a_i\mathbb{Z}$, $1 \leqslant i \leqslant r$. Alors l'ordre de x_i, $o(x_i) = a_i$, divise $|T(G)|$. Donc,

$$a_i = p_1^{w_{i,1}} \dots p_k^{w_{i,k}} \quad \text{avec} \quad 0 \leqslant w_{i,j} \leqslant t_j$$

et

$$t_j = \sum_{1\leqslant i\leqslant r} w_{i,j} \quad \text{avec} \quad w_{i,j} \leqslant w_{i+1,j} \ \text{ car } a_i|a_{i+1}.$$

On en déduit donc que pour tout i, $1 \leqslant i \leqslant r$, on a $\langle x_i\rangle = \bigoplus_{1\leqslant j\leqslant k}\langle x_{i,j}\rangle$, où $o(x_{i,j}) = p_j^{w_{i,j}}$. Par conséquent,

$$T(G) = \bigoplus_{1\leqslant i\leqslant r} \left(\bigoplus_{1\leqslant j\leqslant k} \langle x_{i,j}\rangle \right) = \bigoplus_{1\leqslant j\leqslant k} \left(\bigoplus_{1\leqslant i\leqslant r} \langle x_{i,j}\rangle \right).$$

Comme $|\bigoplus_{1\leqslant i\leqslant r}\langle x_{i,j}\rangle| = p_j^{w_{1,j}+\dots+w_{r,j}} = p_j^{t_j}$, on a

$$\bigoplus_{1\leqslant i\leqslant r} \langle x_{i,j}\rangle = G(p_j)$$

qui, par hypothèse, a une unique décomposition en somme directe de groupes cycliques.

Le même raisonnement, en utilisant l'autre décomposition de $T(G)$ et en notant y_i un générateur de $\mathbb{Z}/b_i\mathbb{Z}$, donne

$$b_i = p_1^{w'_{i,1}} \dots p_k^{w'_{i,k}} \quad \text{avec} \quad 0 \leqslant w'_{i,j} \leqslant t_j$$

et

$$t_j = \sum_{1 \leqslant i \leqslant s} w'_{i,j} \quad \text{et} \quad w'_{i,j} \leqslant w'_{i+1,j} \quad \text{car} \quad b_i | b_{i+1}$$

et

$$T(G) = \bigoplus_{1 \leqslant j \leqslant k} \left(\bigoplus_{1 \leqslant i \leqslant s} \langle y_{i,j} \rangle \right)$$

avec

$$\bigoplus_{1 \leqslant i \leqslant s} \langle y_{i,j} \rangle = G(p_j).$$

On est donc ramené à démontrer l'unicité de la décomposition en somme directe de groupes cycliques pour les p-groupes abéliens de type fini, ce qui sera fait au lemme (VI.4.2) ci-dessous. Mais remarquons tout de suite qu'on déduit de ce lemme (VI.4.2) que $r = s$ et $w_{i,j} = w'_{i,j}$ pour tout i et j, d'où $a_i = b_i$ pour tout i, $1 \leqslant i \leqslant r$.

Lemme VI.4.2. *Soient p un nombre premier et P un p-groupe abélien fini tel que*

$$P \simeq \bigoplus_{1 \leqslant i \leqslant r} \mathbb{Z}/a_i\mathbb{Z} \simeq \bigoplus_{1 \leqslant j \leqslant s} \mathbb{Z}/b_j\mathbb{Z}$$

avec $a_1 | a_2 | \dots | a_r$ et $b_1 | b_2 | \dots | b_s$. Alors, $r = s$ et, pour tout i, $1 \leqslant i \leqslant r$, $a_i = b_i$.

Démonstration. On remarquera qu'on a nécessairement $a_i = p^{\alpha_i}$ et $b_j = p^{\beta_j}$, les relations de divisibilité ci-dessus se traduisant alors par $\alpha_1 \leqslant \dots \leqslant \alpha_r$ et $\beta_1 \leqslant \dots \leqslant \beta_s$, la conclusion se traduit par $r = s$ et $\alpha_i = \beta_i$, pour tout i, $1 \leqslant i < r$.

Écrivons $|P| = p^t$ et faisons un raisonnement par récurrence sur t.

Si $t = 1$, on a $r = s = 1$ et $\alpha_1 = \beta_1 = 1$.

Supposons $t > 1$ et le résultat vrai pour les p-groupes d'ordre p^u pour $u \leqslant (t-1)$. On note H_p le p-sous-groupe de P formé des éléments de P qui sont d'ordre p. Un élément x de H_p s'écrit de manière unique

$$x = \sum_{1 \leqslant i \leqslant r} n_i x_i, \text{ avec } x_i \text{ générateur de } \mathbb{Z}/p^{\alpha_i}\mathbb{Z}, \ 0 \leqslant n_i < p^{\alpha_i}, \ 1 \leqslant i \leqslant r.$$

Puisque $px = 0$, on a $pn_ix_i = 0$, *i.e.* $p^{\alpha_i}|pn_i$, pour tout i, $1 < i \leqslant r$, d'où on a $n_i = m_ip^{(\alpha_i-1)}$. Comme on a $0 \leqslant n_i < p^{\alpha_i}$, on a $0 \leqslant m_i < p$.

Par conséquent, on a $H_p = \sum_{1\leqslant i\leqslant r} m_ix_i$, avec $0 \leqslant m_i < p$. On en déduit que $|H_p| = p^r$.

En utilisant l'autre décomposition de P en somme directe, le même raisonnement donne $|H_p| = p^s$. On en déduit donc que $r = s$.

On considère

$$K_p = \{x \in P \,|\, \exists\, x' \in P,\ x = px'\}.$$

Un élément x de P appartient à K_p si et seulement si x s'écrit $x = \sum_{1\leqslant i\leqslant r} pn_ix_i$. Par conséquent,

$$K_p = \sum_{1\leqslant i\leqslant r} \langle px_i\rangle$$

où $\langle px_i\rangle$ désigne le sous-groupe engendré par px_i.

Un générateur x_i appartient à H_p si et seulement si $\alpha_i = 1$. Supposons qu'on ait $\alpha_1 = \ldots = \alpha_h = 1$ et $1 < \alpha_{h+1} \leqslant \ldots \leqslant \alpha_r$. Alors

$$K_p = \bigoplus_{(h+1)\leqslant i\leqslant r} \langle px_i\rangle$$

et $|px_i| = p^{(\alpha_i-1)}$.

En utilisant l'autre décomposition de P en somme directe, on obtient

$$K_p = \bigoplus_{(h'+1)\leqslant j\leqslant r} \langle py_j\rangle$$

et $|py_j| = p^{(\beta_j-1)}$.

Si tous les termes α_i sont égaux à 1, alors $K_p = 0$, d'où $h' = r$ et $\beta_i = 1$ pour tout i, $1 \leqslant i \leqslant r$, d'où le résultat.

Si $h < r$, K_p est un sous-groupe propre de P, donc d'ordre p^u, avec $1 \leqslant u < t$. En appliquant l'hypothèse de récurrence au p-groupe K_p, on obtient $h' = h$ et $\alpha_i = \beta_i$, pour $(h + 1) \leqslant i \leqslant r$. Puisqu'on a $\alpha_i = \beta_i = 1$ pour $1 \leqslant i \leqslant h$, on a donc $\alpha_i = \beta_i$ pour tout i, $1 \leqslant i \leqslant r$, et le lemme est démontré, ce qui achève la démonstration du théorème (VI.4.2). □

Démonstration du théorème (VI.4.1.(ii)). Soit H' le sous-groupe de G de base $(e_i)_{1\leqslant i\leqslant q}$. Il est clair que $H \subseteq H'$. De plus, puisque $a_1|\ldots|a_q$,

$$H' = \{x \in G \mid \exists\lambda \in \mathbb{Z},\ \lambda x \in H\}.$$

Par conséquent, H'/H est le sous-groupe de torsion de G/H. Ceci détermine H', donc son rang q, de manière unique.

D'autre part, on a

$$H'/H \simeq \left(\bigoplus_{1\leqslant i\leqslant q} \mathbb{Z}e_i\right) / \left(\bigoplus_{1\leqslant i\leqslant q} \mathbb{Z}a_i e_i\right) \simeq \bigoplus_{1\leqslant i\leqslant q} (\mathbb{Z}/a_i\mathbb{Z}).$$

On déduit du théorème (VI.4.2) l'unicité des éléments $(a_i)_{1\leqslant i\leqslant q}$. □

La décomposition en somme directe d'un groupe abélien de type fini donnée par le théorème (VI.4.2) s'appelle la ***décomposition canonique***.

Exercice VI.6. Soit G un groupe abélien fini. Montrer qu'il existe un élément x de G dont l'ordre est le *ppcm* des ordres des éléments de G. (On décompose G sous la forme donnée par le théorème (VI.4.2), on note y la classe de 1 dans $\mathbb{Z}/a_r\mathbb{Z}$, et on pose $x = (0, \dots, 0, y)$.)

Définition VI.4.1. Les éléments a_i, $1 \leqslant i \leqslant q$, du théorème (VI.4.1) sont appelés les ***facteurs invariants de H dans G***. Si $H = G$, on dit que ce sont les ***facteurs invariants de G***.

Si G est un groupe abélien fini, (par exemple le sous-groupe de torsion d'un groupe abélien de type fini), notons $p_1^{t_1} \dots p_k^{t_k}$ la décomposition en facteurs premiers de $|G|$. Comme on l'a vu dans la démonstration du théorème (VI.4.2), chaque facteur invariant a_i de G, $1 \leqslant i \leqslant q$, s'écrit

$$a_i = p_1^{w_{i,1}} \dots p_k^{w_{i,k}} \quad \text{avec} \quad 0 \leqslant w_{i,j} \leqslant t_j$$

et

$$t_j = \sum_{1\leqslant i\leqslant q} w_{i,j} \quad \text{avec} \quad w_{i,j} \leqslant w_{i+1,j} \quad \text{car } a_i | a_{i+1}.$$

Les facteurs invariants étant uniquement déterminés, il en est de même des termes $p_i^{w_{i,j}}$.

Définition VI.4.2. Les entiers $d_{i,j} = p_j^{w_{i,j}}$, pour $1 \leqslant i \leqslant q$ et $1 \leqslant j \leqslant k$, sont appelés les ***diviseurs élémentaires*** de G.

Puisque les entiers p_j sont premiers, il est clair que les entiers $d_{i,j}$, pour i fixé et $1 \leqslant j \leqslant k$, sont premiers entre eux deux à deux. On en déduit que, pour tout i, $1 \leqslant i \leqslant q$, on a

$$\mathbb{Z}/a_i\mathbb{Z} \simeq \bigoplus_{1\leqslant j\leqslant k} \mathbb{Z}/d_{i,j}\mathbb{Z}.$$

Définition* VI.4.3.** Soit G un groupe abélien fini. En écrivant les diviseurs élémentaires de G dans l'ordre croissant, chacun d'entre eux étant écrit un nombre de fois égal au nombre de fois où il apparaît dans l'écriture des facteurs invariants de G, on obtient une suite finie de nombres entiers qu'on appelle le ***type de G.

***Remarque* VI.4.1.** Lorsqu'on a le type d'un groupe abélien fini G, le nombre maximum d'occurrences d'un même facteur premier de $|G|$ qui apparaît dans le type donne le nombre de facteurs invariants de G.

Conclusion

Soit G un groupe abélien fini. On détermine ses facteurs invariants (*cf.* TR.VI.C) $(a_i)_{1\leqslant i\leqslant q}$ et on en déduit sa décomposition canonique

$$G \simeq \bigoplus_{1\leqslant i\leqslant q} \mathbb{Z}/a_i\mathbb{Z}.$$

On calcule ses diviseurs élémentaires, qui permettent de déterminer le type $(c_1,\dots,c_s)$, et on a

$$G \simeq \bigoplus_{1\leqslant i\leqslant s} \mathbb{Z}/c_i\mathbb{Z}.$$

De plus, en regroupant dans cette dernière somme directe les termes correspondant à un même facteur premier p de $|G|$, on a la décomposition en somme directe de la composante p-primaire $G(p)$.

Ceci peut se résumer sous forme d'un tableau. Soit G un groupe abélien fini, $|G| = p_1^{t_1}\dots p_k^{t_k}$ la décomposition de son ordre en facteurs premiers, $a_1,\dots,a_q$ ses facteurs invariants, $d_{i,j} = p_j^{w_{i,j}}$ ses diviseurs élémentaires. On écrit

	p_1	p_2	$\cdots$	p_j	$\cdots$	p_k
a_1	$w_{1,1}$	$w_{1,2}$	$\cdots$	$w_{1,j}$	$\cdots$	$w_{1,k}$
a_2	$w_{2,1}$	$w_{2,2}$	$\cdots$	$w_{2,j}$	$\cdots$	$w_{2,k}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_i	$w_{i,1}$	$w_{i,2}$	$\cdots$	$w_{i,j}$	$\cdots$	$w_{i,k}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_q	$w_{q,1}$	$w_{q,2}$	$\cdots$	$w_{q,j}$	$\cdots$	$w_{q,k}$

Les colonnes donnent le type des composantes p-primaires de G. Par exemple la $j^{\text{ème}}$-colonne donne le type de la composante p_j-primaire $G(p_j)$ et on a $w_{1,j} \leqslant w_{2,j} \leqslant \dots \leqslant w_{q,j}$.

Les lignes permettent de reconstituer les facteurs invariants. Par exemple, la $i^{\text{ème}}$-ligne permet de reconstituer le facteur invariant a_i, par $a_i = \prod_{1 \leqslant j \leqslant k} p_j^{w_{i,j}}$.

Pour obtenir le tableau ci-dessus :

- ou bien on connaît les facteurs invariants, il suffit alors d'écrire la décomposition en facteurs premiers de chacun d'eux ;
- ou bien on connaît le type du groupe, et le nombre de lignes du tableau est donné par la remarque (VI.4.1). Le fait que chaque facteur invariant a_i contient une puissance (éventuellement nulle) de chaque nombre premier p_i et que a_i divise a_{i+1} donne une détermination unique des $w_{i,j}$.

Exemples VI.4.1.

a) Soit G un groupe de type $(2, 2, 3, 2^3, 5, 3^2)$. On veut déterminer les facteurs invariants de G et sa décomposition canonique. Le nombre premier qui apparaît le plus grand nombre de fois est $p_1 = 2$ qui apparaît trois fois. Il y a donc trois facteurs invariants. Ce sont :

$$a_1 = 2, \quad a_2 = 2 \times 3 = 6, \quad a_3 = 2^3 \times 3^2 \times 5 = 360.$$

D'où la décomposition canonique

$$G \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/360\mathbb{Z}.$$

b) Soit $G \simeq \mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$. Puisque 20 ne divise pas 30, cette décomposition de G n'est pas la décomposition canonique.

Cherchons les diviseurs élémentaires de G. On a

$$20 = 2^2 \times 5 \quad \text{et} \quad 30 = 2 \times 3 \times 5,$$

et G est de type $(2, 3, 2^2, 5, 5)$. On en déduit la décomposition de G en somme directe de ses composantes p-primaires :

$$G \simeq (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}) \oplus \mathbb{Z}/3\mathbb{Z} \oplus (\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}).$$

Les facteurs invariants sont donc $2 \times 5 = 10$ et $4 \times 3 \times 5 = 60$, et la décomposition canonique de G est

$$G \simeq \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/60\mathbb{Z}.$$

Exercice VI.7. Déterminer le type, les facteurs invariants, les composantes p-primaires du groupe

$$G = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}.$$

This page intentionally left blank

THÈMES DE RÉFLEXION

♣ TR.VI.A. Rang d'un groupe libre

Nous allons, dans cette partie, montrer des résultats concernant les groupes libres non abéliens évoqués dans le chapitre III, et plus particulièrement, la réciproque du théorème (III.1.3) :

Soient X et Y deux ensembles. Si les groupes libres $L(X)$ et $L(Y)$ sont isomorphes, alors les ensembles X et Y sont équipotents.

La raison d'être de cette étude concernant des groupes non abéliens dans le chapitre consacré aux groupes abéliens est que, par abélianisation, nous passerons à des groupes abéliens et nous utiliserons alors des résultats concernant les groupes abéliens.

Nous allons, pour la commodité du lecteur, faire quelques rappels de notions étudiées au TR.II.A.

Soit G un groupe ; pour tous x et y éléments de G, on pose $[x, y] = xyx^{-1}y^{-1}$. Cet élément de G est appelé ***commutateur*** de x et y. On remarquera que le groupe G est abélien si et seulement si, pour tous x et y éléments de G, on a $[x, y] = 1$.

On note $D(G)$ le sous-groupe de G *engendré* par les commutateurs $[x, y]$ pour x et y parcourant G et on l'appelle sous-groupe ***dérivé*** de G.

Le sous-groupe $D(G)$ est normal dans G et le groupe $G/D(G)$ est abélien. Si H est un sous-groupe normal de G, le groupe G/H est abélien si et seulement si $D(G) \subseteq H$.

Soient X un ensemble et $L(X)$ le groupe libre de base X (*cf.* chapitre III). On considère le groupe G donné par générateurs et relations :

$$G \simeq \langle X \mid [x, y], x \in X, y \in Y \rangle.$$

1. *Montrer que le groupe G est isomorphe au groupe $L(X)/D(L(X))$.*

On note $\mathbb{Z}^{(X)}$ le groupe abélien libre de base X,

$$j_X : X \hookrightarrow \mathbb{Z}^{(X)} \quad \text{et} \quad i_X : X \hookrightarrow L(X)$$

les inclusions canoniques, $\pi : L(X) \to L(X)/D(L(X))$ la projection canonique.

2. *Montrer qu'il existe un unique morphisme de groupes*

$$\varphi : L(X) \to \mathbb{Z}^{(X)}$$

tel que $\varphi \circ i_x = j_X$. (Propriété universelle du groupe libre (théorème III.1.2).)

3. *En déduire qu'il existe un morphisme de groupes*

$$\psi : L(X)/D(L(X)) \to \mathbb{Z}^{(X)}$$

tel que $\psi \circ \pi = \varphi$. (Théorème de passage au quotient, théorème (II.6.2) ou remarque (II.6.1).)

4. *Montrer qu'il existe un unique morphisme de groupes*

$$\alpha : \mathbb{Z}^{(X)} \to L(X)/D(L(X))$$

tel que $\alpha \circ j_x = \pi \circ i_X$. (Propriété universelle du groupe abélien libre, théorème (VI.2.2).)

5. *Montrer que* ψ *et* α *sont des isomorphismes réciproques l'un de l'autre.*

6. *En déduire que* $\langle X \mid [x, y], x \in X, y \in Y\rangle$ *est une présentation par générateurs et relations du groupe abélien libre de base* X.

Soient X et Y deux ensembles tels que les groupes libres $L(X)$ et $L(Y)$ soient isomorphes.

7. *Montrer que les groupes* $L(X)/D(L(X))$ *et* $L(Y)/D(L(Y))$ *sont isomorphes.*

8. *Déduire de ce qui précède que les groupes abéliens* $\mathbb{Z}^{(X)}$ *et* $\mathbb{Z}^{(Y)}$ *sont isomorphes et que les ensembles* X *et* Y *sont équipotents.*

♠ TR.VI.B. Groupes divisibles

Tous les groupes considérés ici sont abéliens. Leur loi est notée additivement et l'élément neutre est noté 0.

Un groupe abélien G est dit ***divisible*** si, pour tout élément x de G et tout n de $\mathbb{N}^*$, il existe un élément y de G tel que $x = ny$.

Il est clair que le groupe $(\mathbb{Q}, +)$ est divisible et que $(\mathbb{Z}, +)$ ne l'est pas.

Nous allons d'abord étudier quelques propriétés des sous-groupes divisibles d'un groupe, puis nous établirons un théorème de structure des groupes divisibles.

1. *Soit G un groupe ; montrer que les sous-groupes divisibles de G engendrent un sous-groupe divisible maximal.*

2. *Montrer que tout sous-groupe divisible D d'un groupe G est en facteur direct dans G.* (On utilisera le lemme de Zorn (*cf.* appendice) pour montrer qu'il existe un sous-groupe maximal H de G tel que $H \cap D = \{0\}$.)

Un groupe est dit ***réduit*** s'il ne possède par de sous-groupe divisible différent de $\{0\}$.

3. *Montrer que tout groupe G s'écrit $G = D \oplus R$, où D est un groupe divisible et R est un groupe réduit.*

4. *Montrer que tout facteur direct d'un groupe divisible est un groupe divisible.*

On sait que tout groupe abélien G est somme directe d'un groupe sans torsion et de son sous-groupe de torsion. Compte tenu de ce qui précède, pour étudier la structure des groupes divisibles, il suffit d'étudier les groupes divisibles sans torsion et les groupes divisibles de torsion.

Comme, de plus, un groupe de torsion est somme directe de ses composantes p-primaires, pour étudier les groupes divisibles de torsion, il suffit d'étudier les p-groupes divisibles.

Étude des groupes divisibles sans torsion

On remarquera que si G est un groupe sans torsion, si $nx = ny$, où $n \in \mathbb{N}^*$ et $x, y \in G$, alors $x = y$.

On considère un groupe G divisible et sans torsion.

5. *Montrer que pour tout élément $x \neq 0$ de G, il existe un unique morphisme injectif de groupes $f : \mathbb{Q} \to G$ tel que $f(1) = x$.*

6. *Déduire de ce qui précède que G est isomorphe à une somme directe de groupes qui sont tous isomorphes à $\mathbb{Q}$.*

Étude des p-groupes divisibles

On note $\mathbb{Q}/\mathbb{Z}(p)$ le groupe des nombres rationnels r, avec $0 \leqslant r < 1$, qui s'écrivent $r = k/p^n$ pour des entiers k et n, la loi étant l'addition modulo 1. (Vérifier que c'est un groupe.)

Un groupe isomorphe au groupe $\mathbb{Q}/\mathbb{Z}(p)$ est appelé un p^∞***-groupe***.

Par exemple, le quotient par $\mathbb{Z}$ du groupe

$$\{(r/s)\,|\,r\in\mathbb{Z},\ s\in\mathbb{Z},\ (r,s)=1,\ \exists n\in\mathbb{N}^*,\ s=p^n\}$$

où la loi est l'addition usuelle des rationnels, est un p^∞-groupe. (Le vérifier.)

7. *Montrer que si H est un sous-groupe cyclique d'ordre maximum d'un p-groupe, alors H est facteur direct dans G.*

8. *Montrer que si G est un p-groupe tel que $pG=G$, alors G a un p^∞-sous-groupe.* (L'hypothèse entraîne qu'il existe dans G une suite d'éléments x_i tels que $px_i=x_{i-1}$, avec $px_1=0$, chaque x_i étant d'ordre p^i. On montrera alors que l'application définie par $f(r/p^i)=rx_i$, induit un morphisme injectif de groupes de $\mathbb{Q}/\mathbb{Z}(p)$ dans G.)

9. *Montrer que si G est un groupe qui n'est pas sans torsion, il admet un facteur direct qui est un groupe cyclique d'ordre une puissance d'un nombre premier, ou qui est un p^∞-groupe, pour un certain nombre premier p.*

10. *En déduire que si G est un p-groupe divisible, il est somme directe de p^∞-groupes.*

On déduit donc qu'un groupe abélien divisible G est somme directe de groupes qui sont isomorphes à $\mathbb{Q}$, ou à des p^∞-groupes pour les nombres premiers p correspondant aux composantes p-primaires de G.

♣ TR.VI.C. Calcul des facteurs invariants

Soient G un groupe abélien libre de rang n et H un sous-groupe de G. On va donner ici un algorithme de calcul des facteurs invariants de H dans G (*cf.* (théorème VI.4.1)).

Notons $a_1,\dots,a_q$ ces facteurs invariants. Pour déterminer les a_i, $1\leqslant i\leqslant q$, il suffit de connaître les produits $a_1a_2\dots a_k$ pour tout k, $1\leqslant k\leqslant q$. D'autre part, puisque $a_1|a_2|\dots|a_q$, quels que soient les entiers $1\leqslant j_1<\dots<j_k\leqslant q$, l'élément $a_1\dots a_k$ divise l'élément $a_{j_1}\dots a_{j_k}$.

On fixe un entier k, $1\leqslant k\leqslant q$.

1. *Montrer que, pour toute application k-linéaire alternée f définie sur G à valeurs dans $\mathbb{Z}$ et quels que soient $x_1,\dots,x_k$ éléments de H, le produit $a_1\dots a_k$ divise $f(x_1,\dots,x_k)$.*

2. *Montrer que l'on peut choisir f et $x_1,\dots,x_k$ tels que $a_1\dots a_k=f(x_1,\dots,x_k)$.*

3. *En déduire que $a_1\dots a_k$ est un pgcd d'éléments de $\mathbb{Z}$ qui sont de la forme $f(x_1,\dots,x_k)$, $x_i\in H$, $1\leqslant i\leqslant k$.*

Ces résultats fournissent un algorithme de calcul des facteurs invariants, de la manière suivante.

Soient $y_1, \dots, y_n$ une base quelconque de G et $x_1, \dots, x_p$ un système de générateurs de H. On note A la matrice dont la $j^{\text{ème}}$-colonne est formée des composantes de x_j dans la base $y_1, \dots, y_n$, $1 \leqslant j \leqslant p$.

4. *Montrer que $a_1 \dots a_k$, $1 \leqslant k \leqslant q$, est le pgcd des mineurs d'ordre k de la matrice A.*

Application aux matrices équivalentes

On rappelle que deux matrices A et B à coefficients dans un anneau R sont ***équivalentes*** s'il existe des matrices inversibles U et V à coefficients dans R telles que $B = UAV$.

5. *Soit A une matrice à coefficients dans $\mathbb{Z}$, à n lignes et p colonnes. Montrer qu'il existe des matrices inversibles U et V, à coefficients dans $\mathbb{Z}$, telles que*

$$UAV = \begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

où les a_i sont des nombres entiers positifs tels que $a_1 | a_2 | \dots | a_q$.

Les nombres a_i, $1 \leqslant i \leqslant q$, sont appelés les facteurs invariants de la matrice A.

6. *En déduire que deux matrices A et B à coefficients dans $\mathbb{Z}$ sont équivalentes si et seulement si elles ont même rang et mêmes facteurs invariants.*

This page intentionally left blank

TRAVAUX PRATIQUES

TP.VI.A. Algorithmes de Gauss-Jordan, de Hermite et de Smith

On se propose de passer en revue quelques algorithmes classiques de manipulation des matrices à coefficients dans $\mathbb{Z}$. Les résultats obtenus sont à interpréter dans le cadre de la théorie des groupes abéliens de type fini ou, de manière équivalente, des $\mathbb{Z}$-modules de type fini.

On rappelle pour commencer l'algorithme de Gauss-Jordan, qui s'applique aux matrices à coefficients dans $\mathbb{Q}$, puis on modifie cet algorithme en n'autorisant que des opérations « réversibles » dans $\mathbb{Z}$ et en utilisant notamment la structure *euclidienne* de $\mathbb{Z}$ (c'est-à-dire l'existence d'une division euclidienne des entiers). Cela permet de répondre de manière effective à des problèmes pratiques d'algèbre linéaire (résolution d'équations linéaires, extraction d'une base à partir d'un système générateur, comparaison de sous-espaces vectoriels, recherche d'une base du noyau et de l'image d'une application linéaire donnée) et de voir comment ces méthodes se transposent au cas des $\mathbb{Z}$-modules. Enfin, l'algorithme de Smith est appliqué au calcul des facteurs invariants (voir également TR.VI.C). Cela constitue une preuve algorithmique du théorème de structure des groupes abéliens de type fini.

Algorithme de Gauss-Jordan

On dit qu'une matrice $A' \in \mathrm{M}_{m,n}(\mathbb{Q})$ est sous *forme normale échelonnée par ligne* (abrégé FNEL) si elle s'écrit :

$$A' = \begin{pmatrix} 0 \ldots\ 0\ 1\ * \ldots * & 0\ * \ldots * & 0 & & \\ & 1\ * \ldots * & 0 & & \\ & & 1\ \ldots & & \\ & & & \ldots\ 0\ * & * \\ & & & & 1\ * \ldots * \\ & & & & 0 \\ & & & & \vdots \\ & & & & 0 \end{pmatrix}.$$

Le premier coefficient non nul de chaque ligne est appelé *pivot* ; il est toujours égal à 1.

D'autre part, on rappelle que les *opérations élémentaires sur les lignes* sont de trois types :

- $L_i \leftrightarrow L_j$ (permutation de deux lignes) ;
- $L_i \leftarrow \lambda L_i$ ($\lambda \in \mathbb{Q}^\times$) ;
- $L_i \leftarrow L_i + aL_j$ ($a \in \mathbb{Q}$).

L'algorithme de Gauss-Jordan que vous connaissez bien permet, par opérations élémentaires sur les lignes, de mettre une matrice $A \in \mathrm{M}_{m,n}(\mathbb{Q})$ sous FNEL. Autrement dit, on peut écrire $A' = PA$, où A' est de la forme précédente et $P \in \mathrm{GL}_n(\mathbb{Q})$ est le produit des matrices élémentaires correspondant aux opérations élémentaires appliquées successivement. On trouve ces matrices élémentaires en appliquant à la matrice identité I_n l'opération élémentaire en question : par exemple, $L_i \leftarrow L_i + aL_j$ correspond à la matrice $\mathrm{I}_n + aE_{i,j}$ (où $E_{i,j}$ désigne la matrice dont tous les coefficients sont nuls, à l'exception de celui en position (i,j), qui vaut 1). L'écriture $A = P^{-1}A'$ est-elle unique ? Il y a unicité de la matrice A' (si $A'_1 = QA'_2$, où A'_1 et A'_2 sont sous FNEL et Q est inversible, démontrer que $A'_1 = A'_2$) mais pas de la matrice P (on peut avoir $Q \neq \mathrm{Id}$ dans l'égalité $A'_1 = QA'_2$, même si $A'_1 = A'_2$).

☞ *Quelques commandes* Maple *utiles* :
`Matrix, SubMatrix, IdentityMatrix, Transpose` et `ReducedRowEchelonForm` de la librairie `LinearAlgebra`, la dernière fonction étant l'implémentation de l'algorithme de Gauss-Jordan.

Cet algorithme permet :

1. De résoudre un système d'équations linéaires : soit $A = \begin{pmatrix} -2 & -4 & 2 & -2 \\ -1 & -2 & 3 & 3 \\ 3 & 6 & -3 & 3 \\ 3 & 6 & 3 & 15 \\ 3 & 6 & 0 & 9 \end{pmatrix}$ et $B = \begin{pmatrix} -2 \\ 1 \\ 3 \\ 9 \\ 6 \end{pmatrix}$; résoudre $AX = 0$ et $AX = B$ à l'aide de la commande Maple `ReducedRowEchelonForm`. Comparer avec le résultat de la commande `LinearSolve`.

2. D'extraire d'un système de vecteurs $(C_1, \ldots, C_n)$ de $\mathbb{Q}^m$ une base du sous-espace vectoriel qu'ils engendrent : soit A la matrice dont les colonnes sont les C_i et soit I l'ensemble des indices des colonnes de $A' = \texttt{ReducedRowEchelonForm}(A)$ contenant un pivot. Démontrer que $(C_i)_{i \in I}$ constitue une base de $\mathrm{Vect}(C_1, \ldots, C_n)$.

Si A est la matrice de la première question, qu'obtenez-vous ?

3. De donner une base échelonnée (canonique) d'un sous-espace vectoriel, connaissant un système générateur $C_1, \ldots, C_n$: on applique l'algorithme de Gauss-Jordan à la *transposée* de la matrice A dont les colonnes sont les C_i. Cela revient à effectuer les opérations élémentaires sur les colonnes au lieu des lignes : ainsi $A^t P = {}^t A'$ est sous forme normale échelonnée par colonne.

On suppose que A est toujours la matrice de la première question ; quelle base échelonnée obtenez-vous ? Comparer au résultat obtenu avec le système de vecteurs $C'_1 = \begin{pmatrix} 2 \\ 1 \\ -3 \\ -3 \\ -3 \end{pmatrix}$, $C'_2 = \begin{pmatrix} 2 \\ 5 \\ -3 \\ 9 \\ 3 \end{pmatrix}$, $C'_3 = \begin{pmatrix} -2 \\ 7 \\ 3 \\ 27 \\ 15 \end{pmatrix}$. Qu'en concluez-vous ?

4. Soit $\phi : \mathbb{Q}^n \to \mathbb{Q}^m$ une application linéaire et $A = Mat_{bc,bc}(\phi)$ sa matrice par rapport aux bases canoniques de $\mathbb{Q}^n$ et $\mathbb{Q}^m$; comment interprétez-vous les matrices $A' =$ `ReducedRowEchelonForm`(A) et P ? Même question pour $A'' =$ `Transpose`(`ReducedRowEchelonForm`(`Transpose`(A))) et Q, où $A'' = AQ$.

En supposant que A est la matrice de la première question, déterminer une base de $\operatorname{Ker}\phi$ et $\operatorname{Im}\phi$. On donnera deux méthodes : l'une utilisant la matrice A', l'autre la matrice A''. Comparer avec les résultats obtenus à l'aide des commandes Maple `ColSpace` et `NullSpace`. D'après vous, quels algorithmes se cachent derrière ces dernières commandes ?

Algorithme de Hermite

On dit qu'une matrice $A' \in \mathrm{M}_{m,n}(\mathbb{Z})$ est sous *forme normale de Hermite* (abrégé FNH) si elle s'écrit :

$$A' = \begin{pmatrix} 0 \ldots 0\ p_1 & * \ldots * & + & * \ldots * & + \\ & & p_2 & * \ldots * & + \\ & & & & p_3 \ldots \\ & & & & \ldots\ p_r \\ & & & & \\ & & & & \end{pmatrix} \begin{matrix} + & * & \\ * & \ldots & * \\ 0 & & \\ \vdots & & \\ 0 & & \end{matrix}.$$

Le premier coefficient non nul de chaque ligne est appelé *pivot* ; le pivot $p_i > 0$ de la ligne i se trouve à droite du pivot p_{i-1} ; enfin, dans chaque colonne contenant un pivot p_i, les coefficients (représentés par un symbole $+$) sont positifs ou nuls et strictement inférieurs à p_i.

L'algorithme de Hermite permet de réduire une matrice $A \in \mathrm{M}_{m,n}(\mathbb{Z})$ donnée sous FNH, par des opérations élémentaires sur les lignes. Avec les notations de la première partie, on a $\lambda = -1$ et $a \in \mathbb{Z}$, de sorte que les matrices élémentaires correspondantes sont dans $\mathrm{GL}_m(\mathbb{Z})$.

Tout d'abord, on note $\delta(x) = |x|$, $x \in \mathbb{Z}$, et $\delta_{i_0,j}(A) = \min_{i \geqslant i_0, A_{i,j} \neq 0} \delta(A_{i,j})$ (avec la convention $\delta_{i_0,j}(A) = 0$ si $A_{i,j} = 0$ pout tout $i \geqslant i_0$). Soit $i_0 = 1$ et soit j_0 le plus petit entier tel que $\delta_{i_0,j_0}(A) \neq 0$; on effectue dans l'ordre :

– Étape 1 : Après permutation éventuelle de deux lignes, on se ramène au cas où $\delta_{i_0,j_0}(A) = \delta(A_{i_0,j_0})$.

– Étape 2 : On fait $L_i \leftarrow L_i - q_i L_{i_0}$ pour tout $i > i_0$, où q_i désigne le quotient de la division euclidienne de A_{i,j_0} par A_{i_0,j_0}. Si tous les A_{i,j_0} sont nuls pour $i > i_0$, alors on ajuste le signe de $p_{i_0} = A_{i_0,j_0}$ (par $L_{i_0} \leftarrow (-1)L_{i_0}$ au besoin) et l'on passe à l'étape 3, sinon on recommence l'étape 1 (noter que $\delta_{i_0,j_0}(A)$ a diminué, ce qui assure que l'algorithme ne boucle pas).

– Étape 3 : On s'occupe des $+$ au-dessus du pivot par des opérations $L_i \leftarrow L_i - q_i L_{i_0}$ puis l'on remplace i_0 par $i_0 + 1$ (tant que $i_0 < n$), on actualise le plus petit entier j_0 tel que $\delta_{i_0,j_0}(A) \neq 0$ (si un tel entier n'existe pas, c'est terminé) et on recommence l'étape 1.

Concernant les écritures $A = P^{-1}A'$, où A' est sous FNH et $P \in \mathrm{GL}_m(\mathbb{Z})$, il y a unicité de la matrice A', mais pas de la matrice P (avec les notations de la définition de la FNH, démontrer que si $\begin{pmatrix} p_1 & + & + \\ & p_2 & + \\ & & \ddots \\ & & & p_r \end{pmatrix} = P_r \begin{pmatrix} p'_1 & + & + \\ & p'_2 & + \\ & & \ddots \\ & & & p'_r \end{pmatrix}$, où $P_r \in \mathrm{GL}_r(\mathbb{Z})$, alors $P_r = \mathrm{Id}_r$ et les deux matrices sont égales).

☞ *Quelques commandes* Maple *utiles* :
`iquo` ; les opérations élémentaires sur les lignes sont disponibles *via* les commandes `Swaprow, AddRow` et `MultiplyRow` du module `LinearAlgebra` de la librairie `Student` (faire `with(Student[LinearAlgebra])`) ; `HermiteForm` de la librairie `LinearAlgebra` est l'implémentation de l'algorithme de Hermite.

5. Dérouler l'algorithme sur la matrice $A = \begin{pmatrix} 10 & -5 & 10 \\ -16 & 8 & -6 \\ -2 & 1 & -1 \\ 8 & -4 & 12 \end{pmatrix}$ en effectuant une succession de commandes `Swaprow,AddRow` et `MultiplyRow`. Enfin, tester la commande `HermiteForm`.

6. On demande de déterminer une base du sous-groupe H de $\mathbb{Z}^5$ engendré par les vecteurs colonnes de la matrice $C = \begin{pmatrix} 10 & 10 & -9 & -8 \\ -16 & -6 & 22 & 20 \\ 6 & -1 & -4 & -6 \\ 8 & 12 & -5 & -4 \\ 12 & 8 & -13 & -12 \end{pmatrix}$. Soit I l'ensemble des indices des colonnes de $C' =$ `HermiteForm`(A) contenant un pivot ; démontrer que $(C_i)_{i\in I}$ est un système libre maximal. Est-ce une base de H ? Déterminer enfin une base échelonnée (canonique) de H en utilisant l'algorithme de Hermite appliqué à ${}^tC$.

7. Soit $\phi : \mathbb{Z}^4 \to \mathbb{Z}^5$ le morphisme de groupes abéliens (c'est donc une application $\mathbb{Z}$-linéaire) dont la matrice dans les bases canoniques est C ; donner également une base de $\mathrm{Ker}\,\phi$.

Algorithme de Smith

On dit qu'une matrice $A' \in \mathrm{M}_{m,n}(\mathbb{Z})$ est sous *forme normale de Smith* (abrégé FNS) si elle s'écrit :

$$A' = \begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

où les coefficients diagonaux $d_i > 0$ vérifient $d_i \mid d_{i+1}$ et les autres coefficients sont nuls.

L'algorithme de Smith permet de mettre une matrice $A \in \mathrm{M}_{m,n}(\mathbb{Z})$ donnée sous FNS en un nombre fini d'étapes ; chaque étape est une opération élémentaire sur les lignes *ou les colonnes*. Le voici :

On note $\delta(A)$ la valeur minimale de δ sur les coefficients non nuls de A (par convention, $\delta(0) = 0$). Si $\delta(A) = 0$, c'est terminé, sinon on procède comme suit :

– Étape 1 : On se ramène au cas où $\delta(A) = \delta(A_{1,1})$.

– Étape 2 : S'il existe sur la première ligne un élément $A_{1,j}$ non multiple de $A_{1,1}$, on le remplace par le reste r de sa division euclidienne par $A_{1,1}$ (en opérant sur les colonnes). On refait les étapes 1 et 2 jusqu'à ce que tous les termes de la première ligne soient multiples de $A_{1,1}$ (pourquoi ce moment arrive-t-il ?). On applique alors le même procédé à la première colonne et l'on obtient finalement une matrice dont tous les termes de la première ligne et première colonne sont multiples de $A_{1,1}$. Finalement, par opération élémentaire toujours, on se ramène au cas où $A_{1,j} = A_{i,1} = 0$ pour $i \neq 1$ et $j \neq 1$.

– Étape 3 : On a obtenu une matrice constituée de deux blocs, le coefficient $A_{1,1}$ et un bloc $B \in \mathrm{M}_{m-1,n-1}(\mathbb{Z})$. Si l'un des coefficients de B n'est pas multiple de $A_{1,1}$, on additionne la ligne de ce coefficient à la première, puis l'on remplace l'élément en question (sur la première ligne) par le reste de sa division euclidienne par $m_{1,1}$. On refait alors les étapes 1, 2 et 3. Il arrive un moment où tous les coefficients de B sont multiples de $A_{1,1}$ (pourquoi ?).

– On réapplique alors l'algorithme à B ; etc.

Cela démontre algorithmiquement :

***Théorème* 1.** *Toute matrice A de $\mathrm{M}_{m,n}(\mathbb{Z})$ est équivalente à une matrice A' qui est sous FNS.*

Nous allons voir que ce résultat implique l'existence des facteurs invariants. De l'unicité de ces derniers découle alors l'unicité de la forme normale de Smith (matrice A').

☞ *Commande* Maple *utile* : `SmithForm` de la librairie `LinearAlgebra` est l'implémentation de l'algorithme de Smith.

8. Soit G un groupe abélien libre de rang fini m et H un sous-groupe de G. Soit $(C_1, \ldots, C_n)$ un système de générateurs de H et $\phi : \mathbb{Z}^n \to G$ le morphisme qui envoie (x_j) sur $\sum_{j=1}^n x_j C_j$. On note $A \in \mathrm{M}_{m,n}(\mathbb{Z})$ la matrice de ϕ après choix d'une base (e_i) de G, prenant pour $\mathbb{Z}^n$ la base canonique. Comment déduisez-vous du théorème précédent une base (e'_i) de G telle que $H = \oplus_{i=1}^r d_i e'_i$? En d'autres termes, nous venons de déterminer les facteurs invariants de H dans G et $G/H \simeq \oplus_{i=1}^r \mathbb{Z}/d_i\mathbb{Z} \oplus \mathbb{Z}^{m-r}$.

9. Calculer P, Q et A' en prenant pour A la matrice C de la question 5 et vérifier que $A' = PAQ$. Trouver les facteurs invariants du sous-groupe H de $\mathbb{Z}^5$ engendré par les vecteurs colonnes de C et déterminer la structure du quotient $\mathbb{Z}^5/H$.

10. Soit G le groupe abélien défini par générateurs et relations :

$$G = \langle \{a, b, c\} | 5a + b - 2c, 12a - 6b + 5c \rangle.$$

Déterminer la structure de G.

11. Résoudre l'équation *en entiers* $AX = B$, où A est la matrice C de la question 5 et $B = \begin{pmatrix} 11 \\ -18 \\ 4 \\ 9 \\ 13 \end{pmatrix}$.

TP.VI.B. Courbes elliptiques et groupe de Mordell

Les courbes elliptiques sont des objets mathématiques très riches, à la fois du point de vue théorique (ils interviennent dans la preuve du fameux théorème de Fermat) et des applications pratiques (factorisation des entiers, cryptographie, ...). De plus, ces objets se prêtent aux calculs.

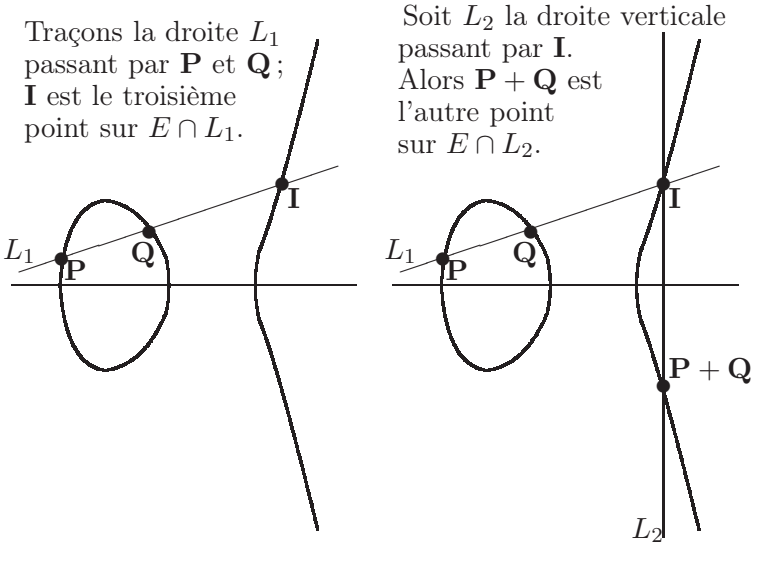
Nous allons, dans ce TP, nous intéresser au groupe de Mordell $E(\mathbb{Q})$ des points rationnels d'une courbe elliptique définie sur $\mathbb{Q}$. C'est un groupe abélien de type fini dont il est aisé de calculer, grâce au théorème de Nagell-Lutz, la partie de

torsion $E(\mathbb{Q})_{tors}$. C'est l'occasion d'illustrer par des exemples (guère accessibles à la main) des énoncés célèbres. Enfin, on s'intéressera au problème des nombres congruents (ce sont les entiers s'interprétant comme l'aire d'un triangle rectangle dont les trois côtés sont rationnels), qui, de manière assez inattendue *a priori*, est relié au calcul du rang du groupe $E(\mathbb{Q})$ pour certaines courbes elliptiques.

La loi de groupe sur une courbe elliptique

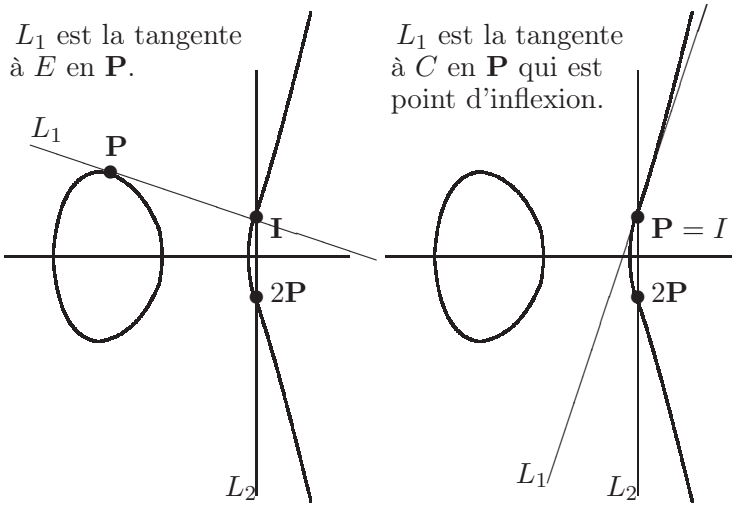
Soit k un corps de caractéristique différente de 2 et 3. Une *courbe elliptique* E définie sur k est une cubique d'équation $y^2 = x^3 + ax + b$[(1)], où le polynôme $x^3 + ax + b \in k[x]$ n'a que des racines simples, *i.e.* est de discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. Pour tout corps K contenant k, on note $E(K)$ l'ensemble des points $P = (x, y)$ dont les coordonnées sont solutions dans K de l'équation E, auquel on rajoute un point, noté O. Ce point est nécessaire afin de munir $E(K)$ d'une loi de groupe, notée $+$ (elle est commutative), dont O sera le neutre. La somme $P + Q$ de deux points est définie géométriquement comme suit :

– *Cas* $P \neq Q$ *:*

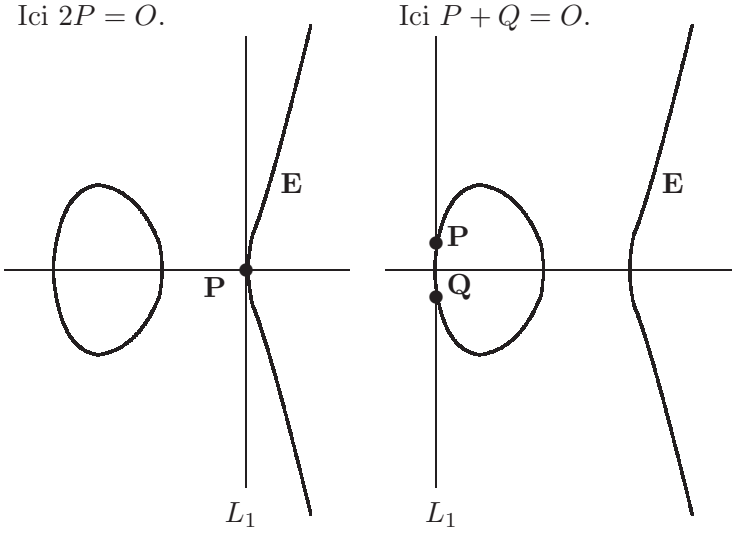


(1) Il existe une définition plus générale, mais nous nous contenterons de celle-ci afin de simplifier l'exposition. En caractéristique 3, on considère des équations du type $y^2 = x^3 + ax^2 + bx + c$. En caractéristique 2, il faut prendre $y^2 + cy = x^3 + ax + b$ ainsi que $y^2 + xy = x^3 + ax^2 + b$.

– *Cas où $P = Q$:*



– *Cas particuliers :*



Remarque. On comprend mieux le sens du point O lorsque l'on considère la courbe comme un objet projectif : O est l'unique « point à l'infini » et une droite verticale passe par O (voir [26], chapitre I, paragraphe 2).

Sauf mention contraire, on suppose que $k = \mathbb{Q}$, *i.e.* E désigne une courbe elliptique définie sur $\mathbb{Q}$.

☞ *Quelques commandes Maple utiles* : `expand, collect, coeff.`

1. Vérifier que l'allure de $E(\mathbb{R})$ correspond à celle des dessins ci-dessus (du moins lorsque x^3+ax+b possède trois racines réelles, sinon il n'y aura qu'une seule composante connexe). Quelle hypothèse permet d'affirmer que la tangente est toujours définie ? Quelles sont les coordonnées de $-P$, où $P=(x,y)$?

Soient P et Q deux points de E qui, s'ils ne coïncident pas avec O, seront de coordonnées respectives (x_1,y_1) et (x_2,y_2). On désire calculer la somme $P+Q$, de coordonnées (x_3,y_3) lorsque $P+Q\neq O$. Pour cela, on note α la pente de la droite (PQ) ou de la tangente en P si $Q=P$. Écrire le polynôme de degré 3 dont les x_i sont les trois racines ; en déduire x_3 à l'aide des relations entre coefficients et racines.

Finalement :

- Cas triviaux : $P+O=P$, $O+Q=Q$, $O+O=O$; on suppose désormais $P\neq O$ et $Q\neq O$.
- Si $x_1\neq x_2$ (*i.e.* $Q\notin\{P,-P\}$) :

$$\begin{cases} x_3=\alpha^2-x_1-x_2\\ y_3=-y_1+\alpha(x_1-x_3)\end{cases}\quad\text{où }\alpha=\frac{y_2-y_1}{x_2-x_1}. \tag{1}$$

- Si $x_1=x_2$ et $y_1\neq -y_2$ (*i.e.* $Q=P$) :

$$\begin{cases} x_3=\alpha^2-2x_1\\ y_3=-y_1+\alpha(x_1-x_3)\end{cases}\quad\text{où }\alpha=\frac{3x_1^2+a}{2y_1}. \tag{2}$$

- Si $x_1=x_2$ et $y_1=-y_2$ (*i.e.* $Q=-P$), alors $P+Q=O$.

2. Afin d'implémenter la loi de groupe, on définit un point P par la liste `P:=[x,y]` de ses coordonnées si $P\neq O$ et l'on représente le point à l'infini O par le symbole `O`. La courbe elliptique E sera définie par le couple `E:=[a,b]`.

Écrire une procédure `appart(E,P)` testant si le point P appartient à E ainsi que deux précédures `somme1(E,P,Q)` et `somme2(E,P)` renvoyant $P+Q$ calculé avec les formules (1) et (2) respectivement. Enfin, écrire une procédure `somme(E,P,Q)` renvoyant `O` si $P+Q=O$ et les coordonnées de $P+Q$ sinon (on prendra soin de traiter tous les cas de figure et de procéder au préalable aux vérifications qui s'imposent).

Tester avec $E : y^2=x^3-36x$, $P=(-3,9)$, $Q=(-2,8)$ et calculer $P+Q$, $2P$ et $2Q$. On doit trouver $(6,0)$, $(\frac{25}{4},\frac{-35}{8})$ et $(\frac{25}{4},\frac{35}{8})$ respectivement. Que remarquez-vous concernant $2P$ et $2Q$?

3. On désire démontrer par le calcul formel l'associativité de la loi de groupe ainsi définie (c'est d'ailleurs la seule vérification non triviale) et se donne donc trois points P, Q et R de E, tous les paramètres étant assimilés à des variables formelles. À l'aide des procédures `somme1` et `somme2` ainsi que de la procédure de simplification suivante (consulter l'aide afin de comprendre son fonctionnement), démontrer le résultat :

```
>simplifier:=proc(expression) local temp,hyp1,hyp2,hyp3;
   hyp1:=P[2]^2=P[1]^3+a*P[1]+b;
   hyp2:=Q[2]^2=Q[1]^3+a*Q[1]+b;
   hyp3:=R[2]^2=R[1]^3+a*R[1]+b;
   temp:=normal(expression,expanded);
   temp:=algsubs(hyp1,temp);
   temp:=algsubs(hyp2,temp);
   temp:=algsubs(hyp3,temp);
   temp:=normal(temp);
   return(temp);
 end:
```

4. Reprenant l'exemple de la fin de la question 2, déterminer les points d'ordre 2 puis 3 dans $E(\mathbb{Q})$, $E(\mathbb{R})$ et $E(\mathbb{C})$. Quelle conjecture faites-vous concernant l'ordre de $P = (-3, 9)$?

Calcul du groupe de Mordell

Le groupe de Mordell d'une courbe elliptique définie sur $\mathbb{Q}$ est le groupe $E(\mathbb{Q})$ de ses points rationnels.

***Théorème 1* (Mordell).** *Le groupe $E(\mathbb{Q})$ est un groupe abélien* de type fini.

On peut donc écrire

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors},$$

où l'entier r est par définition le *rang* de la courbe elliptique et où $E(\mathbb{Q})_{tors}$ désigne le sous-groupe de torsion. Si le calcul du rang est difficile en pratique, la détermination de $E(\mathbb{Q})_{tors}$ est aisée, à l'aide du :

***Théorème 2* (Nagell-Lutz).** *Soit E une courbe elliptique définie sur $\mathbb{Q}$ par une équation $y^2 = x^3 + ax + b$, où a et b sont deux entiers relatifs, et soit $P \neq O$ un point rationnel. Alors $P = (x, y)$ a des coordonnées entières vérifiant ou bien $y = 0$ ou bien $y^2 \mid \Delta = 4a^3 + 27b^2$.*

La preuve se fait en deux temps : on montre qu'un point d'ordre fini a des coordonnées entières, puis on utilise le lemme suivant :

Lemme 1. *Soit $P = (x, y) \in E(\mathbb{Q})$ tel que P et $2P$ sont à coordonnées entières. Alors $y = 0$ ou $y \mid \Delta$.*

Alternativement, le résultat suivant peut s'avérer pertinent dans certains cas :

Proposition 1. *Soit p un nombre premier ne divisant pas 2Δ et $\bar{E}$ la réduction de E modulo p,* i.e. *la courbe elliptique sur $\mathbb{F}_p$ définie par l'équation $y^2 = x^3 + \bar{a}x + \bar{b}$. Alors l'application de réduction $(x, y) \mapsto (\bar{x}, \bar{y})$ définit un* morphisme *de groupes $E(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$ dont la restriction à $E(\mathbb{Q})_{tors}$ est* injective.

En d'autres termes, $E(\mathbb{Q})_{tors}$ s'identifie, *via* le morphisme de réduction, à un sous-groupe de $\bar{E}(\mathbb{F}_p)$; en particulier, Card $E(\mathbb{Q})_{tors}$ divise Card $\bar{E}(\mathbb{F}_p)$.

Enfin, la structure de $E(\mathbb{Q})_{tors}$ n'est pas arbitraire :

***Théorème 3* (Mazur).** *Le groupe de Mordell d'une courbe elliptique définie sur $\mathbb{Q}$ est isomorphe à l'un des groupes abstraits suivants :*

$$\mathbb{Z}/n\mathbb{Z}\,(1 \leqslant n \leqslant 10),\ \mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}\,(1 \leqslant n \leqslant 4).$$

Le lecteur intéressé pourra consulter [26], chapitre II, pour une preuve du théorème de Nagell-Lutz et *loc. cit.* chapitre III pour une preuve du théorème de Mordell. Par contre, la démonstration du théorème de Mazur est hors de portée.

☞ *Quelques commandes Maple utiles* : `type, integer, ifactor, subs`.

5. Écrire des procédures `appartmodp(E,P,p)` et `sommemodp(E,P,Q,p)` qui respectivement vérifient si $P \in \bar{E}(\mathbb{F}_p)$ et renvoient $P + Q$, calculé dans $\bar{E}(\mathbb{F}_p)$ (on modifiera de façon adéquate les programmes de la question 1).

Écrire ensuite une procédure `ordremodp(E,P,p)` qui donne l'ordre de P dans $\bar{E}(\mathbb{F}_p)$. Enfin, sachant que la commande `numtheory[msqrt](y,p)` renvoie un entier x tel que $x^2 \equiv y \mod p$ ou `FAIL` si c'est impossible, écrire une procédure `pointsmodp(E,p)` donnant la liste

```
[N,[[O,1],[[x1,y1],r1],...,[[xn,yn],rn]]]
```

des N éléments de $\bar{E}(\mathbb{F}_p)$, qui sont, outre O (d'ordre 1), les (x_i, y_i), d'ordre r_i.

Tester avec l'exemple de la question 2 et déterminer $\bar{E}(\mathbb{F}_5)$; quelle est la structure de ce groupe fini ?

6. On désire déterminer l'ordre d'un point $P \in E(\mathbb{Q})$ dont les coordonnées (x, y) sont entières : on calcule donc les multiples nP successivement. Si P est d'ordre infini, dire pourquoi on trouvera un point nP n'ayant plus ses coordonnées entières au bout de quelques itérations. Pourquoi est-il suffisant d'aller jusqu'à $n = 12$? En déduire un algorithme de calcul de l'ordre. La procédure `ordre(E,P)` renverra `infinity` si P est d'ordre infini, et l'entier égal à l'ordre de P sinon.

Tester votre procédure sur l'exemple habituel ; on répondra notamment à la conjecture de la question 4.

7. Écrire une procédure `NagellLutz(E)` renvoyant la liste formatée comme suit : `[N,[[O,1],[[x1,y1],r1],...,[[xn,yn],rn]]]` des N éléments de $E(\mathbb{Q})_{tors}$, qui sont, outre O (d'ordre 1), les (x_i, y_i), d'ordre r_i. On pourra utiliser les lignes de commandes suivantes :

```
>candidatsy:=proc(E) local L,r,i,d;
   L:=ifactors(4*E[1]^3+27*E[2]^2); r:=1;
   for d in L[2] do r:=r*d[1]^iquo(d[2],2); od;
   return([O,op(numtheory[divisors](r))]);
 end:

>trouverx:=proc(E,y) local x,sol,L,d;
   sol:={solve(y^2=x^3+E[1]*x+E[2],x)};
   L:=[]; for d in sol do if type(d,integer) then
   L:=[op(L),d]; fi; od;
   return(L);
 end:
```

Ces procédures donnent respectivement la liste `[y1,...,yn]` des entiers naturels y tels que $y = 0$ ou $y^2 \mid \Delta$ et la liste des abscisses entières des points de E d'ordonnée y.

Tester sur l'exemple habituel ; quelle est la structure de $E(\mathbb{Q})_{tors}$?

8. Pour chaque courbe elliptique suivante, déterminer la structure de la partie de torsion du groupe de Mordell. On utilisera deux méthodes : d'une part la réduction de E modulo différents p, d'autre part Nagell-Lutz.

- $E_1 : y^2 = x^3 + 3$;
- $E_2 : y^2 = x^3 + x$;

– $E_3 : y^2 = x^3 - 43x + 166$ (peut-on conclure sans déterminer un point rationnel non-trivial ?).

9. À la vue du théorème de Mazur, suffit-il de connaître $\mathrm{Card}\, E(\mathbb{Q})_{tors}$ pour déterminer la structure de $E(\mathbb{Q})_{tors}$? Donner un critère permettant de trancher les cas indécidables. On désire maintenant fournir un exemple pour chaque cas possible.

La procédure `transf(eq)` ci-dessous transforme une équation longue $eq : y^2 + ay + bxy = x^3 + cx^2 + dx + e$ en une équation courte du type indiqué dans notre définition d'une courbe elliptique. En fait, on applique successivement des transformations affines qui conservent la verticalité. On aurait pu définir de la même manière une loi de groupe sur ces cubiques plus compliquées et les groupes de Mordell des courbes avant et après transformation sont isomorphes.

```
>transf:=proc(eq) local F,a,b,c;
   F:=-lhs(eq)+rhs(eq); a:=coeff(F,y);
   if a<>0 then F:=expand(subs(y=y+a/2,F); fi;
   b:=coeff(coeff(F,x),y);
   if b<>0 then F:=expand(subs(y=y+b*x/2,F)); fi;
   c:=coeff(F,x^2);
   if c<>0 then F:=expand(subs(x=x-c/3,F)); fi;
   return(y^2=sort(subs(y^2=0,F)));
 end:
```

Calculer $E(\mathbb{Q})_{tors}$ dans les cas suivants :

– $E_1 : y^2 + 7xy = x^3 + 16x$;
– $E_2 : y^2 + xy - 5y = x^3 - 5x^2$;
– $E_3 : y^2 - y = x^3 - x^2$;
– $E_4 : y^2 + xy + y = x^3 - x^2 - 14x + 29$;
– $E_5 : y^2 + xy = x^3 - 45x + 81$;
– $E_6 : y^2 + 43xy - 210y = x^3 - 210x^2$;
– $E_7 : y^2 + 5xy - 6y = x^3 - 3x^2$;
– $E_8 : y^2 + 17xy - 120y = x^3 - 60x^2$.

On appliquera une dernière transformation du type $x \rightsquigarrow x/d^2, y \rightsquigarrow y/d^3$ afin de se ramener à une équation à coefficients entiers.

Au final, quels sont les cas du théorème de Mazur qui manquent à l'appel ? En faisant varier les paramètres a et b, trouver des exemples.

Les nombres congruents

Un entier naturel n non nul est « congruent » s'il s'écrit $n = \frac{XY}{2}$ pour un triplet pythagoricien rationnel (X, Y, Z) (*i.e.* $X^2 + Y^2 = Z^2$, où X, Y et Z sont trois nombres rationnels positifs non nuls). Géométriquement, il correspond à l'aire d'un triangle rectangle dont les côtés sont rationnels.

On peut démontrer que les triplets pythagoriciens *primitifs* (*i.e.* X, Y et Z sont entiers et premiers entre eux dans leur ensemble) sont paramétrés par les couples (a, b) d'entiers premiers entre eux tels que $a > b > 0$ et le produit ab est pair : à un tel couple correspond le triplet $(a^2 - b^2, 2ab, a^2 + b^2)$.

Enfin, la proposition suivante établit le lien entre nombres congruents et courbes elliptiques :

Proposition 2. *Les assertions suivantes sont équivalentes :*

(i) $n = \frac{XY}{2}$, *pour un triplet pythagoricien rationnel* (X, Y, Z).

(ii) *La courbe elliptique* E_n *donnée par l'équation* $y^2 = x^3 - n^2x$ *possède un point rationnel distinct des solutions triviales* $(\pm n, 0)$, $(0, 0)$ *(qui correspondent aux points d'ordre 2) et du point à l'infini.*

(iii) *Le rang de la courbe elliptique* E_n *est strictement positif.*

Le lecteur intéressé pourra consulter [15], chapitre I, paragraphes 2 et 9, pour une preuve de ces affirmations.

☞ *Quelques commandes Maple utiles* :
`igcd, even, sort, algsubs, normal.`

10. Démontrer que tout nombre congruent n est de la forme $n = s^2m$, où $s \in \mathbb{Q}^\times$ et m est un nombre congruent correspondant à un triplet pythagoricien primitif. Avec les notations précédentes, faisant varier a et b entre 1 et 10, dresser une liste de nombres congruents.

Remarque. Cela ne permet en rien de déterminer si un nombre donné n est congruent : en effet, on ne sait pas à quel moment un m tel que $n = s^2m$ va apparaître dans la liste. Par exemple, voyez-vous 31 dans la liste précédente ? Nous allons pourtant démontrer qu'il est congruent.

11. Soit n un nombre congruent correspondant à un triplet pythagoricien (X, Y, Z) ; vérifier par le calcul que $(\frac{Z^2}{4}, \frac{(X^2-Y^2)Z}{8})$ est un point rationnel de la courbe elliptique E_n. Réciproquement, soit $P = (x, y)$ un point rationnel de E_n qui n'est pas d'ordre 2 ; vérifier que $(\frac{n^2-x^2}{y}, -2\frac{nx}{y}, \frac{n^2+x^2}{y})$ est un triplet pythagoricien (quitte à ajuster les signes) et que n est congruent.

D'autre part, quelle conjecture faites-vous concernant $E_n(\mathbb{Q})_{tors}$ lorsque n est congruent ? La preuve de cette conjecture est la partie difficile de la proposition 2 (iii).

12. Soit E la courbe elliptique d'équation $y^2 = x^3 - 30^2x$. Exhiber un point rationnel qui ne soit pas de torsion. Réciproquement, vérifier que $(\frac{41^2}{7^2}, \frac{720 \cdot 41}{7^3})$ est un point de la courbe elliptique E_{31} et qu'il est d'ordre infini. En déduire que 31 est congruent et donner même plusieurs triplets pythagoriciens convenables.

This page intentionally left blank

VII

GROUPES RÉSOLUBLES

La notion de groupe résoluble est centrale dans la caractérisation, au moyen de la théorie de Galois, des équations polynomiales qui sont résolubles par radicaux, comme on le verra au chapitre XVI.

VII.1. Suites de composition

***Définitions* VII.1.1.** Soit G un groupe.

a) Une ***suite de composition*** de G est une suite finie de sous-groupes G_i de G, $0 \leqslant i \leqslant n$, telle que

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_{i+1} \lhd G_i \lhd \cdots \lhd G_1 \lhd G_0 = G.$$

(On rappelle que la notation $H \lhd G$ signifie que H est un sous-groupe normal de G.)

b) Les groupes quotients G_i/G_{i+1} sont appelés les ***quotients*** de la suite de composition et n est sa ***longueur*** (n est le nombre de quotients).

c) Si, pour tout i, $0 \leqslant i \leqslant n-1$, on a $G_i \neq G_{i+1}$, on dit que la suite de composition est ***strictement décroissante***.

***Définitions* VII.1.2.** Soient Σ et Σ' deux suites de composition d'un groupe G :

$\Sigma : \{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$

$\Sigma' : \{e\} = K_p \lhd K_{p-1} \lhd \cdots \lhd K_1 \lhd K_0 = G.$

a) On dit que Σ' est un ***raffinement*** de Σ, si $p \geqslant n$ et pour tout i, $0 \leqslant i \leqslant n$, il existe j_i, $0 \leqslant j_i \leqslant p$ tel que $G_i = K_{j_i}$ (autrement dit, la suite Σ est extraite de Σ'). On écrit alors $\Sigma \subseteq \Sigma'$. Si, de plus, il existe j, $0 \leqslant j \leqslant p$, tel que pour tout i, $0 \leqslant i \leqslant n$, $K_j \neq G_i$, on dit que Σ' est un ***raffinement propre*** de Σ. On écrit alors $\Sigma \subset \Sigma'$.

b) On dit que les suites de composition Σ et Σ' sont ***équivalentes*** si $n = p$ et s'il existe une permutation $\sigma \in S_n$ telle que, pour tout i, $0 \leqslant i \leqslant n-1$, les groupes G_i/G_{i+1} et $K_{\sigma(i)}/K_{\sigma(i)+1}$ soient isomorphes. On écrit alors $\Sigma \sim \Sigma'$.

Remarques - Exemples VII.1.1.

a) Tout groupe a une suite de composition $\{e\} \lhd G$.

b) La suite $\{e\} \lhd K \lhd V_4 \lhd A_4 \lhd S_4$ est une suite de composition de S_4 (*cf.* TR.II.B).

c) Une suite extraite d'une suite de composition peut ne pas être une suite de composition (non transitivité des sous-groupes normaux).

Lemme VII.1.1. *Soient H, H', K, K' des sous-groupes d'un groupe G, tels que $H' \lhd H$ et $K' \lhd K$. On a*

(i) $H'(H \cap K') \lhd H'(H \cap K)$, $K'(H' \cap K) \lhd K'(H \cap K)$

(ii) $H'(H \cap K)/H'(H \cap K') \simeq K'(H \cap K)/K'(H' \cap K)$.

Démonstration. L'assertion (i) est évidente. Pour démontrer l'assertion (ii), on montre que chacun des deux groupes est isomorphe au groupe $(H \cap K)/(H \cap K')(H' \cap K)$. Pour cela, on va construire un morphisme surjectif de groupes

$$\varphi : H'(H \cap K) \longrightarrow (H \cap K)/(H \cap K')(H' \cap K)$$

et montrer que $Ker(\varphi) = H'(H \cap K')$, d'où l'isomorphisme cherché. Soient $x \in H'$, $y \in H \cap K$; posons $\varphi(xy) = \overline{y}$, où $\overline{y}$ est la classe de y modulo $(H \cap K')(H' \cap K)$. Montrons que φ est une application : soient $x' \in H'$, $y' \in H \cap K$ tels que $xy = x'y'$. Alors, $x^{-1}x' = yy'^{-1}$ et $yy'^{-1} \in H' \cap K$, d'où $\overline{y} = \overline{y'}$ et $\varphi(xy) = \varphi(x'y')$. Montrons que φ est un morphisme de groupes : soient $x, x' \in H'$, $y, y' \in H \cap K$, on a $xyx'y' = xyx'y^{-1}yy'$ et $yx'y^{-1} \in H'$. D'où, en posant $x_1 = yx'y^{-1}$, on a $\varphi(xyx'y') = \varphi(xx_1yy') = \overline{yy'} = \overline{y}\,\overline{y'} = \varphi(xy)\varphi(x'y')$. Le morphisme φ est surjectif par construction. On a $xy \in Ker(\varphi)$ si et seulement si $y \in (H \cap K')(H' \cap K)$, d'où $Ker(\varphi) = H'(H \cap K')$.

On fait la même démonstration pour le groupe $K'(H \cap K)/K'(H' \cap K)$. □

Théorème VII.1.1. *Soient Σ_1 et Σ_2 deux suites de composition d'un groupe G. Il existe deux suites de composition Σ_1' et Σ_2' telles que*

$$\Sigma_1 \subseteq \Sigma_1', \quad \Sigma_2 \subseteq \Sigma_2', \quad \Sigma_1' \sim \Sigma_2'.$$

Démonstration. Soient

$$\Sigma_1 \ : \ \{e\} = H_n \lhd H_{n-1} \lhd \cdots \lhd H_1 \lhd H_0 = G$$

$$\Sigma_2 \ : \ \{e\} = K_p \lhd K_{p-1} \lhd \cdots \lhd K_1 \lhd K_0 = G.$$

On pose $H_{i,j} = H_i(H_{i-1} \cap K_j)$ et $K_{l,m} = K_l(K_{l-1} \cap H_m)$, $1 \leqslant i \leqslant n$, $1 \leqslant m \leqslant n$, $1 \leqslant j \leqslant p$, $1 \leqslant l \leqslant p$. Puisque $H_i \lhd H_{i-1}$ et $K_l \lhd K_{l-1}$, $H_{i,j}$ et $K_{l,m}$ sont des sous-groupes de G. On considère Σ_1' la suite de sous-groupes de G obtenue en intercalant entre H_i et H_{i-1} les sous-groupes $H_{i,j}$, $1 \leqslant j \leqslant p$. D'après le lemme (VII.1.1.(i)), on a

$$H_i = H_{i,p} \lhd H_{i,p-1} \lhd \cdots \lhd H_{i,j} \lhd H_{i,j-1} \lhd \cdots \lhd H_{i,0} = H_{i-1}$$

et la suite Σ_1' est une suite de composition de G, de longueur np, qui est un raffinement de Σ_1. On procède de la même manière à partir de Σ_2, en intercalant les $K_{l,m}$, pour obtenir une suite de composition Σ_2', de longueur np, qui est un raffinement de Σ_2. D'après le lemme (VII.1.1.(ii)), on a $H_{i,j-1}/H_{i,j} \simeq K_{j,i-1}/K_{j,i}$. On en déduit donc que $\Sigma_1' \sim \Sigma_2'$. □

VII.2. Suites de Jordan-Hölder

Définition VII.2.1. Une suite de composition d'un groupe G est une ***suite de Jordan-Hölder*** si tous les quotients de la suite sont des groupes simples.

Proposition VII.2.1. *Une suite de composition d'un groupe G est une suite de Jordan-Hölder si et seulement si elle est strictement décroissante et n'admet aucun raffinement propre.*

Démonstration. Soit Σ une suite de composition de G,

$$\Sigma \ : \ \{e\} = G_n \lhd \cdots \lhd G_1 \lhd G_0 = G.$$

Le groupe G_i/G_{i+1} est simple si et seulement si $G_i \neq G_{i+1}$ et, pour tout sous-groupe normal N de G_i contenant G_{i+1}, on a $N = G_i$ ou $N = G_{i+1}$. Autrement dit, G_i/G_{i+1} est simple si et seulement si G_{i+1} est un sous-groupe normal maximal de G_i. D'où le résultat. □

Remarques - Exemples VII.2.1.

a) Si Σ et Σ' sont deux suites de composition équivalentes et si Σ est une suite de Jordan-Hölder, il en est de même de Σ'.

b) Un groupe simple G admet une suite de Jordan-Hölder $\{e\} = G_1 \lhd G_0 = G$.

c) La suite $\{e\} \lhd A_3 \lhd S_3$ est de Jordan-Hölder.

d) La suite $\{e\} \lhd K \lhd V_4 \lhd A_4 \lhd S_4$ est de Jordan-Hölder.

Proposition VII.2.2.

(i) *Si un groupe abélien admet une suite de Jordan-Hölder, il est fini.*

(ii) *Un groupe fini (non trivial) admet une suite de Jordan-Hölder.*

Démonstration. (i). Soit G un groupe abélien et

$$\{e\} = G_n \lhd \cdots \lhd G_0 = G$$

une suite de Jordan-Hölder de G. Chaque groupe quotient G_i/G_{i+1} est abélien simple, donc cyclique d'ordre premier p_i (TR.I.B). On en déduit que $|G| = p_0 \dots p_{n-1}$ est fini.

(ii). Soit G un groupe fini (non simple) et $\mathcal{N}_0$ l'ensemble de ses sous-groupes normaux propres. C'est un ensemble non vide fini. Toute suite strictement croissante d'éléments de $\mathcal{N}_0$ est finie, donc $\mathcal{N}_0$ a un élément maximal G_1 et le groupe G/G_1 est simple. Si le groupe G_1 est simple, on a une suite de Jordan-Hölder $\{e\} \lhd G_1 \lhd G$. Sinon, on recommence en considérant l'ensemble $\mathcal{N}_1$ des sous-groupes normaux propres de G_1. Puisque le nombre de sous-groupes de G est fini, en un nombre fini de telles opérations, on a une suite de Jordan-Hölder

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G. \qquad \square$$

Théorème VII.2.1. *Soit G un groupe admettant une suite de Jordan-Hölder.*

(i) *Toute suite de composition strictement décroissante de G admet un raffinement qui est une suite de Jordan-Hölder.*

(ii) *Deux suites de Jordan-Hölder quelconques de G sont équivalentes.*

Démonstration. (i). Notons Σ_0 une suite de Jordan-Hölder donnée de G et soit Σ une suite de composition strictement décroissante de G. D'après le théorème (VII.1.1), Σ_0 et Σ admettent des raffinements équivalents Σ'_0 et Σ'. Mais, d'après la proposition (VII.2.1), $\Sigma'_0 = \Sigma_0$, d'où $\Sigma' \sim \Sigma_0$ et Σ' est une suite de Jordan-Hölder.

(ii). Avec les mêmes notations, si Σ est une suite de Jordan-Hölder, on a $\Sigma' = \Sigma$, d'où $\Sigma \sim \Sigma_0$. $\square$

VII.3. Groupes résolubles

Définition VII.3.1. Un groupe G est ***résoluble*** s'il admet une suite de composition dont les quotients sont des groupes abéliens.

On rappelle que les sous-groupes dérivés $D_i(G)$ d'un groupe G sont définis par $D_0(G) = G$, $D_1(G) = [G, G]$ (sous-groupe engendré par les commutateurs d'éléments de G (*cf.* TR.II.A), $D_{i+1}(G) = D(D_i(G))$. Il est clair que ces sous-groupes forment une suite décroissante et que $D_{i+1}(G) \lhd D_i(G)$.

Proposition VII.3.1. *Le groupe G est résoluble si et seulement s'il existe un entier $n \geqslant 0$ tel que $D_n(G) = \{e\}$.*

Démonstration. Si le groupe G est résoluble, il admet une suite de composition (qu'on peut supposer strictement décroissante)

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

telle que G_i/G_{i+1}, $0 \leqslant i \leqslant n-1$, soient des groupes abéliens. Or, le groupe G_i/G_{i+1} est abélien si et seulement si $D_{i+1}(G) \subset D_i(G_1)$ (TR.II.A). D'où, par récurrence,

$$D_{i+1}(G) \subset D_i(G_1) \subset \cdots \subset D(G_i) \subset G_{i+1}$$

et, en particulier, $D_n(G) \subset G_n = \{e\}$.

Réciproquement, s'il existe $n \geqslant 0$ tel que $D_n(G) = \{e\}$, on a une suite de composition

$$\{e\} = D_n(G) \lhd D_{n-1}(G) \lhd \cdots \lhd D(G) \lhd G.$$

Par construction, chaque quotient $D_i(G)/D_{i+1}(G)$ est abélien ; le groupe G est donc résoluble. □

Exemples VII.3.1.

a) Tout groupe abélien est résoluble.

b) Le groupe S_3 est résoluble, car $\{e\} \lhd A_3 \lhd S_3$ est une suite de composition et $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$, $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$.

c) Le groupe S_4 est résoluble, car $\{e\} \lhd V_4 \lhd A_4 \lhd S_4$ est une suite de composition et $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $A_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$, $S_4/A_4 \simeq \mathbb{Z}/2\mathbb{Z}$.

Théorème VII.3.1. *Soit G un groupe.*

(i) *Si G est résoluble tout sous-groupe de G est résoluble.*

(ii) *Si H est un sous-groupe normal de G, alors G est résoluble si et seulement si H et G/H sont résolubles.*

Démonstration. (i). Soit

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots G_1 \lhd G_0 = G$$

une suite de composition de G dont les quotients sont abéliens et soit H un sous-groupe de G. On pose $H_i = H \cap G_i$: alors,

$$\{e\} = H_n \lhd H_{n-1} \lhd \cdots \lhd H_1 \lhd H_0 = H$$

est une suite de composition de H. On a,

$$H_i/H_{i+1} = (H \cap G_i)/(H \cap G_{i+1}).$$

Ce dernier groupe est, d'après le lemme (VII.1.1.(ii)), isomorphe à $(G_{i+1}(H \cap G_i))/G_{i+1}$ qui est un sous-groupe de G_i/G_{i+1}, donc abélien.

(ii). Soit H un sous-groupe normal de G. Supposons que G soit résoluble. D'après (i), H est résoluble ; montrons que G/H est résoluble. On considère la suite de composition de G/H,

$$\{e\} = H/H = G_nH/H \lhd G_{n-1}H/H \lhd \cdots \lhd G_1H/H \lhd G_0H/H = G/H.$$

On a,

$$(G_iH/H)/(G_{i+1}H/H) \simeq (G_i(G_{i+1}H))/G_{i+1}H$$
$$\simeq G_i/(G_i \cap G_{i+1}H) \simeq (G_i/G_{i+1})/((G_i \cap G_{i+1}H)/G_{i+1})$$

qui est un quotient de G_i/G_{i+1}, donc abélien.

Réciproquement, supposons que H et G/H soient résolubles. On a deux suites de composition

$$\{e\} = H_n \lhd H_{n-1} \lhd \cdots \lhd H_1 \lhd H_0 = H$$
$$\{e\} = G_p/H \lhd G_{p-1}/H \lhd \cdots \lhd G_1/H \lhd G_0/H = G/H$$

dont les groupes quotients sont abéliens. On considère la suite de composition de G,

$$\{e\} = H_n \lhd H_{n-1} \lhd \cdots \lhd H_0 = H = G_p \lhd G_{p-1} \lhd \cdots \lhd G_1 \lhd G_0 = G.$$

Les groupes quotients sont H_i/H_{i+1} ou $G_i/G_{i+1} \simeq (G_i/H)/(G_{i+1}/H)$, qui sont abéliens, donc G est résoluble. □

VII.4. Applications

Proposition VII.4.1. *Les groupes simples résolubles sont les groupes cycliques d'ordre premier.*

Démonstration. Il est clair que les groupes cycliques d'ordre premier sont simples et résolubles. Réciproquement, soit G un groupe simple et résoluble. Puisqu'il est simple, sa seule suite de composition décroissante est $\{e\} \lhd G$ et puisqu'il est résoluble, il est donc abélien. On sait qu'un groupe abélien simple est cyclique d'ordre premier (TR.I.B). □

Corollaire VII.4.1. *Les groupes S_n, pour $n \geqslant 5$, ne sont pas résolubles.*

Démonstration. Soit $n \geqslant 5$ un entier ; si le groupe S_n est résoluble, le groupe A_n l'est aussi, d'après le théorème (VII.3.1.(ii)). Or, on sait que pour $n \geqslant 5$ le groupe A_n est simple (TR.II.B) ; d'après la proposition (VII.4.1) il serait donc cyclique, ce qui est absurde. □

Proposition VII.4.2. *Un groupe fini non trivial est résoluble si et seulement si les quotients de ses suites de Jordan-Hölder sont des groupes cycliques d'ordre premier.*

Démonstration. Soit G un groupe fini non trivial. Il admet des suites de Jordan-Hölder, proposition (VII.2.2.(ii)), qui sont toutes équivalentes, théorème (VII.2.1.(ii)). Supposons que G soit résoluble ; alors, d'après la proposition (VII.3.1), on a $D(G) \neq G$. On peut donc considérer l'ensemble $\mathcal{N}_0$ des sous-groupes normaux de G contenant $D(G)$. Cet ensemble est non vide ($D(G) \in \mathcal{N}_0$), fini, ordonné par inclusion : il admet donc un élément maximal G_1. On a $D(G) \subset G_1$, donc le groupe G/G_1 est abélien (TR.II.A), et il est simple puisque G_1 est maximal. Le groupe G/G_1 est donc cyclique d'ordre premier. Le groupe G_1 est résoluble, comme sous-groupe d'un groupe résoluble : on applique le même procédé que ci-dessus pour construire un sous-groupe normal G_2 de G_1 tel G_1/G_2 soit cyclique d'ordre premier. Puisque G est fini, en réitérant un nombre fini de fois ce procédé, on obtient une suite de composition

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

qui est une suite de Jordan-Hölder dont les quotients sont des groupes cycliques d'ordre premier.

Réciproquement, supposons que le groupe G admette une suite de Jordan-Hölder dont les quotients sont des groupes cycliques d'ordre premier : c'est une suite de composition dont les quotients sont des groupes abéliens, donc G est résoluble. □

Corollaire VII.4.2. *Si p est un nombre premier, tout p-groupe fini est résoluble.*

Démonstration. C'est une conséquence du lemme suivant :

Lemme VII.4.1. *Un groupe G d'ordre p^n, où p est un nombre premier, admet une suite de composition de longueur n, $\{e\} = G_0 \triangleleft \cdots \triangleleft G_n = G$, avec $|G_i| = p^i$.*

Démonstration. On fait un raisonnement par récurrence sur n. Si $n = 1$, c'est évident, puisque G est cyclique d'ordre premier. Supposons le résultat vrai pour $n-1$ et soit G un groupe d'ordre p^n. On sait que G étant un p-groupe, son centre $Z(G)$ n'est pas réduit à $\{e\}$, (exercice IV.4). Le groupe $Z(G)$ est d'ordre p^m, il a donc un sous-groupe H d'ordre p, normal dans G (puisque $H \subset Z(G)$). Le groupe G/H est un p-groupe d'ordre p^{n-1}. Par hypothèse de récurrence, il admet une suite de composition

$$\{e\} = H/H \triangleleft G_1/H \triangleleft \cdots \triangleleft G_n/H = G/H$$

telle que $|G_i/H| = p^{i-1}$. D'où, on a

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

avec $|G_i| = p^i$. □

Deuxième partie

THÉORIE DES CORPS

This page intentionally left blank

VIII

ANNEAUX DE POLYNÔMES

Les anneaux de polynômes sont au cœur de la théorie de Galois. Nous allons, dans ce chapitre, donner les définitions et principales propriétés de ces anneaux, ainsi que quelques critères d'irréductibilité des polynômes. Nous traiterons également des polynômes symétriques.

Bien que les généralités classiques sur les anneaux soient, sans aucun doute, connues par le lecteur, pour être complet nous commencerons par les rappeler sans démonstrations dans les paragraphes 1 à 5. Par contre, le fait que l'anneau $K[X]$, des polynômes à coefficients dans un corps, soit principal est essentiel pour la suite : aussi nous développerons en détail cette notion et établirons ses propriétés.

VIII.1. Définitions - Exemples

Définitions VIII.1.1.

a) Un **anneau** est la donnée d'un ensemble non vide A et de deux lois de composition interne, notées $+$ et $.$ (appelées respectivement addition et multiplication) telles que

(i) $(A, +)$ est un groupe abélien (on notera 0 son élément neutre) ;

(ii) $\forall\,(a,b,c) \in A \times A \times A,\ (a.b).c = a.(b.c)$;

(iii) $\exists\, 1 \in A,\ \forall\, a \in A\ a.1 = 1.a = a$ (élément unité) ;

(iv) $\forall\,(a,b,c) \in A \times A \times A,\ a.(b+c) = a.b + a.c$ et $(b+c).a = b.a + c.a.$

b) Si de plus la propriété suivante est vérifiée :

$$\forall\,(a,b)\in A\times A,\ a.b=b.a,$$

l'anneau A est dit **commutatif**.

c) Un **corps** est un anneau A non réduit à $\{0\}$ tel que $(A\setminus\{0\},.)$ soit un groupe.

***Exemples* VIII.1.1.**

a) L'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition et de la multiplication usuelles, est un anneau commutatif.

b) Les ensembles $\mathbb{Q}$ des nombres rationnels, $\mathbb{R}$ des nombres réels, $\mathbb{C}$ des nombres complexes, munis des opérations usuelles, sont des corps.

c) L'ensemble $M_n(k)$ des matrices (n,n) à coefficients dans un anneau commutatif k, muni de l'addition et de la multiplication des matrices, est un anneau, non commutatif pour $n\geqslant 2$.

d) Soit G un groupe abélien (noté additivement), alors $End(G)$ muni de l'addition et de la composition des morphismes de groupes est un anneau (en général non commutatif).

e) Pour tout entier $n>0$, le groupe abélien $\mathbb{Z}/n\mathbb{Z}$ (*cf.* exemple I.1.2.b)), muni de la multiplication définie par $cl(p)cl(q)=cl(pq)$ est un anneau commutatif, dont l'unité est $cl(1)$.

***Exercice* VIII.1.**

1. Soient X un ensemble et A un anneau. On note $\mathcal{F}(X,A)$ l'ensemble des applications de X dans A. Montrer que $\mathcal{F}(X,A)$ muni des opérations définies par

$$\forall f\in\mathcal{F}(X,A),\ \ \forall g\in\mathcal{F}(X,A),\ \ \forall x\in X,\ \ (f+g)(x)=f(x)+g(x)$$

$$\forall f\in\mathcal{F}(X,A),\ \ \forall g\in\mathcal{F}(X,A),\ \ \forall x\in X,\ \ (fg)(x)=f(x)g(x)$$

est un anneau (commutatif si et seulement si A est commutatif).

2. Soient X un ensemble et $\mathcal{P}(X)$ l'ensemble des parties de X. Pour deux éléments A et B de $\mathcal{P}(X)$ on pose

$$A\Delta B=(A\cap(X\setminus B))\cup(B\cap(X\setminus A)),$$

qu'on appelle **différence symétrique** de A et B. Montrer que $\mathcal{P}(X)$ muni des opérations

$$\forall A \in \mathcal{P}(X),\ \ \forall B \in \mathcal{P}(X),\ \ (A,B) \mapsto A\Delta B$$
$$\forall A \in \mathcal{P}(X),\ \ \forall B \in \mathcal{P}(X),\ \ (A,B) \mapsto A \cap B$$

est un anneau commutatif.

Sauf dans quelques exemples,

TOUS LES ANNEAUX CONSIDÉRÉS DANS CE LIVRE
SONT COMMUTATIFS.

Par conséquent, dans toute la suite nous ne traiterons que le cas des anneaux commutatifs.

Définition VIII.1.2. Un élément a d'un anneau A admet un **inverse** s'il existe un élément b de A tel que $ab = 1$. Un élément a d'un anneau A est **inversible** s'il admet un inverse (qui est alors unique). On note alors a^{-1} son inverse et $\mathbb{U}(A)$ l'ensemble des éléments inversibles de A.

Proposition VIII.1.1. *Soit A un anneau. Alors $\mathbb{U}(A)$, muni de la multiplication induite par celle de A, est un groupe (abélien) dont l'unité de A est l'élément neutre.* □

Exercice VIII.2.

1. Déterminer $\mathbb{U}(\mathbb{R}[X])$.

2. Déterminer $\mathbb{U}(\mathcal{F}(X,A))$, où $\mathcal{F}(X,A)$ est l'anneau défini à l'exercice I.1.1. □

Remarque VIII.1.1. Il est clair qu'un anneau $A \neq \{0\}$ est un corps si et seulement si $\mathbb{U}(A) = A \setminus \{0\}$.

Exercice VIII.3. (¶).

1. Soient K un corps commutatif et G un sous-groupe fini de $K^* = \mathbb{U}(K)$. Montrer que le groupe G est formé de racines de l'unité, (*cf.* XV.1), et qu'il est cyclique. (En notant n le *ppcm* des ordres des éléments de G, on montrera, en utilisant le théorème de structure des groupes abéliens de type fini (*cf.* chapitre VI), qu'il existe un élément x de G d'ordre n et on montrera que $G = \langle x \rangle$).

2. En déduire que si K est un corps fini commutatif à q éléments, le groupe K^* est cyclique d'ordre $(q-1)$.

Dans la question ci-dessus, l'hypothèse corps fini commutatif est redondante puisque tout corps fini est commutatif (*cf.* chapitre XV).

Définition VIII.1.3. Une partie B d'un anneau (resp. corps) A est un **sous-anneau** (resp. **sous-corps**) de A si, munie des lois induites par celles de A, c'est un anneau (resp. corps).

Proposition VIII.1.2. *Une partie B d'un anneau A est un sous-anneau de A si et seulement si les trois conditions suivantes sont vérifiées :*

(i) *B munie de l'addition induite par celle de A est un sous-groupe abélien de $(A, +)$*

(ii) *B contient l'élément unité 1 de A*

(iii) *B est stable pour la multiplication de A.* □

Exercice VIII.4. Montrer que l'ensemble

$$A = \{a + ib \mid a \in \mathbb{Z},\, b \in \mathbb{Z}, \quad i^2 = -1\}$$

est un sous-anneau de $\mathbb{C}$. Déterminer $\mathbb{U}(A)$. (Indication : utiliser le module d'un nombre complexe et le fait que $\mathbb{U}(\mathbb{Z}) = \{1\}$.)

Proposition - Définition VIII.1.3. *Soient A un anneau (resp. corps) et S une partie de A. Le sous-anneau (resp. sous-corps) de A engendré par S est le plus petit sous-anneau (resp. sous-corps) de A contenant S (pour la relation d'ordre induite par l'inclusion). C'est l'intersection des sous-anneaux (resp. sous-corps) de A contenant S.* □

Remarque VIII.1.2. Pour $S = \{0, 1\}$, cela conduit à la notion de sous-corps **premier** étudiée au chapitre IX.

Exercice VIII.5.

1. Déterminer le sous-anneau et le sous-corps de $\mathbb{R}$ engendré par $\sqrt{2}$. Mêmes questions avec $\sqrt[3]{2}$.

2. Soient A un anneau et S une partie de A. Montrer que le sous-anneau de A engendré par S est formé des éléments $\sum_{finie} s_{i_1}^{n_{i_1}} \dots s_{i_k}^{n_{i_k}}$, avec $s_{i_j} \in S$ et $n_{i_j} \in \mathbb{N}$.

VIII.2. Idéaux – Morphismes

L'étude faite au chapitre II montre que, si $\mathcal{R}$ est une relation d'équivalence définie sur un anneau A, l'addition et la multiplication de A induisent sur l'ensemble

$A/\mathcal{R}$ une addition et une multiplication ($\overline{x}+\overline{y}=\overline{x+y}, \overline{x}.\overline{y}=\overline{xy}$) qui munissent $A/\mathcal{R}$ d'une structure d'anneau si et seulement si $\mathcal{R}$ est compatible avec l'addition et la multiplication de A.

D'après (II.2), en notant I la classe de 0 pour la relation $\mathcal{R}$, le groupe abélien $(A/\mathcal{R},+)$ s'identifie au groupe abélien $(A/I,+)$ et la multiplication de A induit une multiplication sur A/I. La relation $\mathcal{R}$ est compatible avec la multiplication de A si et seulement si

$$\forall\, x\in I, \forall\, a\in A,\quad a.x\in I.$$

Ceci conduit à la définition :

Définition VIII.2.1. Une partie I d'un anneau A est un **idéal de** A si I est un sous-groupe abélien de A pour l'addition et si

$$\forall\, x\in I, \forall\, a\in A,\ a.x\in I.$$

Remarques VIII.2.1.

a) Il est clair que A et $\{0\}$ sont des idéaux de A.

b) Il est évident que si I est un idéal d'un anneau A et si $1\in I$, alors $I=A$.

La discussion précédente montre que :

Théorème VIII.2.1. *Soient A un anneau et I un idéal de A. Alors l'addition et la multiplication induites par celles de A sur A/I le munissent d'une structure d'anneau.* □

Proposition - Définition VIII.2.1. *Si I et J sont deux idéaux d'un anneau A, alors*

$I+J=\{x+y \mid x\in I, y\in J\}$ est un idéal de A, appelé somme des idéaux I et J ;

$IJ=\Big\{\sum_{finie} x_l y_l \mid x_l\in I, y_l\in J\Big\}$ est un idéal de A, appelé produit des idéaux I et J.

Si $\{I_l\}_{l\in L}$ est une famille non vide d'idéaux d'un anneau A, alors $\bigcap_{l\in L} I_l$ est un idéal de A. □

Proposition - Définition VIII.2.2. *Soient A un anneau et S une partie de A. On appelle idéal de A* **engendré** *par S le plus petit idéal de A contenant S. C'est l'intersection des idéaux de A contenant S.* □

Proposition VIII.2.3. *Soient A un anneau et S une partie de A. L'idéal de A engendré par S est formé des éléments de A s'écrivant $\sum_{finie} a_i s_i$, $a_i \in A$, $s_i \in S$.* □

Notation : Si la partie S est réduite à un élément, $S = \{a\}$, on note (a) l'idéal engendré par a.

Définition VIII.2.2. Un idéal I d'un anneau A est dit **propre** si $I \neq \{0\}$ et $I \neq A$.

Proposition VIII.2.4. *Un anneau commutatif A est un corps si et seulement s'il ne possède aucun idéal propre.* □

Attention. *Le résultat précédent est faux si l'anneau A est non commutatif.* (Considérer un anneau de matrices.) Plus précisément, un corps ne possède pas d'idéaux propres ; l'hypothèse de commutativité de l'anneau est nécessaire pour démontrer l'implication dans l'autre sens.

Exercice VIII.6. Montrer que les idéaux de l'anneau $\mathbb{Z}$ sont les (n) pour n parcourant $\mathbb{N}$. (On utilisera la division euclidienne dans $\mathbb{Z}$.)

Définition VIII.2.3. Soient A et B deux anneaux (resp. corps). Un **morphisme d'anneaux** (resp. **de corps**) de A dans B est une application $f : A \to B$ vérifiant

$$\forall\, (x,y) \in A \times A, \quad f(x+y) = f(x) + f(y)$$

$$\forall\, (x,y) \in A \times A, \quad f(x.y) = f(x).f(y)$$

$$f(1_A) = 1_B.$$

Un morphisme d'anneaux (resp. corps) $f : A \to B$ est un **isomorphisme** d'anneaux (resp. corps) s'il existe un morphisme d'anneaux (resp. corps) $g : A \to B$ tel que $g \circ f = id_A$ et $f \circ g = id_B$.

Proposition VIII.2.5. *Soient A un anneau et I un idéal de A. La projection canonique $A \to A/I$, qui à un élément de A associe sa classe modulo I, est un morphisme surjectif d'anneaux.* □

Proposition VIII.2.6. *Soit $f : A \to B$ un morphisme d'anneaux.*

(i) *Le noyau de f, $Ker(f) = \{x \in A \mid f(x) = 0\}$, est un idéal de A et l'image de f, $Im(f)$, est un sous-anneau de B.*

(ii) *Si J est un idéal de B, alors $I = f^{-1}(J)$ est un idéal de A.*

(iii) *Le morphisme f est un isomorphisme si et seulement si c'est un morphisme bijectif.* □

Exercice VIII.7.

1. Déterminer tous les morphismes d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}$, de $\mathbb{Q}$ dans $\mathbb{Z}$, de $\mathbb{R}$ dans $\mathbb{Q}$. (On remarquera que la condition $f(1) = 1$ est très contraignante et diminue fortement le nombre de morphismes possibles entre deux anneaux.)

2. Soit $f : A \to B$ un morphisme d'anneaux. Montrer que $f(\mathbb{U}(A)) \subseteq \mathbb{U}(B)$.

3. Montrer qu'un morphisme de corps est toujours injectif.

Théorème VIII.2.2 **(de passage au quotient).**

(i) *Soient A et B deux anneaux, I (resp. J) un idéal de A (resp. B), $\pi : A \to A/I$ (resp. $\pi' : B \to B/J$) la projection canonique. Pour tout morphisme d'anneaux $f : A \to B$ tel que $f(I) \subseteq J$, il existe un unique $\overline{f}$ de A/I dans A/J tel que $\overline{f} \circ \pi = \pi' \circ f$.*

(ii) *Soit $f : A \to B$ un morphisme d'anneaux, alors les anneaux $Im(f)$ et $A/Ker(f)$ sont canoniquement isomorphes.* □

Théorème VIII.2.3. *Soient $f : A \to B$ un morphisme surjectif d'anneaux et $K = Ker(f)$.*

(i) *Il existe une correspondance biunivoque entre les idéaux I de A qui contiennent K et les idéaux de B.*

(ii) *Si $I \subseteq A$ ($K \subseteq I$) et $J \subseteq B$ sont des idéaux qui se correspondent par cette bijection, alors*

$$A/I \simeq B/J \simeq (A/K)/(I/K).$$ □

Remarque VIII.2.2. Si A est un anneau et I un idéal de A, la proposition précédente, appliquée à la projection $A \to A/I$, montre qu'il y a une correspondance biunivoque entre les idéaux de l'anneau A/I et les idéaux de A qui contiennent I.

Exercice VIII.8. Montrer que les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$ correspondent aux nombres entiers positifs qui divisent n.

Les exercices VIII.6 et VIII.8 montrent qu'il y a une relation étroite entre nombres et idéaux. Nous pouvons expliciter maintenant l'interprétation de la divisibilité des nombres en termes d'idéaux.

***Définition* VIII.2.4.** Soient A un anneau, a et b deux éléments de A. On dit que a **divise** b, ou que a est un **diviseur** de b, et on écrit $a|b$, s'il existe un élément $c \in A$ tel que $b = ac$.

Dans cette situation, on considère les ideaux (a) et (b) de A, engendrés par a et b respectivement. Tout élément de (b) s'écrivant xb, avec $x \in A$, s'écrit xac, donc appartient à (a). On en déduit donc que

$$[a|b] \Longrightarrow [(a) \supset (b)] \Longleftrightarrow [b \in (a)].$$

Réciproquement, soient a et b deux éléments d'un anneau commutatif A et (a), (b) les idéaux qu'ils engendrent. Si $(a) \supset (b)$, alors $b \in (a)$, *i.e.* il existe $c \in A$ tel que $b = ac$, *i.e.* a divise b.

On voit donc que la divisibilité des éléments dans un anneau se traduit par l'inclusion des idéaux qu'ils engendrent. On peut remarquer, d'après la définition du produit de deux idéaux, que si I et J sont des idéaux d'un anneau A, on a $I \supset IJ$, ce qui correspond bien à l'idée naturelle que I divise le produit IJ.

On sait que dans l'anneau $\mathbb{Z}$ les nombres premiers jouent un rôle capital, puisque tout nombre entier se décompose de manière unique (à l'ordre près des facteurs) en un produit de nombres premiers. Le parallèle entre divisibilité des éléments et inclusion d'idéaux évoqué ci dessus, nous conduit à introduire la notion d'idéal premier (et d'idéal maximal), qui joue dans les anneaux principaux (et dans des anneaux plus généraux), relativement aux idéaux, un rôle analogue à celui des nombres premiers, relativement aux nombres entiers.

VIII.3. Idéaux maximaux, idéaux premiers

***Définition* VIII.3.1.** Un anneau A non nul est **intègre** si

$$\forall\, a \in A,\ \ \forall\, b \in A,\ \ [ab = 0] \Rightarrow [a = 0 \ \ ou \ \ b = 0].$$

Si l'anneau A n'est pas intègre, des éléments non nuls a et b tels que $ab = 0$ sont appelés des **diviseurs de zéro**.

***Exemple* VIII.3.1.** L'anneau $\mathbb{Z}$ est intègre. Tout corps est intègre. L'anneau $M_2(\mathbb{R})$ n'est pas intègre.

Exercice VIII.9.

1. Soit p un nombre premier. Déterminer tous les diviseurs de zéro de l'anneau $\mathbb{Z}/p^2\mathbb{Z}$.

2. Montrer que pour tout $n \geqslant 2$ et pour tout corps commutatif k, l'anneau $M_n(k)$ n'est pas intègre.

3. Montrer que si X est un ensemble tel que $card(X) > 1$, l'anneau $\mathcal{F}(X, A)$ défini à l'exercice VIII.1.1 n'est pas intègre.

4. Un élément a d'un anneau A est **nilpotent** s'il existe un entier $n > 0$ tel que $a^n = 0$.

a) Montrer que dans $M_n(k)$, $n \geqslant 2$, il existe des éléments nilpotents.

b) Soient a et b des éléments d'un anneau A. Montrer que si ab est nilpotent, alors ba l'est aussi.

c) Montrer que si $ab = ba$ et si a et b sont nilpotents, alors ab et $a + b$ sont nilpotents.

Remarque VIII.3.1. Il est clair qu'un sous-anneau d'un anneau intègre est intègre. Ce n'est pas le cas pour le quotient par un idéal, comme on le voit facilement avec $\mathbb{Z}/4\mathbb{Z}$ par exemple.

On va dégager une notion d'idéal telle que l'intégrité de l'anneau soit conservée par passage au quotient par les idéaux de ce type.

Proposition VIII.3.1. *Soient A un anneau et $\mathfrak{p} \neq A$ un idéal de A. Les assertions suivantes sont équivalentes :*

(i) *L'anneau $A/\mathfrak{p}$ est intègre*

(ii) *Pour tous a et b éléments de A, on a $[ab \in \mathfrak{p}] \Rightarrow [a \in \mathfrak{p}$ ou $b \in \mathfrak{p}]$.* □

Définition VIII.3.2. Soit A un anneau, un idéal de A, distinct de A, est dit **premier** s'il vérifie les assertions de la proposition (VIII.3.1).

Remarque VIII.3.2. L'idéal (0) d'un anneau A est premier si et seulement si A est intègre.

Proposition VIII.3.2. *Soient A un anneau et $\mathfrak{m}$ un idéal propre de A. Les assertions suivantes sont équivalentes :*

(i) *Si I est un idéal de A tel que $\mathfrak{m} \subseteq I \subseteq A$ alors $I = \mathfrak{m}$ ou $I = A$*

(ii) *Si a est un élément de A qui n'appartient pas à $\mathfrak{m}$, l'idéal engendré par $\mathfrak{m} \cup \{a\}$ est égal à A.* □

Définition VIII.3.3. Un idéal propre $\mathfrak{m}$ d'un anneau A, est dit **maximal** s'il vérifie les conditions de la proposition (VIII.3.2).

Proposition VIII.3.3. *Soit A un anneau, un idéal propre $\mathfrak{m}$ de A est maximal si et seulement si l'anneau $A/\mathfrak{m}$ est un corps.* □

Proposition VIII.3.4. *Un idéal maximal est premier.* □

Attention. *La réciproque est fausse.* (Considérer, par exemple, l'idéal engendré par X dans l'anneau de polynômes $\mathbb{Z}[X]$.)

Théorème VIII.3.1. *Soit A un anneau, tout idéal I de A est contenu dans un idéal maximal de A.* □

Exercice VIII.10.

1. Montrer qu'un idéal (p) de $\mathbb{Z}$ est maximal (resp. premier) si et seulement si p est un nombre premier (resp. nul ou premier). (On remarquera donc que dans l'anneau $\mathbb{Z}$ un idéal non nul est maximal si et seulement s'il est premier. Ceci est une propriété générale des anneaux principaux qui sera étudiée au paragraphe 7.)

2. Déduire de ce qui précède que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si c'est un anneau intègre.

Ceci est vrai de façon plus générale pour les anneaux finis, comme le montre la question suivante.

3. Soit A un anneau fini intègre.

a) Montrer que pour tout élément $a \in A$, $a \neq 0$, les applications $\delta_a : x \mapsto xa$ et $\gamma_a : x \mapsto ax$ sont des automorphismes du groupe $(A, +)$.

b) En déduire qu'un anneau fini est un corps si et seulement s'il est intègre.

(On pourra remarquer que, si l'on suppose que A est un ensemble fini muni de deux lois satisfaisant les axiomes définissant un anneau, sauf celui concernant l'existence d'un élément unité, l'assertion a) ci-dessus est encore vraie et qu'elle entraîne l'existence de l'élément unité.)

VIII.4. Produit d'anneaux - Théorème chinois

Soient $\{A_i\}_{i\in I}$ une famille non vide d'anneaux : on note $\prod_{i\in I} A_i$ l'ensemble des éléments $(a_i)_{i\in I}$ où, pour tout $i \in I$, $a_i \in A_i$.

***Proposition - Définition* VIII.4.1.** *L'ensemble* $\prod_{i\in I} A_i$, *muni de l'addition composante par composante et de la multiplication composante par composante, est un anneau dont l'élément neutre (pour l'addition) est la famille formée des éléments neutres des* A_i, $i \in I$, *et l'élément unité est la famille formée des éléments unités des* A_i, $i \in I$. *Cet anneau est appelé le produit des anneaux* A_i, $i \in I$.

Les axiomes d'anneau sont vérifiés pour $\prod_{i\in I} A_i$ car ils sont vérifiés pour chaque composante. □

***Théorème* VIII.4.1 (propriété universelle du produit d'anneaux).**
Soient $\{A_i\}_{i\in I}$ *une famille non vide d'anneaux et* p_i, $i \in I$, *les projections canoniques de* $\prod_{i\in I} A_i$ *sur* A_i, $i \in I$. *Pour tout anneau* B *et tout morphisme d'anneaux* $f_i : B \to A_i$, $i \in I$, *il existe un unique morphisme d'anneaux* $h : B \to \prod_{i\in I} A_i$ *tel que* $p_i \circ h = f_i$, $i \in I$. □

***Définition* VIII.4.1.** Deux idéaux I et J d'un anneau A sont **étrangers** si $I + J = A$.

***Proposition* VIII.4.2.** *Soient* A *un anneau,* I *et* J *deux idéaux de* A.

(i) *L'anneau* $A/(I \cap J)$ *est isomorphe à un sous-anneau de* $A/I \times A/J$.

(ii) *Si les idéaux* I *et* J *sont étrangers, alors :*

$$IJ = I \cap J$$

et

$$\forall a \in A, \forall b \in A, \exists\, x \in A \quad \text{tel que} \quad x \equiv a \ (mod\ I) \text{ et } x \equiv b \ (mod\ J).$$

(iii) *Si les idéaux* I *et* J *sont étrangers, alors les anneaux* A/IJ *et* $A/I \times A/J$ *sont isomorphes.* □

Plus généralement, on a le résultat suivant :

***Théorème* VIII.4.2 (le théorème chinois).** *Soient* A *un anneau et* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *des idéaux de* A *tels que* $\mathfrak{a}_i + \mathfrak{a}_j = A$ *pour tout* $i \neq j$.

(i) *Soient $x_1, \ldots, x_n$ des éléments de A, alors il existe un élément x de A tel que $x \equiv x_i \pmod{\mathfrak{a}_i}$, $i = 1, ..., n$.*

(ii) *Les projections canoniques $\pi_i : A \to A/\mathfrak{a}_i$, $i = 1, \ldots, n$, induisent un isomorphisme d'anneaux*

$$A/\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) \to \prod_{i=1}^{n} (A/\mathfrak{a}_i). \qquad \square$$

Exercice VIII.11.

a) Montrer que si p et q sont des entiers positifs, $p\mathbb{Z} \cap q\mathbb{Z} = pq\mathbb{Z}$ si et seulement si p et q sont premiers entre eux.

Montrer que les anneaux $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et $\mathbb{Z}/pq\mathbb{Z}$ sont isomorphes si et seulement si p et q sont premiers entres eux.

b) Généraliser cette dernière assertion en montrant que les anneaux

$$\mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/p_1 \ldots p_k\mathbb{Z}$$

sont isomorphes si et seulement si les entiers p_i, $1 \leqslant i \leqslant k$, sont premiers entre eux deux à deux.

c) Montrer que pour tout nombre $n \in \mathbb{N}^*$ dont la décomposition en facteurs premiers est $n = p_1^{s_1} \ldots p_k^{s_k}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est canoniquement isomorphe à l'anneau $\mathbb{Z}/p_1^{s_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{s_k}\mathbb{Z}$.

VIII.5. Corps des fractions d'un anneau intègre

Le but de ce paragraphe est d'associer, à tout anneau intègre A, un corps $F(A)$ et un morphisme injectif d'anneaux $A \to F(A)$. Ceci entraîne que tout anneau intègre peut être identifié à un sous-anneau d'un corps. Le corps $F(A)$ est construit à partir de l'anneau A comme $\mathbb{Q}$ est construit à partir de $\mathbb{Z}$. Ce corps s'appelle le **corps des fractions** de l'anneau A.

Soit A un anneau intègre. On pose $S = A \setminus \{0\}$ et on définit sur l'ensemble $A \times S$ une relation d'équivalence par

$$[(a, s)\ \mathcal{R}\ (a', s')] \iff [s'a - sa' = 0]$$

On note a/s la classe d'équivalence du couple (a, s). On définit sur l'ensemble quotient $(A \times S)/\mathcal{R}$ une addition et une multiplication par

$$a/s + a'/s' = (s'a + sa')/ss'$$

$$(a/s)(a'/s') = aa'/ss'$$

où les opérations apparaissant dans les seconds membres sont celles de A.

Théorème VIII.5.1. *Les opérations ci-dessus sont bien définies et munissent l'ensemble quotient $(A \times S)/\mathcal{R}$ d'une structure de corps, qu'on notera $F(A)$. L'application $a \mapsto a/1$ est un morphisme injectif d'anneaux de A dans $F(A)$.* □

Exemples VIII.5.1.

a) Si $A = \mathbb{Z}$, $F(A) = \mathbb{Q}$.

b) Si $A = \mathbb{R}[X]$, $F(A)$ est le corps des fractions rationnelles en X à coefficients dans $\mathbb{R}$. Plus généralement, si A est un anneau intègre, $F(A[X]) = F(A)(X)$, le corps des fractions rationnelles à coefficients dans le corps $F(A)$.

L'exercice ci-dessous montre que le corps des fractions d'un anneau intègre est solution d'un problème universel. Ceci montre l'unicité (à isomorphisme unique près) du corps construit ci-dessus et permet, en particulier, de vérifier si un corps donné est le corps des fractions d'un anneau intègre donné.

Exercice VIII.12. (¶). Soit A un anneau intègre ; montrer qu'un corps K est isomorphe au corps des fractions de A si et seulement s'il existe un morphisme injectif d'anneaux $\varphi : A \longrightarrow K$ et si, pour tout corps L et tout morphisme injectif d'anneaux $\sigma : A \longrightarrow L$, il existe un unique morphisme (injectif) de corps $\psi : K \longrightarrow L$ tel que $\sigma = \psi \circ \varphi$.

VIII.6. Anneaux de polynômes

Soit n un entier strictement positif. On note $\underline{i} = (i_1, \ldots, i_n)$ les éléments de $\mathbb{N}^n$ et, pour deux éléments $\underline{i} = (i_1, \ldots, i_n)$ et $\underline{j} = (j_1, \ldots, j_n)$ de $\mathbb{N}^n$, on pose $\underline{i} + \underline{j} = (i_1 + j_1, \ldots, i_n + j_n)$. On remarquera que l'élément $\underline{0} = (0, \ldots, 0)$ est un élément neutre pour cette loi.

Soit A un anneau commutatif. On note $P_n(A)$ l'ensemble des applications $f : \mathbb{N}^n \to A$ telles que $f(\underline{i}) = 0$ sauf pour un nombre fini de $\underline{i} \in \mathbb{N}^n$. On définit sur $P_n(A)$ deux opérations en posant : quels que soient $f, g \in P_n(A)$

$$\begin{array}{rccc} f+g & : \mathbb{N}^n & \longrightarrow & A \\ & \underline{i} & \mapsto & f(\underline{i}) + g(\underline{i}) \\ h = fg & : \mathbb{N}^n & \longrightarrow & A \\ & \underline{i} & \mapsto & h(\underline{i}) = \sum_{\underline{j}+\underline{k}=\underline{i}} f(\underline{j})g(\underline{k}). \end{array}$$

Exercice VIII.13.

1. Vérifier que ces opérations munissent $P_n(A)$ d'une structure d'anneau commutatif, dont l'élément unité est l'application définie par

$$\begin{cases} \underline{i} \longmapsto 0 & \text{si } \underline{i} \neq \underline{0} \\ \underline{0} \longmapsto 1. \end{cases}$$

2. Montrer que l'application $A \longrightarrow P_n(A)$, définie par $a \longmapsto f_a$, avec $f_a(\underline{0}) = a$ et $f_a(\underline{i}) = 0$ si $\underline{i} \neq \underline{0}$, est un morphisme injectif d'anneaux.

Dans la suite, on identifiera, par ce morphisme, le sous-anneau $\{f_a\}_{a\in A}$ de $P_n(A)$ à l'anneau A.

VIII.6.1. Cas $n = 1$

Les éléments de $\mathbb{N}$ seront notés i (et non pas $\underline{i}$). On note X l'application $\mathbb{N} \to A$ définie par $X(1) = 1$ et $X(i) = 0$ si $i \neq 1$. D'après la définition de la multiplication dans $P_1(A)$, on a

$$X^2(i) = \sum_{j+k=i} X(j)X(k) = \begin{cases} 0 & \text{si } i \neq 2 \\ 1 & \text{si } i = 2 \end{cases}$$

et

$$\forall s \in \mathbb{N}, s \geqslant 1, \qquad X^s(i) = \begin{cases} 0 & \text{si } i \neq s \\ 1 & \text{si } i = s. \end{cases}$$

On pose $X^0 = f_1$, *i.e.* $X^0(i) = 0$ si $i \neq 0$ et $X^0(0) = 1$.

Pour tout élément $a \neq 0 \in A$ et tout entier s de $\mathbb{N}$, l'application aX^s définie par

$$aX^s(i) = \begin{cases} 0 & \text{si } i \neq s \\ a & \text{si } i = s \end{cases}$$

est appelée ***monôme de coefficient*** a ; s est le ***degré*** de aX^s.

Par conséquent, en posant, pour tout $i \in \mathbb{N}$, $f(i) = a_i$, tout élément f de $P_1(A)$ admet une écriture ***unique***

$$f = \sum_{i=0}^{n} a_i X^i,$$

avec $n = sup\{i \in \mathbb{N} \,|\, f(i) \neq 0\}$. On dit que f est un ***polynôme en*** X.

Les a_i sont les ***coefficients*** de f et $a_i = 0$ pour tout i si et seulement si $f = f_0 = 0$.

Si $f \neq 0$, on définit le ***degré*** de f, noté $deg(f)$, comme étant le plus grand entier n tel que, dans l'expression $f = \sum a_i X^i$, a_n soit non nul. Le coefficient a_n est alors appelé le ***coefficient dominant*** de f. Le coefficient a_0 est appelé ***coefficient constant*** de f. Un polynôme non nul de degré n est dit ***unitaire*** si son coefficient dominant est égal à 1.

Si $f = 0$, par convention, on pose $deg(f) = -\infty$.

On note $A[X]$ l'anneau $P_1(A)$. On remarquera que les opérations définies ci-dessus dans $P_n(A)$, correspondent, dans le cas $n = 1$, à l'addition et à la multiplication usuelles des polynômes.

VIII.6.2. Cas $n \geqslant 2$

On considère les n-uples suivants :

$$\underline{i}_1 = (1, 0, \ldots, 0),\ \ldots,\ \underline{i}_j = (0, \ldots, 0, 1, 0, \ldots, 0),\ \ldots,\ \underline{i}_n = (0, \ldots, 0, 1),$$

où dans $i_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ le 1 est à la $j^{\text{ème}}$ place, et on définit $X_k \in P_n(A)$, $1 \leqslant k \leqslant n$, par

$$X_k(\underline{i}) = \begin{cases} 1 & \text{si } \underline{i} = \underline{i}_k \\ 0 & \text{si } \underline{i} \neq \underline{i}_k. \end{cases}$$

On pose X_k^0 égal à l'élément unité de $P_n(A)$, quel que soit k.

Pour tout $a \in A$ et tout $\underline{i} = (i_1, \ldots, i_n)$, d'après la définition de la multiplication dans $P_n(A)$, l'élément $a\, X_1^{i_1} \ldots X_n^{i_n}$ de $P_n(A)$ vérifie

$$a\, X_1^{i_1} \ldots X_n^{i_n}(\underline{j}) = \begin{cases} a & \text{si } \underline{j} = \underline{i} \\ 0 & \text{si } \underline{j} \neq \underline{i} \end{cases}$$

(vérification par récurrence sur $|\underline{i}| = i_1 + \ldots + i_n$). Un tel élément est appelé un ***monôme*** et, s'il n'est pas nul (*i.e.* si $a \neq 0$), son ***degré*** est $|\underline{i}| = i_1 + \ldots + i_n$.

Par conséquent, en posant $f(\underline{i}) = a_{\underline{i}}$, chaque élément de $P_n(A)$ s'écrit alors de façon **unique** sous forme d'une **somme finie** de monômes **distincts**

$$f = \sum_{\underline{i}} a_{\underline{i}}\, X_1^{i_1} \ldots X_n^{i_n},$$

avec $\underline{i} = (i_1, \ldots, i_n)$. Une telle expression est appelée ***polynôme en les*** n ***indéterminées*** $X_1, \ldots, X_n$, les $a_{\underline{i}}$ sont les ***coefficients*** de ce polynôme, a_0 est le ***coefficient constant***. Le ***degré total***, noté $deg(f)$, du polynôme $f \neq 0$ est le sup des $|\underline{i}| = i_1 + \ldots + i_n$ tel que $a_{\underline{i}}$ soit non nul. Par convention, si $f = 0$, on pose $deg(f) = -\infty$.

On note l'anneau $P_n(A)$ sous la forme $A[X_1, \ldots, X_n]$.

Définition VIII.6.1. Un polynôme non nul f est dit ***homogène de degré*** s, si tous ses monômes $a_{\underline{i}} X_1^{i_1} \dots X_n^{i_n}$ non nuls ont même degré $|\underline{i}| = s$. Si $f = 0$, il est homogène de degré $-\infty$.

Proposition VIII.6.1. *Si f et g sont deux polynômes homogènes et si $fg \neq 0$, alors fg est homogène de degré total égal à la somme des degrés de f et g.*

Démonstration. Les polynômes f et g étant homogènes de degré total respectif s et t, ils s'écrivent

$$f = \sum_{\underline{i}} a_{\underline{i}} X_1^{i_1} \dots X_n^{i_n}, \quad i_1 + \dots + i_n = s$$

et

$$g = \sum_{\underline{j}} b_{\underline{j}} X_1^{j_1} \dots X_n^{j_n}, \quad j_1 + \dots + j_n = t.$$

Si fg est non nul, il existe au moins un coefficient non nul

$$c_{\underline{h}} = \sum_{\underline{i}+\underline{j}=\underline{h}} a_{\underline{i}} b_{\underline{j}},$$

et chacune de ces expressions non nulles est coefficient du monôme

$$c_{\underline{h}} X_1^{i_1+j_1} \dots X_n^{i_n+j_n}$$

qui est de degré $i_1 + j_1 + \dots + i_n + j_n = s + t$, d'où le résultat. □

Proposition VIII.6.2. *Un polynôme f de $A[X_1, \dots, X_n]$, de degré total m, s'écrit de façon unique comme une somme $f = f_0 + f_1 + \dots + f_m$, où f_s est soit nul, soit homogène de degré s et où $f_m \neq 0$.*

Démonstration. Pour tout s, $0 \leqslant s \leqslant m$, f_s est la somme de tous les monômes de degré s de f ; s'il n'y en a pas, on pose $f_s = 0$. Puisque f est de degré total m, on a $f_m \neq 0$. □

Corollaire VIII.6.1. *Si f et g sont deux polynômes de $A[X_1, \dots, X_n]$, on a*

$$deg(fg) \leqslant deg(f) + deg(g).$$ □

***Remarque* VIII.6.1.** Si on a $1 \leqslant m < n$, on peut identifier $P_m(A)$ à un sous-anneau de $P_n(A)$, en identifiant $\mathbb{N}^m$ à l'ensemble des éléments de $\mathbb{N}^n$ dont les $(n-m)$ dernières composantes sont nulles. Ceci permet d'identifier

$$A[X_1, \ldots, X_n] \quad \text{et} \quad A[X_1, \ldots, X_m][X_{m+1}, \ldots, X_n].$$

En particulier, en écrivant $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$, une récurrence évidente montre que si une propriété $\mathcal{P}$, vérifiée par un anneau A, est également vérifiée par l'anneau $A[X]$, alors cette propriété $\mathcal{P}$ est aussi vérifiée par l'anneau $A[X_1, \ldots, X_n]$, pour tout $n \geqslant 1$.

***Proposition* VIII.6.3.** *Si l'anneau A est intègre, il en est de même de l'anneau $A[X_1, \ldots, X_n]$ et si f et g sont deux polynômes non nuls, le degré total de fg est la somme des degrés totaux de f et g.* □

Remarque* VIII.6.2.** Si K est un corps, l'anneau $K[X_1, \ldots, X_n]$ est intègre, donc, d'après le théorème (VIII.5.1), il admet un corps de fractions, noté $K(X_1, \ldots, X_n)$, appelé corps des ***fractions rationnelles sur K en n indéterminées.

***Théorème* VIII.6.1 (propriété universelle de $A[X_1, \ldots, X_n]$).** *Soient A et B deux anneaux, $\varphi : A \to B$ un morphisme d'anneaux et $y_1, \ldots, y_n$ des éléments de B. Il existe un unique morphisme d'anneaux $\psi : A[X_1, \ldots, X_n] \to B$ tel que $\psi_{|A} = \varphi$ et $\psi(X_i) = y_i$, $i = 1, \ldots, n$.*

Démonstration. Tout élément f de $A[X_1, \ldots, X_n]$ s'écrit de manière unique comme somme d'un nombre fini de monômes distincts

$$f = \sum_{\underline{i}} a_{\underline{i}}\, X_1^{i_1} \ldots X_n^{i_n}.$$

En posant

$$\psi(f) = \sum_{\underline{i}} \phi(a_{\underline{i}})\, y_1^{i_1} \ldots y_n^{i_n},$$

on obtient une application ψ bien définie qui vérifie $\psi_{|A} = \varphi$ et, pour tout i, $\psi(X_i) = y_i$. Vérifions que ψ est un morphisme d'anneaux.

On a $\psi(1) = \varphi(1) = 1$. D'autre part, soient

$$f = \sum_{\underline{i}} a_{\underline{i}}\, X_1^{i_1} \ldots X_n^{i_n} \quad \text{et} \quad g = \sum_{\underline{j}} b_{\underline{j}}\, X_1^{j_1} \ldots X_n^{j_n},$$

alors

$$f + g = \sum_{\underline{i}} (a_{\underline{i}} + b_{\underline{i}})\, X_1^{i_1} \ldots X_n^{i_n}$$

où $a_{\underline{i}}$ (resp. $b_{\underline{i}}$) est nul si le monôme $X_1^{i_1} \dots X_n^{i_n}$ n'apparaît pas dans f (resp. g), et

$$fg = \sum_{\underline{h}} c_{\underline{h}}\, X_1^{h_1} \dots X_n^{h_n}, \quad c_{\underline{h}} = \sum_{\underline{i}+\underline{j}=\underline{h}} a_{\underline{i}} b_{\underline{j}}.$$

On a donc

$$\psi(f+g) = \sum_{\underline{i}} \varphi(a_{\underline{i}} + b_{\underline{i}})\; y_1^{i_1} \dots y_n^{i_n} =$$

$$\sum_{\underline{i}} \varphi(a_{\underline{i}})\; y_1^{i_1} \dots y_n^{i_n} + \sum_{\underline{i}} \varphi(b_{\underline{i}})\; y_1^{i_1} \dots y_n^{i_n} = \psi(f) + \psi(g).$$

D'autre part,

$$\psi(fg) = \sum_{\underline{h}} \varphi(c_{\underline{h}})\; y_1^{h_1} \dots y_n^{h_n},$$

mais

$$\varphi(c_{\underline{h}}) = \sum_{\underline{i}+\underline{j}=h} \varphi(a_{\underline{i}})\varphi(b_{\underline{j}}),$$

d'où

$$\psi(fg) = \sum_{\underline{h}} \left(\sum_{\underline{i}+\underline{j}=\underline{h}} \varphi(a_{\underline{i}})\varphi(b_{\underline{j}}) \right)\; y_1^{h_1} \dots y_n^{h_n} =$$

$$\left(\sum_{\underline{i}} \varphi(a_{\underline{i}}) y_1^{i_1} \dots y_n^{i_n} \right) \left(\sum_{\underline{j}} \varphi(b_{\underline{j}})\; y_1^{j_1} \dots y_n^{j_n} \right) = \psi(f)\psi(g). \qquad \square$$

Théorème VIII.6.2 **(division euclidienne).** *Soient A un anneau intègre et f, g deux éléments de l'anneau $A[X]$. On suppose que le coefficient dominant de g est un élément inversible de A. Alors, il existe un couple unique $(q, r) \in A[X] \times A[X]$ tel que $f = gq + r$ et $deg(r) < deg(g)$.*

Démonstration. *Existence* : On pose $m = deg(f)$ et $deg(g) = n$. Si $m < n$, le couple $(0, f)$ répond à la question. Si $m = n$, c'est évident. On suppose que $m > n$ et le résultat est vrai pour $m - 1$. On peut écrire $f = bX^m + \dots$ et $g = aX^n + \dots$, alors $af - bX^{(m-n)}g$ est de degré inférieur ou égal à $m - 1$ et, par hypothèse de récurrence, il existe un couple (q_1, r_1), avec $deg(r_1) < deg(g)$, tel que

$$af - bX^{m-n}g = gq_1 + r_1.$$

D'où

$$f = a^{-1}(bX^{m-n} + q_1)g + a^{-1}r_1,$$

ce qui est l'égalité cherchée, avec $q = a^{-1}(bX^{m-n} + q_1)$ et $r = a^{-1}r_1$.

Unicité : Supposons qu'il existe un autre couple (q', r'), avec $deg(r') < deg(g)$, tel que $f = gq' + r'$. Alors $g(q - q') = r' - r$ et, si $r' - r \neq 0$, $deg(q - q') + deg(g) = deg(r' - r)$, ce qui est impossible. D'où $r = r'$, ce qui entraîne $q = q'$. □

VIII.7. Anneaux principaux

Soient K un corps et I un idéal de $K[X]$. Si $I = \{0\}$, alors I est engendré par 0. Supposons $I \neq \{0\}$ et soit P un polynôme non nul appartenant à I et de degré minimal pour cette propriété. Tout polynôme $S \in I$ est tel que $deg(S) \geqslant deg(P)$ et l'on peut faire la division euclidienne $S = PQ + R$. Le polynôme R appartient à I, donc est nul par minimalité du degré de P. Par conséquent, S est un multiple de P, autrement dit, $I = (P)$.

Cette propriété conduit à la notion d'anneau principal.

***Définitions* VIII.7.1.**

a) Soient A un anneau et I un idéal de A. On dit que I est **principal** s'il est engendré par un élément (*i.e.* $\exists\ a \in A$ tel que $I = (a)$).

b) Un anneau A est **principal** s'il est intègre et si tout idéal de A est principal.

La discussion précédente montre le résultat fondamental suivant :

***Théorème* VIII.7.1.** *Si K est un corps, l'anneau de polynômes $K[X]$ est principal.* □

***Remarques importantes* VIII.7.1.**

a) Si l'élément $a \in A$ est inversible, alors $aa^{-1} = 1 \in (a)$ et, d'après la remarque VIII.2.1.b, $(a) = A$.

b) Dans un anneau intègre, $(a) = (a')$ est équivalent à $a' = ua$ avec u élément inversible de A. En effet, si $(a) = (a')$, il existe $u \in A$ et $v \in A$ tels que $a' = ua$ et $a = va'$: on a donc $a' = uva'$, d'où $a'(1 - uv) = 0$ et, puisque l'anneau A est intègre, $uv = 1$. Si $a' = ua$, alors $(a') \subset (a)$. Si u est inversible, on a $a = u^{-1}a'$, d'où $(a) \subset (a')$.

Autrement dit, dans un anneau principal, les générateurs d'un idéal quelconque sont « ***égaux à un élément inversible près*** ».

***Exercice* VIII.14.** Montrer que l'anneau $\mathbb{Z}[X]$ n'est pas principal. (Considérer l'idéal de $\mathbb{Z}[X]$ engendré par 2 et X.)

***Remarque* VIII.7.2.** Une démonstration analogue à celle du théorème VIII.7.1 montre que l'anneau $\mathbb{Z}$ est principal. L'exercice VIII.14 ci-dessus montre que la propriété pour un anneau A d'être principal ne se transmet pas nécessairement à l'anneau de polynômes $A[X]$.

Nous allons montrer que les anneaux principaux satisfont une propriété de « finitude ».

Nous allons d'abord établir un résultat général.

***Théorème* VIII.7.2.** *Soit E un ensemble ordonné ; les assertions suivantes sont équivalentes :*

(i) *Toute famille non vide d'éléments de E admet un élément maximal*

(ii) *Toute suite croissante $(x_n)_{n\geqslant 0}$ d'éléments de E est stationnaire.*

Démonstration. Montrons que (i) implique (ii). Soient $(x_n)_{n\in\mathbb{N}}$ une suite croissante d'éléments de E et x_q un élément maximal de l'ensemble $\{x_n\}_{n\in\mathbb{N}}$. Pour $n \geqslant q$, on a $x_n \geqslant x_q$, d'après la croissance de la suite, d'où $x_n = x_q$ d'après la maximalité de x_q.

Montrons que (ii) implique (i). Supposons qu'il existe une famille non vide F de E sans élément maximal. Alors, pour $x \in F$, l'ensemble des $y \in F$ tels que $y > x$ est non vide. D'après l'axiome du choix (*cf.* appendice), il existe une application $f : F \to F$ telle que, pour tout $x \in F$, $f(x) > x$. En fixant un élément x_0 et en posant $x_1 = f(x_0), \ldots, x_{n+1} = f(x_n)$, on obtient une suite strictement croissante. Elle ne peut donc être stationnaire. □

***Théorème* VIII.7.3.** *Soit A un anneau principal.*

(i) *Toute suite croissante d'idéaux de A est stationnaire.*

(ii) *Toute partie non vide de l'ensemble des idéaux de A, ordonné par inclusion, admet un élément maximal.*

Démonstration. D'après le théorème (VIII.7.2), il suffit de démontrer l'assertion (i). Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A : alors $I = \bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A, d'où il existe $a \in A$ tel que $I = (a)$. Donc il existe $m \in \mathbb{N}$ tel que $a \in I_m$. Or, pour tout $p \geqslant m$, on a $I_m \subseteq I_p \subseteq I = (a) \subseteq I_m$. Ce qui signifie que la suite $(I_n)_{n\in\mathbb{N}}$ est stationnaire, à partir du rang m. □

***Définition* VIII.7.2.** Soient A un anneau intègre et a un élément non nul de A.

a) L'élément a est dit **irréductible** s'il n'est pas inversible et si l'égalité $a = bc$, $(b, c) \in A \times A$, implique que b ou c est un élément inversible de A.

b) L'élément a est dit **premier** si l'idéal (a) est premier.

***Remarques* VIII.7.3.**

a) D'après la définition d'un idéal premier, définition (VIII.3.2), un élément $a \in A$ est premier s'il est non nul et non inversible et vérifie

$$a|bc \Longrightarrow (a|b \quad \text{ou} \quad a|c).$$

b) Un élément a d'un anneau A est irréductible (resp. premier) si et seulement si, pour tout élément inversible u de A, ua est irréductible (resp. premier, d'après la remarque (VIII.7.1)) dans A. Par conséquent, on considérera les éléments irréductibles (resp. premiers) d'un anneau, « aux inversibles près ». Il est facile de vérifier que ceci définit une relation d'équivalence sur l'ensemble des éléments irréductibles (resp. premiers) de l'anneau A. Dans la suite, on notera $\mathcal{P}$ un système de représentants des classes pour cette relation d'équivalence.

***Proposition* VIII.7.1.** *Si A est un anneau intègre, tout élément premier non nul est irréductible.*

Démonstration. Puisque l'idéal (a) est premier, on a $(a) \neq A$, donc a est non inversible dans A. Si $a = bc$, alors $b \in (a)$ ou $c \in (a)$ puisque (a) est un idéal premier. Si $b \in (a)$, alors $b = ua$, d'où $a = bc = uac$ et $a(1 - uc) = 0$. Puisque l'anneau A est intègre, on a $(1 - uc) = 0$, ce qui signifie que c est inversible. Si c'est c qui appartient à (a), le même raisonnement montre que b est inversible. □

Attention. *La réciproque est fausse (*cf. *exercice VIII.15 ci-dessous). Cependant, voir la remarque VIII.7.4 ci-dessous.*

***Exercice* VIII.15.** Soient K un corps et A le sous-anneau de $K[X, Y]$ formé des polynômes dont le degré total est pair. Montrer que l'élément XY est irréductible dans A, mais pas premier.

***Proposition* VIII.7.2.** *Soient A un anneau intègre et $a \neq 0$ un élément de A.*

(i) *Si l'idéal (a) est maximal, l'élément a est irréductible.*

(ii) *Si A est principal et si a est irréductible, l'idéal (a) est maximal.*

Démonstration. (i). Si l'idéal (a) est maximal, il est premier, l'élément a est donc premier, et par conséquent irréductible.

(ii). Supposons que l'élément a soit irréductible et que l'anneau A soit principal. Supposons qu'il existe un idéal $I = (b)$ de A tel que $(a) \subseteq I$. Alors $a = bc$ et, puisque a est irréductible, b ou c est inversible. Si b est inversible, alors $(b) = A$ et si c est inversible, alors $b = ac^{-1}$ et $(b) = (a)$. On en déduit que l'idéal (a) est maximal. □

***Remarque* VIII.7.4.** Un idéal maximal étant premier, ce qui précède montre que, dans un anneau principal, les éléments premiers (resp. les idéaux premiers non nuls) et les éléments irréductibles (resp. les idéaux maximaux) coïncident. En particulier, si K est un corps et si f est un polynôme de $K[X]$, on a les équivalences suivantes :

$$f \text{ est irréductible} \Leftrightarrow K[X]/(f) \text{ est un corps} \Leftrightarrow K[X]/(f) \text{ est intègre.}$$

***Exercice* VIII.16.** Montrer que l'anneau $A[X]$ est principal si et seulement si A est un corps.

***Proposition* VIII.7.3.** *Soit A un anneau intègre dans lequel tout élément non nul et non inversible est produit fini d'éléments irréductibles de A. Alors les assertions suivantes sont équivalentes :*

(i) *Si a est un élément non nul et non inversible de A et si $a = p_1 \dots p_n = q_1 \dots q_m$, où les éléments $p_1, \dots, p_n$, $q_1, \dots, q_m$ sont des éléments irréductibles de A, alors $m = n$ et il existe une permutation $\sigma \in S_n$ et des éléments inversibles de A, $u_1, \dots, u_n$, tels que $q_i = u_i\, p_{\sigma(i)}$, $i = 1, \dots, n$*

(ii) *Si a est un élément irréductible de A, alors a est un élément premier.*

Démonstration. Montrons que (i) implique (ii). Soient b et c deux éléments non nuls de A et supposons que a divise bc. Si b (resp. c) est inversible, il est évident que a divise c (resp. b). On suppose donc que b et c sont non inversibles. On a alors $bc = ad$ avec d non inversible, sinon l'élément a étant irréductible, on aurait b ou c inversible. On a donc

$$b = p_1 \dots p_r, \quad c = p_{r+1} \dots p_{r+s}, \quad d = q_1 \dots q_t$$

où les p_i et q_j, $1 \leqslant i \leqslant r+s$, $1 \leqslant j \leqslant t$, sont des éléments irréductibles de A. L'égalité $bc = ad$ s'écrit alors

$$p_1 \dots p_r p_{r+1} \dots p_{r+s} = a q_1 \dots q_t.$$

D'après la condition (i), il existe un i_0, $1 \leqslant i_0 \leqslant r+s$, et un élément inversible u_{i_0} de A tels que $a = u_{i_0} p_{i_0}$. On en déduit que si $1 \leqslant i_0 \leqslant r$, alors a divise b et si $r+1 \leqslant i_0 \leqslant r+s$, alors a divise c.

Montrons que (ii) implique (i). Soit $a = p_1 \dots p_n = q_1 \dots q_m$, où les éléments $p_1, \dots, p_n$, $q_1, \dots, q_m$ sont des éléments irréductibles de A. Il s'agit de montrer que $m = n$ et que, pour tout i, il existe une permutation $\sigma \in S_n$ et un élément inversible u_i tels que $q_i = u_i p_{\sigma(i)}$. On procède par récurrence sur $n+m$: si $n+m = 2$, alors $p_1 = q_1$. Supposons le résultat établi pour $n'+m' < n+m$; comme $q_1 | p_1 \dots p_n$ et que q_1 est irréductible, d'après (ii) $q_1 | p_j$ pour un certain j et il existe u_1 tel que $q_1 = u_1 p_j$. On peut donc appliquer l'hypothèse de récurrence à $q_2 \dots q_m$ et $p_1 \dots p_{j-1} p_{j+1} \dots p_n$: on a $n-1 = m-1$, il existe une permutation $\mu \in S_{n-1}$ et des éléments inversibles $u_2, \dots, u_n$ tels que $q_i = u_i p_{\mu(i)}$. On a donc $n = m$ et on étend μ en un élément $\sigma \in S_n$ en posant $\sigma(1) = j$ et $\sigma(i) = \mu(i)$ pour $i = 2, \dots, n$. □

Théorème VIII.7.4. *Soit A un anneau principal, alors :*

(i) *Chaque élément non nul et non inversible de A s'écrit comme produit fini d'éléments irréductibles de A*

(ii) *Les deux assertions équivalentes de la proposition VIII.7.3 sont vérifiées.*

Démonstration. (i). Si A est un corps, l'ensemble des éléments non nuls et non inversibles est vide et toutes les assertions ci-dessus sont vérifiées. On suppose donc que A n'est pas un corps.

Soient a un élément non nul et non inversible de A. Si a est irréductible, l'assertion est vérifiée. Supposons que a est non irréductible : montrons d'abord que a admet un facteur irréductible. S'il n'en admettait pas, on pourrait écrire $a = a_1 b_1$ avec a_1 et b_1 non inversibles. De la même manière, on aurait $a_1 = a_2 b_2$ avec a_2 et b_2 non inversibles. En réitérant ce procédé, on aurait une suite d'éléments a_i avec $a_i | a_{i+1}$ et, pour tout i, $a_i \neq u_i a_{i+1}$ avec u_i inversible. Autrement dit, on aurait une suite strictement croissante d'idéaux $\{(a)\}_{i \in \mathbb{N}}$, ce qui est en contradiction avec le fait que A est un anneau principal, d'après le théorème (VIII.7.3). Ceci montre que $a = p_1 a_1$ avec p_1 irréductible : si a_1 est inversible, c'est terminé. Sinon, on a $a_1 = p_2 a_2$ avec p_2 irréductible. Ce processus s'arrête au bout d'un nombre fini d'étapes, sinon on aurait à nouveau une suite strictement croissante d'idéaux $\{(a)\}_{i \in \mathbb{N}}$. Il existe donc un entier n tel que $a = a_n p_1 \dots p_n$, avec a_n inversible et $p_1, \dots, p_n$ irréductibles.

(ii). Supposons que q soit un élément irréductible de A et que $q | bc$. D'après l'assertion (i), on peut écrire $b = u \prod_{p \in \mathcal{P}} p^{n_p}$, avec u inversible et n_p entiers positifs

ou nuls, non nuls pour un nombre fini de p, et $c = v\prod_{p\in\mathcal{P}} p^{n'_p}$, avec v inversible et n'_p entiers positifs ou nuls, non nuls pour un nombre fini de p. Puisque $q|bc$, on a $n_q + n'_q \geqslant 1$, donc $n_q \geqslant 1$ ou $n'_q \geqslant 1$ et $q|b$ ou $q|c$. □

***Remarques* VIII.7.5.** Nous allons ici préciser la remarque VIII.7.3.b. Soit A un anneau principal, il existe un ensemble $\mathcal{P}$ d'éléments irréductibles de A tel que :

(i) $\forall p, q \in \mathcal{P}$, si $p \neq q$, alors $\forall u \in \mathbb{U}(A)$, $q \neq up$

(ii) Tout élément irréductible de A est multiple d'un unique élément de $\mathcal{P}$ par un élément inversible de A

(iii) Tout élément a de A, non nul et non inversible, s'écrit de manière unique $a = u\,p_1^{\alpha_1}\dots p_n^{\alpha_n}$, où $u \in \mathbb{U}(A)$ et $p_i \in \mathcal{P}$, $i = 1,\dots,n$, $\alpha_i \in \mathbb{N}^*$, $i = 1,\dots,n$.

Un tel ensemble $\mathcal{P}$, qui est un système de représentants des classes d'éléments irréductibles modulo les éléments inversibles, est appelé ensemble ***complet*** d'éléments irréductibles.

VIII.8. Divisibilité

***Définition* VIII.8.1.** Soient a et b deux éléments d'un anneau A.

a) On appelle **plus grand diviseur commun** de a et b, et on note $pgcd(a,b)$, tout élément d de A vérifiant les deux propriétés suivantes :

(i) $d|a$ et $d|b$

(ii) $\forall x \in A$ tel que $x|a$ et $x|b$, alors $x|d$.

b) On appelle **plus petit commun multiple** de a et b, et on note $\mathrm{ppcm}(a,b)$, tout élément m de A vérifiant les propriétés suivantes :

(i) $a|m$ et $b|m$

(ii) $\forall x \in A$ tel que $a|x$ et $b|x$, alors $m|x$.

***Proposition* VIII.8.1.** *Soient a et b deux éléments d'un anneau intègre A. Alors, si d et d' (resp. m et m') sont deux pgcd (resp. ppcm) de a et b, il existe un élément u inversible de A tel que $d' = ud$ (resp. $m' = um$).*

Démonstration. Soient d et d' deux *pgcd* de a et b. Alors, puisque d est un diviseur de a et b, d divise d' et, pour les mêmes raisons, d' divise d. Par conséquent, il existe des éléments u et v de A tels que $d' = ud$ et $d = vd'$. On a donc $d = uvd$, *i.e.* $d(1-uv) = 0$ et, puisque A est intègre, u et v sont inversibles.

La démonstration pour les *ppcm* est analogue. □

***Remarque* VIII.8.1.** On peut aussi énoncer la proposition précédente de la façon suivante : si deux éléments d'un anneau intègre admettent un *pgcd* (resp. *ppcm*), il est **unique à la multiplication par un élément inversible près**.

***Théorème* VIII.8.1.** *Soient deux éléments quelconques, non nuls, a et b d'un anneau principal A.*

(i) *Ils ont un pgcd et un ppcm dans A.*

(ii) *Il existe un pgcd d et un ppcm m de a et b tels que $ab = dm$.*

Démonstration. Le résultat est évident si les éléments a ou b sont inversibles. Soient a et b des élément non nuls et non inversibles : on a

$$a = u\prod_{i\in I} p_i^{\alpha_i} \quad , \quad b = v\prod_{j\in J} p_j^{\beta_j}$$

où u et v sont des éléments inversibles de A, les p_i et p_j sont des éléments irréductibles, α_i et β_j sont des entiers positifs. En acceptant que des α_i et β_j soient éventuellement nuls, on peut supposer que $I = J$. Alors,

$$\prod_{k\in I} p_k^{\gamma_k} \quad , \quad \prod_{k\in I} p_k^{\delta_k}$$

avec

$$\gamma_k = inf(\alpha_k, \beta_k) \quad , \quad \delta_k = sup(\alpha_k, \beta_k)$$

sont respectivement un *pgcd* et un *ppcm* de a et b. Si l'on pose

$$d = u\prod_{k\in I} p_k^{\gamma_k} \quad , \quad m = v\prod_{k\in I} p_k^{\delta_k}$$

on a $dm = ab$. □

***Remarque* VIII.8.2.** La définition d'un *pgcd* (resp. *ppcm*) de deux éléments d'un anneau s'étend clairement à une famille finie d'éléments $a_1, \ldots, a_n$ de A. Le même procédé que celui montrant l'existence d'un pgcd (resp. ppcm) de deux éléments d'un anneau principal, montre l'existence d'un pgcd (resp. ppcm) d'une famille finie d'éléments.

Définition* VIII.8.2.** Des éléments $a_1, \ldots, a_n$ d'un anneau principal A sont dits ***étrangers s'ils admettent l'unité de A pour pgcd.

Proposition VIII.8.2.

(i) *Soient $a_1, \ldots, a_n$ des éléments d'un anneau principal A et d un pgcd de ces éléments. Posons $a_i = da_i'$, $i = 1, \ldots, n$. Les éléments a_i', $i = 1, \ldots, n$, sont étrangers.*

(ii) *Si $a_1, \ldots, a_n$ sont des éléments étrangers deux à deux d'un anneau principal, le produit $a_1, \ldots, a_n$ est un ppcm de $a_1, \ldots, a_n$.*

Démonstration. Laissée au lecteur à titre d'exercice. □

On a les propriétés plus précises suivantes.

***Théorème VIII.8.2* (de Bezout).** *Soient $a_1, \ldots, a_n$, d des éléments d'un anneau principal. Les assertions suivantes sont équivalentes :*

(i) *d est un pgcd de $a_1, \ldots, a_n$*

(ii) *d est un générateur de l'idéal de A engendré par les éléments $a_1, \ldots, a_n$.*

Démonstration. Si $d = pgcd(a_1, \ldots, a_n)$, alors l'idéal $(a_1, \ldots, a_n)$ est contenu dans l'idéal (d). Puisque A est un anneau principal, il existe un élément $b \in A$ tel que $(a_1, \ldots, a_n) = (b)$, d'où b divise les éléments a_i, $i = 1, \ldots, n$, et par conséquent b divise d, *i.e.* (d) est contenu dans (b). On en déduit que $(d) = (a_1, \ldots, a_n)$.

Soit d un élément de A tel que $(d) = (a_1, \ldots, a_n)$. Alors, pour tout $i = 1, \ldots, n$, d divise a_i. Soit b un élément de A divisant les éléments a_i, $i = 1, \ldots, n$. Alors, $(d) = (a_1, \ldots, a_n)$ est contenu dans (b), donc b divise d. On en déduit que d est un *pgcd* de $a_1, \ldots, a_n$. □

Théorème VIII.8.3. *Soient $a_1, \ldots, a_n$, m des éléments d'un anneau principal A. Les assertions suivantes sont équivalentes :*

(i) *m est un ppcm de $a_1, \ldots, a_n$*

(ii) *m est un générateur de l'idéal $\bigcap_{i=1}^{n}(a_i)$.*

Démonstration. Laissée au lecteur à titre d'exercice. □

VIII.9. Irréductibilité des polynômes

Nous avons vu, dans les paragraphes précédents, l'importance de l'existence, dans un anneau, d'éléments irréductibles. Nous allons ici nous intéresser au cas des anneaux de polynômes, donc essayer de déterminer les **polynômes irréductibles**.

Dans tout ce paragraphe, A est un anneau **principal** et K est son **corps des fractions**.

Soit p un élément irréductible (ou premier) d'un ensemble complet $\mathcal{P}$ d'éléments irréductibles de A. Pour tout élément a de K^*, on peut écrire $a = p^r b$, $b \in K^*$, $r \in \mathbb{Z}$, p ne divisant ni le numérateur ni le dénominateur de b. L'unicité de la décomposition en produit de facteurs irréductibles dans A implique que l'entier r ainsi défini est unique. On pose $r = ord_p(a)$ et on appelle cet entier l'**ordre** de a en p. Si a est nul, on pose $ord_p(a) = -\infty$ pour tout p.

Il est clair que

$$\forall a, a' \in K,\ ord_p(aa') = ord_p(a) + ord_p(a').$$

Soit $f(X) = a_0 + a_1X + \ldots + a_nX^n$ un élément de $K[X]$. Si $f = 0$, on pose $ord_p(f) = -\infty$, si $f \neq 0$, on pose $ord_p(f) = \inf_i(ord_p(a_i))$, le inf étant pris sur les i tels que $a_i \neq 0$. On pose alors

$$c(f) = \prod_{p \in \mathcal{P}} p^{ord_p(f)}$$

le produit étant pris sur tous les p tels que $ord_p(f) \neq 0$.

On notera que $c(f)$ est défini à un élément inversible de A près. Si

$$f(x) = \sum_{i=0}^{n} a_i X^i \in A[X],$$

alors $c(f) = pgcd(a_i)_{0 \leqslant i \leqslant n}$, le *pgcd* étant pris sur les coefficients non nuls de f.

Il est clair que si b est un élément de K^*, alors $c(bf) = bc(f)$. On peut donc écrire $f(X) = c(f)f_1(X)$, avec $c(f_1) = 1$ et $f_1 \in A[X]$. En effet, écrivons

$$f(X) = \sum_{i=0}^{n} \frac{a_i}{b_i} X^i,$$

avec $a_i, b_i \neq 0$ dans A. Notons b un *ppcm* des b_i, $0 \leqslant i \leqslant n$, alors f s'écrit

$$f(X) = \frac{1}{b} \sum_{i=0}^{n} a'_i X^i.$$

En posant $a'_i = da''_i$, où d est un *pgcd* des a'_i, $0 \leqslant i \leqslant n$, on obtient

$$f(X) = \frac{d}{b} f_1(X), \quad \text{avec } f_1(X) = \sum_{i=0}^{n} a''_i X^i.$$

On suppose qu'on a réduit $\frac{d}{b}$ de telle sorte que d et b soient étrangers. On a donc $c(f) = c(\frac{d}{b}f_1) = \frac{d}{b}c(f_1)$. Puisque les coefficients de f_1 sont étrangers, il est évident que $c(f_1) = 1$. On en déduit donc que $c(f) = \frac{d}{b}$.

Autrement dit, pour tout polynôme $f(X) \in K[X]$, l'écriture $f(X) = c(f)f_1(X)$ consiste à « réduire au même dénominateur » et à « mettre en facteur les facteurs communs aux coefficients ».

Autrement dit, pour un polynôme $f \in A[X]$, montrer que $c(f) = 1$ revient à montrer qu'il n'existe aucun élément irréductible p de A qui divise tous les coefficients de f.

***Lemme VIII.9.1* (de Gauss).** *Soient a un élément irréductible d'un anneau principal A, $f \in A[X]$ et $g \in A[X]$. Si a divise le produit fg, alors a divise f ou a divise g.*

Démonstration. Écrivons

$$f(X) = b_0 + b_1X + \ldots + b_nX^n\,, \quad g(X) = c_0 + c_1X + \ldots + c_mX^m.$$

Si $n = m = 0$, le résultat est clair d'après la définition d'un anneau principal. On suppose que $n \neq 0$ ou $m \neq 0$ et que a ne divise ni f, ni g. De manière générale, un élément a d'un anneau intègre A divise un polynôme $f \in A[X]$ si et seulement si a divise chaque coefficient de f. Il existe donc un coefficient $b_{i_0} \neq 0$ qui n'est pas divisible par a. On peut donc considérer k le plus petit entier, $0 \leqslant k \leqslant n$, tel que a ne divise pas b_k, *i.e.* a divise b_i pour $i < k$. De la même manière, on considère le plus petit entier h tel que a divise c_i pour $i < h$. Le coefficient du terme de degré $h + k$ de fg est

$$b_0c_{h+k} + b_1c_{h+k-1} + \ldots + b_kc_h + \ldots + b_{h+k}c_0.$$

L'élément a divise tous les termes de cette somme sauf le terme b_kc_h ; par conséquent a ne divise pas le coefficient du terme de degré $h + k$ de fg, il ne divise donc pas fg.

Lemme VIII.9.2. *Soient A un anneau principal, $f \in A[X]$, $g \in A[X]$ et a un élément de A qui divise le produit fg. Si f est irréductible, alors a divise g.*

Démonstration. On applique le lemme précédent à tous les facteurs irréductibles de a. □

Lemme VIII.9.3. *Soient A un anneau principal et K son corps des fractions. Soient f et g deux éléments de $K[X]$, alors $c(fg) = c(f)c(g)$.*

Démonstration. Puisque $f(X) = c(f)f_1(X)$ et $g(X) = c(g)g_1(X)$, il suffit de montrer que si $c(f) = c(g) = 1$, alors $c(fg) = 1$, avec f et g dans $A[X]$. Posons

$$f(X) = a_0 + \ldots + a_nX^n,\ a_n \neq 0, \quad \text{et} \quad g(X) = b_0 + \ldots + b_mX^m,\ b_m \neq 0.$$

Soit p un élément irréductible de A et soit r (resp. s) le plus petit entier compris entre 0 et n (resp. m) tel que p ne divise pas a_r (resp. b_s). Le coefficient de X^{r+s} dans $f(X)g(X)$ est égal à

$$a_rb_s + a_{r+1}b_{s-1} + \ldots + a_{r-1}b_{s+1} + \ldots$$

Or p ne divise pas a_rb_s, mais divise tous les autres termes de cette somme, il ne divise donc pas la somme. □

***Remarques* VIII.9.1.**

a) On déduit de ce qui précède que si $f(X) \in A[X]$ s'écrit $f(X) = g(X)h(X)$ dans $K[X]$, alors, en posant $g(X) = c(g)g_1(X)$, avec $g_1(X) \in A[X]$, et $h(X) = c(h)h_1(X)$, avec $h_1(X) \in A[X]$, on a $f(X) = c(g)c(h)g_1(X)h_1(X)$, où $c(g)c(h)$ est un élément de A. En effet, $c(f) = c(g)c(h)c(g_1h_1) = c(g)c(h)$ et, puisque $f(X) \in A[X]$, $c(f)$ est un élément de A.

b) Il est clair que si $f \in A[X]$ est un polynôme de degré strictement positif tel que $c(f) \neq 1$, (ou $c(f)$ non inversible dans A), f n'est pas irréductible dans $A[X]$ puisqu'il s'écrit $f = c(f)f_1$, avec $c(f)$ et f_1 non inversibles. La condition $c(f) = 1$ est donc nécessaire pour que le polynôme f soit irréductible dans $A[X]$.

Théorème VIII.9.1. *Soient A un anneau principal et K son corps des fractions. Un polynôme $f \in A[X]$ est irréductible dans $A[X]$ si et seulement si f est un élément irréductible de A, ou un polynôme de degré supérieur ou égal à 1 irréductible dans $K[X]$ et tel que $c(f) = 1$.*

Démonstration. Montrons que la condition est nécessaire. Soit $P(X) \in A[X]$ un polynôme irréductible dans $A[X]$.

Si $deg(P) = 0$, alors $P(X)$ est un élément de A, irréductible par hypothèse.

Si $deg(P) > 0$, alors $c(P) = 1$ d'après la remarque (VIII.9.1.b). Montrons que P est irréductible dans $K[X]$. Faisons un raisonnement par l'absurde : supposons que P s'écrive $P(X) = Q(X)R(X)$ avec $Q(X) \in K[X]$ et $R(X) \in K[X]$ non nuls. D'après la remarque (VIII.9.1.a), on a $P(X) = c(Q)c(R)Q_1(X)R_1(X)$ avec $Q_1(X) \in A[X]$, $R_1(X) \in A[X]$ et $c(Q)c(R) = c(P) = 1$. Par conséquent, P n'est pas irréductible dans $A[X]$, contrairement à l'hypothèse.

Montrons que la condition est suffisante. Si p est un élément irréductible de A, il est irréductible dans $A[X]$ (vérification évidente). Soit $P(X) \in A[X]$, irréductible dans $K[X]$ et tel que $c(P) = 1$. Supposons que $P(X) = Q(X)R(X)$, avec $Q(X) \in A[X]$ et $R(X) \in A[X]$. Comme $A[X] \subset K[X]$, on a $deg(Q) = 0$ ou $deg(R) = 0$. Supposons, pour fixer les idées, que ce soit $deg(Q) = 0$. Alors $Q(X) = a \in A$ et $P(X) = aR(X)$. Puisque $c(P) = 1$, on en déduit que $a \in \mathbb{U}(A)$ et P est irréductible dans $A[X]$. □

Exercice VIII.17. Soient A un anneau principal, K son corps des fractions, $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in A[X]$, avec $a_0 \neq 0$.

a) Montrer que, si $x \in K$ est tel que $f(x) = 0$, alors x divise a_0 et $x \in A$.

b) En déduire que le polynôme $X^3 - 5X^2 + 1$ est irréductible dans $\mathbb{Q}[X]$.

Ce qui précède montre que l'étude de l'irréductibilité des polynômes à coefficients dans A se ramène à celle des polynômes à coefficients dans K. Ce qui suit a pour but de donner quelques méthodes d'étude de l'irréductibilité des polynômes de $K[X]$.

***Théorème VIII.9.2* (critère d'Eisenstein).** *Soient A un anneau principal et K son corps des fractions. Soit $f(X) = a_0 + \ldots + a_nX^n$ un polynôme de $A[X]$, $n \geqslant 1$. S'il existe un élément irréductible p de A tel que*

$$a_n \not\equiv 0\,(mod\,p), \quad a_i \equiv 0\,(mod\,p)\ i < n, \quad a_0 \not\equiv 0\,(mod\,p^2),$$

alors $f(X)$ est irréductible dans $K[X]$.

Démonstration. En mettant en facteur le *pgcd* des coefficients de f, on peut supposer que $c(f) = 1$. Supposons que $f(X)$ s'écrive comme produit de deux polynômes de $K[X]$, de degré supérieur ou égal à 1. D'après la remarque (VIII.9.1.a), on a $f(X) = g(X)h(X)$ dans $A[X]$. Posons

$$g(X) = b_0 + \ldots + b_pX^p\,, \quad h(X) = c_0 + \ldots + c_qX^q,$$

avec $b_p \neq 0$, $c_q \neq 0$, $p \geqslant 1$, $q \geqslant 1$.

Puisque $b_0c_0 = a_0$ est divisible par p mais pas par p^2, l'un et l'un seulement des éléments b_0 ou c_0 est divisible par p. On peut supposer que b_0 n'est pas divisible par p et que c_0 est divisible par p. Puisque $a_n = b_pc_q$ n'est pas divisible par p, c_q n'est pas divisible par p. On peut donc considérer r, $r \leqslant q < n$, le plus petit entier tel que c_r ne soit pas divisible par p. Alors, $a_r = b_0c_r + b_1c_{r-1} + \ldots$ n'est pas divisible par p, puisque p ne divise pas b_0c_r mais divise tous les autres termes de la somme, ce qui est contraire à l'hypothèse. □

***Exemples* VIII.9.1.**

a) Soit $a \neq 1 \in \mathbb{Z}^*$ un élément sans facteur carré. Alors pour tout $n \geqslant 1$, le polynôme $X^n - a$ est irréductible dans $\mathbb{Q}[X]$.

b) Soit p un nombre premier. Alors le polynôme

$$f(X) = 1 + X + X^2 + \ldots + X^{p-1}$$

est irréductible dans $\mathbb{Q}[X]$. En effet, il suffit de montrer que $f(X+1)$ est irréductible dans $\mathbb{Q}[X]$. On a

$$f(X+1) = (X+1)^{p-1} + \ldots + (X+1) + 1 = \frac{(X+1)^p - 1}{(X+1) - 1}$$

$$= \frac{1}{X}\left(X^p + \sum_{k=1}^{p-1} C_p^k X^k\right) = X^{p-1} + \sum_{k=2}^{p-2} C_p^{k+1} X^k + p$$

et C_p^k est divisible par p. On peut donc appliquer le critère d'Eisenstein.

On verra aux TR.VIII.A, TR.VIII.B et TP.IX.A d'autres méthodes d'étude de l'irréductibilité des polynômes, qui sont très utiles et efficaces.

VIII.10. Racines – Ordre de multiplicité

Définition* VIII.10.1.** Soient A un anneau, B un sur-anneau de A et $f(X_1, \ldots, X_n)$ un polynôme de $A[X_1, \ldots, X_n]$. Un n-uple $(b_1, \ldots, b_n) \in B^n$ est un ***zéro (ou une **racine** si $n = 1$) de f si $f(b_1, \ldots, b_n) = 0$.

***Théorème* VIII.10.1.** *Soient A un anneau intègre, $f(X)$ un polynôme de $A[X]$ et a un élément de A. Alors a est racine de $f(X)$ si et seulement si $(X - a)$ divise $f(X)$ dans $A[X]$.*

Démonstration. La division euclidienne de $f(X)$ par $(X - a)$ dans $A[X]$,

$$f(X) = (X - a)q(X) + r(X)$$

montre que $f(a) = 0$ si et seulement si $r(a) = 0$. Or, $deg(r) < 1$ implique que $r(X)$ est une constante, par conséquent $r(a) = 0$ si et seulement si $r(X) = 0$. □

Exercice VIII.18. Soit $P(X)$ un polynôme de degré 2 ou 3, à coefficients dans un anneau intègre A.

a) Montrer que si $P(X)$ est unitaire, il est réductible si et seulement s'il possède un zéro dans A.

b) Donner un exemple de polynôme non unitaire de $\mathbb{Z}[X]$ qui est réductible mais qui ne possède pas de zéro dans $\mathbb{Z}$.

Exercice VIII.19. Soit $f(X) = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{Z}[X], a_n \neq 0, n \geqslant 1$.

a) Montrer que si $x = \frac{p}{q} \in \mathbb{Q}$, avec p et q étrangers, est racine de $f(X)$, alors p divise a_0 et q divise a_n.

b) En déduire les racines dans $\mathbb{Q}$ du polynôme $f(X) = 6X^3 - 7X^2 - X + 2$.

Théorème VIII.10.2. *Soient A un anneau intègre et $f(X)$ un polynôme non nul de $A[X]$. Le nombre de racines distinctes de $f(X)$ dans $A[X]$ est au plus égal au degré de $f(X)$.*

Démonstration. Soient $a_1, \ldots, a_n$ des racines distinctes de $f(X)$ dans A. Montrons, par récurrence sur n, que $f(X)$ est divisible dans $A[X]$ par $(X - a_1) \ldots (X - a_n)$. D'après le théorème (VIII.10.1), l'assertion est vraie pour $n = 1$. Supposons qu'elle soit vraie pour $n-1$. On a $f(X) = (X - a_1) \ldots (x - a_{n-1})g(X)$. L'anneau A étant intègre et $a_n \neq a_i$, $i < n$, $f(a_n) = 0$ implique que $g(a_n) = 0$. Le polynôme $g(X)$ est donc divisible par $(X - a_n)$, d'où le résultat. □

Corollaire VIII.10.1. *Soient A un anneau intègre et S une partie infinie de A. Si $f(X)$ est un polynôme de $A[X]$ tel que $f(a) = 0$ pour tout a dans S, alors $f(X)$ est le polynôme nul.* □

Corollaire VIII.10.2. *Soient A un anneau intègre et $S_1, \ldots, S_n$ des parties infinies de A. Si $f(X_1, \ldots, X_n)$ est un polynôme de $A[X_1, \ldots, X_n]$ tel que $f(a_1, \ldots, a_n) = 0$ pour tout $(a_1, \ldots, a_n)$ dans $S_1 \times \ldots \times S_n$, alors $f(X)$ est le polynôme nul.*

Démonstration. On procède par récurrence sur n. Si $n = 1$, c'est le résultat précédent. On suppose le résultat vrai pour $(n - 1) \geqslant 1$. Soit $f(X_1, \ldots, X_n)$ un polynôme de $A[X_1, \ldots, X_n]$ tel que $f(a_1, \ldots, a_n) = 0$ pour tout $(a_1, \ldots, a_n)$ dans $S_1 \times \ldots \times S_n$. On écrit $f(X_1, \ldots, X_n)$ suivant les puissances croissantes de X_n,

$$f(X_1, \ldots, X_n) = \sum_{i=0}^{s} g_i(X_1, \ldots, X_{n-1})X_n^i,$$

avec $g_i(X_1,\dots,X_{n-1}) \in A[X_1,\dots,X_{n-1}]$. Si $g_i(a_1,\dots,a_{n-1}) = 0$ pour tout $(a_1,\dots,a_{n-1})$ dans $S_1 \times \dots \times S_{n-1}$, alors l'hypothèse de récurrence entraîne que $g_i(X_1,\dots,X_{n-1}) = 0$. Donc, si $f(X_1,\dots,X_n) \neq 0$, il existe un indice i_0 et $(a_1,\dots,a_{n-1}) \in S_1 \times \dots \times S_{n-1}$ tels que $g_{i_0}(a_1,\dots,a_{n-1}) \neq 0$. Alors $f(a_1,\dots,a_{n-1},X_n)$ est un polynôme non nul en X_n, ce qui contredit le fait qu'il est nul pour une infinité de valeurs de X_n. □

***Définition* VIII.10.2.** Soient A un anneau intègre, $f(X)$ un polynôme de $A[X]$ et $a \in A$ une racine de f. L'**ordre de multiplicité** de a est le plus grand entier m tel que $(X-a)^m$ divise $f(X)$. Si $m > 1$, on dit que a est une **racine multiple** d'ordre de multiplicité m ; si $m = 1$, on dit que a est une **racine simple**.

Attention. *Soient A un anneau intègre et*

$$f(X) = a_nX^n + a_{n-1}x^{n-1} + \dots + a_1X + a_0$$

un polynôme de $A[X]$. On sait, depuis les cours d'analyse du lycée, que son polynôme dérivé s'écrit

$$f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \dots + a_1.$$

Mais la définition d'une dérivée utilise la notion de limite, qui n'existe pas en algèbre. Cependant, il existe une notion de dérivation en algèbre et l'on montre (cf. *[14]*), *ce que l'on admettra ici, que tout polynôme admet un polynôme dérivé dont l'expression est la même que ci-dessus.*

***Proposition* VIII.10.1.** *Avec les mêmes notations que ci-dessus, a est une racine multiple de f si et seulement si $f(a) = 0$ et $f'(a) = 0$, où f' est le polynôme dérivé de f.*

Démonstration. Si a est racine multiple d'ordre m de $f(X)$, on a $f(X) = (X-a)^m g(X)$ avec $g(a) \neq 0$, d'où $f'(X) = (X-a)^m g'(X) + m(X-a)^{m-1}g(X)$. Si $m > 1$, alors $f'(a) = 0$; si $m = 1$, alors $f'(X) = (X-a)g'(X) + g(X)$, donc $f'(a) = g(a) \neq 0$. □

***Proposition* VIII.10.2.** *Si K est un corps de caractéristique nulle définition* (cf. *définition IX.1.3), pour que $a \in K$ soit une racine d'ordre r d'un polynôme $f \in K[X]$, il faut et il suffit que*

$$f(a) = f'(a) = \dots = f^{(r-1)}(a) = 0 \text{ et } f^{(r)}(a) \neq 0.$$

Démonstration. Si $a \in K$ est une racine d'ordre r d'un polynôme $f \in K[X]$, on a $f(X) = (X-a)^r g(X)$, avec $g(a) \neq 0$. On calcule la dérivée k-ième de cette égalité :

$$f^{(k)}(X) = r(r-1)\dots(r-k+1)(X-a)^{r-k}g(X) + (X-a)^{r-k+1}g_k(X).$$

On en déduit que $f^{(k)}(a) = 0$ pour $0 \leqslant k \leqslant r-1$. D'autre part, $f^{(r)}(a) = r!g(a)$ et, puisque $g(a) \neq 0$ et que K est un corps de caractéristique nulle, $f^{(r)}(a) \neq 0$.

Réciproquement, supposons que

$$f(a) = f'(a) = \dots = f^{(r-1)}(a) = 0 \text{ et } f^{(r)}(a) \neq 0.$$

Puisque K est un corps de caractéristique nulle, on peut diviser par $k!$ et on écrit :

$$f(X) = \sum_{k=0}^{k=n} (X-a)^k \frac{f^{(k)}(a)}{k!}$$

(utiliser le fait que les polynômes $\{(X-a)^k\}_{k\in\mathbb{N}}$ forment un base de $K[X]$ et identifier les coefficients).

Par hypothèse, tous les termes pour $k \leqslant r-1$ sont nuls, d'où :

$$f(X) = (X-a)^r \left[\frac{f^{(r)}(a)}{r!} + (X-a)\frac{f^{(r+1)}(a)}{(r+1)!} + \dots \right].$$

Autrement dit, on a $f(X) = (X-a)^r g(X)$ avec $g(a) \neq 0$. Si $f(X)$ était divisible par $(X-a)^{r+1}$, alors $g(X)$ serait divisible par $(X-a)$, ce qui est en contradiction avec $g(a) \neq 0$. Donc r est bien le plus grand entier k tel que $(X-a)^k$ divise $f(X)$. □

VIII.11. Polynômes symétriques

Soient A un anneau et $T_1, \dots, T_n, X$ des indéterminées. On forme le polynôme en X, à coefficients dans $A[T_1, \dots, T_n]$, suivant :

$$F(X) = (X-T_1)\dots(X-T_n).$$

En développant, on obtient

$$F(X) = X^n - s_1 X^{n-1} + \dots + (-1)^n s_n,$$

où les s_i sont les éléments de $A[T_1, \ldots, T_n]$ définis par

$s_1 = T_1 + \ldots + T_n$

$s_2 = T_1T_2 + T_1T_3 + \ldots + T_{n-1}T_n = \sum_{1 \leqslant i < j \leqslant n} T_iT_j$

. . . . . .

$s_k = \sum_{1 \leqslant i_1 < \ldots < i_j < \ldots < i_k \leqslant n} T_{i_1} \ldots T_{i_k}$

. . . . . .

$s_n = T_1T_2 \ldots T_n$.

***Définition* VIII.11.1.** Les polynômes $s_1, \ldots, s_n$ sont appelés **polynômes symétriques élémentaires** en $T_1, \ldots, T_n$.

On remarquera que chaque polynôme s_i est homogène de degré i.

Soit σ une permutation de l'ensemble $\{1, \ldots, n\}$. Étant donné un polynôme $f \in A[T_1, \ldots, T_n]$, on définit le polynôme ${}^{\sigma}f$ par

$$ {}^{\sigma}f(T_1, \ldots, T_n) = f(T_{\sigma(1)}, \ldots, T_{\sigma(n)}). $$

***Remarque* VIII.11.1.** Si σ et τ sont deux permutations de l'ensemble $\{1, \ldots, n\}$ et ε est la permutation identique, on a ${}^{\tau}({}^{\sigma}f) = {}^{(\tau\sigma)}f$ et ${}^{\varepsilon}f = f$. De plus, pour f et g dans $A[T_1, \ldots, T_n]$ et $\sigma \in S_n$, on a ${}^{\sigma}(f+g) = ({}^{\sigma}f) + ({}^{\sigma}g)$ et ${}^{\sigma}(fg) = ({}^{\sigma}f)({}^{\sigma}g)$. Autrement dit, le groupe S_n opère sur $A[T_1, \ldots, T_n]$.

***Définition* VIII.11.2.** Un polynôme f de $A[T_1, \ldots, T_n]$ est dit **symétrique** si ${}^{\sigma}f = f$ pour tout élément σ de S_n.

On vérifiera que les polynômes $s_1, \ldots, s_n$ sont symétriques au sens de cette définition. Il est clair que l'ensemble des polynômes symétriques est un sous-anneau de $A[T_1, \ldots, T_n]$. On va montrer le théorème suivant :

***Théorème* VIII.11.1.** *Le sous-anneau de $A[T_1, \ldots, T_n]$ formé des polynômes symétriques est isomorphe à l'anneau $A[s_1, \ldots, s_n]$.*

Démonstration. Il est clair que le sous-anneau de $A[T_1, \ldots, T_n]$ formé des polynômes symétriques contient A et les polynômes symétriques élémentaires $s_1, \ldots, s_n$. Il contient donc $A[s_1, \ldots, s_n]$. Nous allons montrer que, réciproquement, tout polynôme symétrique de $A[T_1, \ldots, T_n]$ appartient à $A[s_1, \ldots, s_n]$. Ce sera l'objet de la proposition (VIII.11.2) ci-dessous.

***Proposition* VIII.11.1.** *Si l'on substitue $T_n = 0$ dans les polynômes symétriques élémentaires $s_1, \ldots, s_{n-1}$, les expressions obtenues sont les polynômes symétriques élémentaires en $T_1, \ldots, T_{n-1}$.*

Démonstration. On a

$$F(X) = (X - T_1)\dots(X - T_n) = X^n - s_1X^{n-1} + \dots + (-1)^n s_n.$$

En faisant $T_n = 0$, on obtient

$$(X - T_1)\dots(X - T_{n-1})X = X^n - \tilde{s}_1X^{n-1} + \dots + (-1)^{n-1}\tilde{s}_{n-1}X$$

$$= X(X^{n-1} - \tilde{s}_1X^{n-2} + \dots + (-1)^{n-1}\tilde{s}_{n-1}).$$

D'où, $(X-T_1)\dots(X-T_{n-1}) = X^{n-1}-\tilde{s}_1X^{n-2}+\dots+(-1)^{n-1}\tilde{s}_{n-1}$, ce qui prouve que les polynômes $\tilde{s}_1, \dots, \tilde{s}_{n-1}$ sont les polynômes symétriques élémentaires en $T_1, \dots, T_{n-1}$. □

***Définition* VIII.11.3.** On appelle **poids d'un monôme** $S_1^{m_1}S_2^{m_2}\dots S_n^{m_n}$ en les s_i, l'entier $m_1 + 2m_2 + \dots + nm_n$. On définit le **poids en les s_i d'un polynôme** f de $A[S_1, \dots, S_n]$ comme étant le plus grand des poids en les s_i des monômes de f.

***Proposition* VIII.11.2.** *Soit $f \in A[T_1, \dots, T_n]$ un polynôme symétrique de degré d. Alors, il existe un polynôme $g \in A[T_1, \dots, T_n]$ tel que $f(T_1, \dots, T_n) = g(s_1, \dots, s_n)$, g étant de poids d en les s_i.*

Démonstration. On fait un raisonnement par récurrence sur n. Pour $n = 1$, c'est évident. On suppose le résultat vrai pour tout polynôme symétrique $f \in A[T_1, \dots, T_{n-1}]$ et on considère les polynômes symétriques de $A[T_1, \dots, T_n]$. On fait alors un raisonnement par récurrence sur le degré d de f. Si $d = 0$, c'est évident. On suppose le résultat vrai pour les polynômes de degré inférieur ou égal à $(d - 1)$. Soit $f \in A[T_1, \dots, T_n]$ un polynôme symétrique de degré d. Si on fait $T_n = 0$ dans f, d'après la proposition (VIII.11.1) et l'hypothèse de récurrence, il existe un polynôme $g_1(T_1, \dots, T_{n-1})$, de poids d en les $\tilde{s}_i$, tel que

$$f(T_1, \dots, T_{n-1}, 0) = g_1(\tilde{s}_1, \dots, \tilde{s}_{n-1}).$$

Le polynôme $g_1(s_1, \dots, s_{n-1})$ est symétrique en $T_1, \dots, T_n$, il en est donc de même du polynôme

$$f_1(T_1, \dots, T_n) = f(T_1, \dots, T_n) - g_1(s_1, \dots, s_{n-1}).$$

On a $f_1(T_1, \dots, T_{n-1}, 0) = 0$, donc f_1 est divisible par T_n et, puisqu'il est symétrique, il est divisible par le produit $T_1 \dots T_n = s_n$. Il existe donc un polynôme f_2 tel que $f_1 = s_n f_2$ et f_2 est nécessairement symétrique (car $s_n({}^\sigma f_2 - f_2) = 0$).

De plus, le polynôme g_1 étant de poids d en les $\tilde{s}_i$, $g_1(s_1, \ldots, s_{n-1})$ est de degré total en $T_1, \ldots, T_n$ au plus égal à d : en effet, puisque $deg(s_i) = i$, le monôme $s_1^{m_1} \ldots s_{n-1}^{m_{n-1}}$, exprimé en fonction des $T_1, \ldots, T_n$, est de degré total inférieur ou égal à $m_1 + 2m_2 + \ldots + (n-1)m_{n-1}$, qui est inférieur ou égal à d.

Par conséquent, le degré total de f_2 est inférieur ou égal à $d - n < d$. Par hypothèse de récurrence sur d, il existe un polynôme $g_2 \in A[T_1, \ldots, T_n]$, de poids égal à $d - n$ en les s_i, tel que

$$f_2(T_1, \ldots, T_n) = g_2(s_1, \ldots, s_n).$$

On obtient alors,

$$f(T_1, \ldots, T_n) = g_1(s_1, \ldots, s_{n-1}) + s_n g_2(s_1, \ldots, s_n)$$

et le second membre est un polynôme de poids d en les s_i. □

Ceci achève la démonstration du théorème (VIII.11.1). □

This page intentionally left blank

THÈMES DE RÉFLEXION

Nous allons étudier ci-dessous deux critères d'irréductibilité des polynômes. On en trouvera d'autres, utiles et efficaces, au TP.IX.A.

♠ TR.VIII.A. Critère d'irrédutibilité par extension

Si K est un corps, on appelle ***extension*** de K tout corps E qui contient K comme sous-corps.

1. *Montrer que la multiplication de E munit le groupe abélien $(E,+)$ d'une structure naturelle de K-espace vectoriel.*

On dit que E est une ***extension finie*** de K si E est une extension de K telle que le K-espace vectoriel E soit de dimension finie. On pose $[E:K] = dim_K(E)$.

Soient K un corps et $P(X) \in K[X]$. Nous admettrons qu'il existe une extension E de K, telle que le polynôme $P(X)$ admette une racine x dans E. (Pour tout corps K et tout polynôme $P(X) \in K[X]$, ce corps existe, *cf.* chapitre XII). On note $K(x)$ le plus petit sous-corps de E qui contienne K et x.

2. *Soient K un corps et $P(X) \in K[X]$ un polynôme de degré n et x une racine de $P(X)$. Montrer que si $P(X)$ est irréductible dans $K[X]$, alors $K(x) \simeq K[X]/P(X)$. Montrer que $[K(x):K] = n$.* (Montrer que $1, x, \ldots, x^{n-1}$ est une base du K-espace vectoriel $K(x)$.)

3. *Soient K un corps, $P(X) \in K[X]$ un polynôme de degré n. Montrer que $P(X)$ est irréductible dans $K[X]$ si et seulement s'il n'a pas de racine dans toute extension E de K telle que $[E:K] \leqslant n/2$.*

♣ TR.VIII.B. Critère d'irréductibilité par réduction

Soient A et B deux anneaux commutatifs et $f : A \longrightarrow B$ un morphisme d'anneaux. Pour tout polynôme $P \in A[X]$, $P(X) = a_nX^n + \ldots + a_0$, on note $f(P)$ le polynôme $f(a_n)X^n + \ldots + f(a_0)$ de $B[X]$.

1. *Soient A et B des anneaux intègres, K et L leurs corps des fractions respectifs, $f : A \longrightarrow B$ un morphisme d'anneaux. Soit $P \in A[X]$ tel que $f(P) \neq 0$ et $deg(f(P)) = deg(P)$. Montrer que si $f(P)$ est irréductible dans $L[X]$, alors on ne peut avoir $P(X) = Q(X)R(X)$ avec $Q, R \in A[X]$ de degré supérieur ou égal à 1.*

En déduire le résultat suivant :

2. *Soient A un anneau principal, K son corps des fractions, I un idéal premier de A, $B = A/I$, L le corps des fractions de B. Soient $P(X) = a_nX^n + \ldots + a_0 \in A[X]$ et $\overline{P}$ sa réduction modulo I. On suppose que $\overline{a_n} \neq 0$. Montrer que si $\overline{P}$ est irréductible dans $B[X]$ ou $L[X]$, alors P est irréductible dans $K[X]$.*

3. *Montrer que le polynôme X^2+Y^2+1 est irréductible dans $\mathbb{R}[X, Y]$.* (Considérer $I = (Y)$.)

On remarquera que P n'est pas nécessairement irréductible dans $A[X]$. (Considérer $P(X) = 2X \in \mathbb{Z}[X]$ et $I = (3)$.) Bien évidemment, d'après le théorème (VIII.9.1), si $deg(P) \geqslant 1$ et $c(P) = 1$, le polynôme P est irréductible dans $A[X]$.

On peut, en particulier, appliquer le résultat ci-dessus avec $A = \mathbb{Z}$ et $I = (p)$ avec p premier.

Nous allons montrer que, pour tout nombre premier p, le polynôme $f(X) = X^p - X - 1$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, ce qui, d'après le résultat ci-dessus, prouvera qu'il est irréductible dans $\mathbb{Z}[X]$. (En fait, il suffit que l'assertion soit vérifiée pour un seul p.)

Nous avons précisé au TR.VIII.A. qu'il existe un corps K, contenant le corps $\mathbb{Z}/p\mathbb{Z}$, dans lequel le polynôme $f(X)$ admet une racine a.

4. *Montrer que les racines de $f(X)$ sont les $a + j$, où j parcourt les entiers $0, 1, \ldots, (p - 1)$.*

On suppose que $f(X) = g(X)h(X)$, avec $g(X), h(X)$ appartenant à $\mathbb{Z}/p\mathbb{Z}[X]$ et $0 < r = deg(g) < p$, $0 < s = deg(h) < p$.

Alors, dans $K[X]$, on a $g(X) = \prod_{l=1}^{l=r}(X - (a + j_l))$, avec $j_l \in \{0, 1, \ldots, p-1\}$.

5. *En calculant le coefficient de X^{r-1}, montrer que $a \in \mathbb{Z}/p\mathbb{Z}$. En déduire une contradiction.*

Le résultat démontré à la question 2 est une condition suffisante, mais **non nécessaire**, comme le montre l'exemple ci-dessous. (♠)

6. *Montrer que le polynôme* $f(X) = X^4 + 1$ *est irréductible dans* $\mathbb{Z}[X]$. (On appliquera le critère d'Eisenstein à $f(X+1)$.)

On considère maintenant la réduction $f_p(X)$ de $f(X)$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$, pour p premier.

7. *Montrer que* $f_2(X)$ *n'est pas irréductible dans* $(\mathbb{Z}/2\mathbb{Z})[X]$.

On suppose maintenant que $p \geqslant 3$. On a alors, dans $(\mathbb{Z}/p\mathbb{Z})[X]$,

$$X^8 - 1 = (X^4 - 1)(X^4 + 1).$$

8. *Soit* E *une extension quelconque de* $\mathbb{Z}/p\mathbb{Z}$. *Montrer qu'un élément* $x \in E \setminus \{0\}$ *est racine du polynôme* $X^4 + 1$ *si et seulement si* x *est un élément d'ordre 8.*

9. *Montrer que* $(p^2 - 1)$ *est divisible par 8. En déduire qu'il existe un élément d'ordre 8 dans toute extension* E *de* $\mathbb{Z}/p\mathbb{Z}$ *telle que* $card(E) = p^2$. (Indication : utiliser le fait que le groupe E^* est cyclique, *cf.* exercice VIII.3.)

10. *Montrer que pour une telle extension* E, $[E : \mathbb{Z}/p\mathbb{Z}] = 2$. *En déduire que le polynôme* $X^4 + 1$ *n'est pas irréductible dans* $\mathbb{Z}/p\mathbb{Z}[X]$.

♡ TR.VIII.C. Résultant - Discriminant

On démontrera au chapitre XII que, pour tout corps K, il existe un corps $\overline{K}$, appelé *clôture algébrique* de K, tel que tout polynôme $f(X) \in K[X]$ s'écrive dans $\overline{K}[X]$ sous la forme $f(X) = a \prod_{1 \leqslant i \leqslant m} (X - a_i)$, où m est le degré de f.

A - Résultant de deux polynômes

Soient K un corps, $\overline{K}$ une clôture algébrique de K, $f(X) \neq 0$ et $g(X) \neq 0$ deux polynômes à coefficients dans K, de degrés respectifs m et n. Dans $\overline{K}[X]$, on a $f(X) = a \prod_{1 \leqslant i \leqslant m} (X - a_i)$ et $g(X) = b \prod_{1 \leqslant i \leqslant n} (X - b_i)$.

On appelle ***résultant*** des polynômes $f(X)$ et $g(X)$, le produit

$$Res(f, g) = a^n b^m \prod_{1 \leqslant i \leqslant m,\, 1 \leqslant j \leqslant n} (a_i - b_j).$$

Si $f = 0$ ou $g = 0$, on pose $Res(f, g) = 0$.

1. *Soient* $f(x) \neq 0$ *et* $g(X) \neq 0$ *des polynômes à coefficients dans* K. *Montrer que :*

(i) $Res(f, g) \in K$

(ii) *$Res(f,g) = 0$ si et seulement si $f(X)$ et $g(X)$ ont une racine commune*

(iii) *$Res(f,g) = 0$ si et seulement si $f(X)$ et $g(X)$ ont un pgcd non constant dans $K[X]$*

(iv) $Res(g,f) = (-1)^{mn} Res(f,g)$

(v) $Res(f,g) = a^n \prod_{1 \leqslant i \leqslant m} g(a_i)$

(vi) *Si $f(x)$ et $g(x)$ sont non constants et si $r(X)$ est le reste de la division euclidienne de $f(X)$ par $g(X)$, $Res(f,g) = (-1)^{mn} b^{(m-deg(r))} Res(g,r)$*

(vii) $Res(f, g_1 g_2) = Res(f,g_1) Res(f,g_2)$.

B - Discriminant d'un polynôme

Soient K un corps, $\overline{K}$ une clôture algébrique de K et $f(X) \in K[X]$ un polynôme non nul, de coefficient dominant a. Le ***discriminant*** de $f(X)$ est l'expression

$$D(f) = \frac{(-1)^{\frac{n(n-1)}{2}} Res(f, f')}{a}$$

où f' est le polynôme dérivé de f.

2. *Montrer que $D(aX^2 + bX + c) = b^2 - 4ac$, $D(X^3 + pX + q) = -4p^3 - 27q^2$ et que si $f(X) = a \prod\limits_{1 \leqslant i \leqslant n} (X - a_i)$, alors $D(f) = a^{(2n-2)} \prod\limits_{1 \leqslant i < j \leqslant n} (a_i - a_j)^2$.*

3. *Montrer que $D(f) = 0$ si et seulement si le polynôme $f(X)$ a une racine d'ordre de multiplicité supérieur ou égal à 2 dans $\overline{K}$.*

4. *Montrer que $D(X^{n-1} + X^{n-2} + \ldots + 1) = (-1)^{\frac{(n-1)(n-2)}{2}} n^{(n-2)}$.* (Utiliser (1.v).)

♣ TR.VIII.D. Algèbres - Algèbres de polynômes

Soient K un corps commutatif et $K[X]$ l'anneau de polynômes en une indéterminée, à coefficients dans K. Il est évident que la multiplication des polynômes par les constantes de K et l'addition des polynômes munissent $K[X]$ d'une structure de K-espace vectoriel. De plus, la loi externe de K sur $K[X]$ et la multiplication dans $K[X]$ vérifient la condition

$$\forall k \in K, \forall P,\ Q \in K[X],\ (kP)Q = P(kQ) = k(PQ).$$

On a donc la situation suivante : un corps commutatif K, un ensemble $A(= K[X])$, une loi externe de K sur A, deux lois internes sur A, notées $+$ et $.$, telles que

– la loi externe et $+$ munissent A d'une structure de K-espace vectoriel ;

– la loi $+$ est distributive par rapport à la loi $.$;

– la loi externe et la loi $.$ vérifient la condition de compatibilité

$$\forall k \in K,\ \forall x, y \in A,\ (kx).y = x.(ky) = k(x.y).$$

Dans le cas de $K[X]$, on a, de plus, que la loi $.$ est associative, commutative, possède un élément unité.

On formalise cette nouvelle structure de la façon suivante.

Soit K un corps commutatif, une K-***algèbre*** A est la donnée d'un K-espace vectoriel A et d'une application K-bilinéaire

$$f : A \times A \longrightarrow A.$$

La K-algèbre A est dite ***associative*** si l'application f vérifie la condition
(1) $\forall x, y, z \in A,\ f(f(x, y), z) = f(x, f(y, z))$.

La K-algèbre A est dite ***commutative*** si l'application f vérifie la condition
(2) $\forall x, y \in A,\ f(x, y) = f(y, x)$.

La K-algèbre A est dite ***unitaire*** s'il existe un élément $1 \in A$ vérifiant la condition
(3) $\forall x \in A,\ f(1, x) = f(x, 1) = x$.

1. *On suppose que A est une K-algèbre et on pose $f(x, y) = xy$. Montrer que la bilinéarité de l'application f se traduit alors par la distributivité de la somme par rapport au produit et par la compatibilité de la loi externe et du produit. Montrer que si la K-algèbre A est associative et unitaire, A a une structure d'anneau compatible avec sa structure de K-espace vectoriel. Tester ces affirmations avec $A = K[X]$.*

Ceci montre qu'on peut toujours considérer qu'une K-algèbre associative et unitaire est un anneau muni d'une structure de K-espace vectoriel, ces deux structures étant compatibles.

Algèbre d'un groupe

Soient K un corps commutatif et G un groupe. On pose

$$K(G) = \left\{ \sum_{g \in G} a_g g \,|\, a_g \in K,\ a_g = 0 \text{ sauf pour un nombre fini de } g \right\}.$$

On définit sur $K(G)$ deux opérations internes, somme et produit, par

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}(a_g + b_g)g$$

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g'\in G} b_{g'} g'\right) = \sum_{g,g'\in G} a_g b_{g'} gg'$$

et une opération externe de K sur $K(G)$ définie par

$$\lambda\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} \lambda a_g g, \quad \lambda \in K.$$

2. *Montrer que, muni de ces opérations, $K(G)$ est une K-algèbre.*

On remarquera que la structure de K-algèbre définie ci-dessus ne fait pas intervenir le fait que tout élément de G admet un inverse. On peut donc étendre la définition de cette K-algèbre au cas où G est un monoïde.

Ce qui précède permet de définir la notion de polynôme en un nombre quelconque de variables, de la façon suivante.

Soit S un ensemble ; on considère l'ensemble

$$\mathbb{N}(S) = \{f : S \longrightarrow \mathbb{N} \mid f(s) = 0 \text{ sauf pour un nombre fini de } s \in S\}.$$

On définit sur $\mathbb{N}(S)$ une opération interne, notée multiplicativement, par $(fg)(s) = f(s) + g(s)$.

3. *Montrer que, muni de cette loi, $\mathbb{N}(S)$ est un monoïde, dont l'élément neutre est l'application nulle.*

4. *Montrer que tout élément f de $\mathbb{N}(S)$ s'écrit, de manière unique, $\prod_{s\in S} s^{\mu(s)}$, avec $\mu(s) = 0$ sauf pour un nombre fini de s, où $\mu(s) \in \mathbb{N}$ et s^n est l'application de S dans $\mathbb{N}$ définie par $s^n(x) = 0$ si $x \neq s$ et $s^n(s) = n$.*

Soit K un corps commutatif ; on appelle ***anneau de polynômes en*** S, à coefficients dans K, l'algèbre $K(\mathbb{N}(S))$, que l'on notera $K[S]$ dans la suite.

5. *Montrer que si $card(S) = n$, l'anneau $K[S]$ est isomorphe à l'anneau $K[X_1, \ldots, X_n]$.*

6. *Montrer que tout élément de $K[S]$ s'écrit, de manière unique,*

$$\sum_{\mu\in\mathbb{N}(S)} a_{(\mu)} \prod_{s\in S} s^{\mu(s)}$$

avec les $a_{(\mu)} \in K$ nuls sauf pour un nombre fini de μ et les $\mu(s)$ nuls sauf pour un nombre fini de s.

TRAVAUX PRATIQUES

TP.VIII. Entiers de Gauss et sommes de deux carrés

Les anneaux des entiers des corps de nombres constituent, avec les anneaux de polynômes, les deux grands types d'anneaux qui intéressent particulièrement les arithméticiens. Un exemple est l'anneau $\mathbb{Z}[i] \subset \mathbb{C}$ des entiers de Gauss, constitué des nombres complexes à coordonnées entières. Son corps des fractions est $\mathbb{Q}(i) \subset \mathbb{C}$, qui est le $\mathbb{Q}$-espace vectoriel de base $\{1, i\}$, et $\mathbb{Z}[i]$ joue pour le corps de nombres $\mathbb{Q}(i)$ le même rôle que joue $\mathbb{Z}$ pour $\mathbb{Q}$. Pour déterminer les inversibles de l'anneau $\mathbb{Z}[i]$, on introduit la norme N définie par $N(a+ib) = a^2 + b^2$. C'est aussi le produit $z\bar{z}$, où $z = a + ib$, d'où résulte la multiplicativité de la norme : $N(zz') = N(z)N(z')$. Il est alors facile de voir que les unités sont $\mathbb{U}(\mathbb{Z}[i]) = \{z, N(z) = 1\} = \{\pm 1\}$.

Dans $\mathbb{Q}[x]$, étant donné deux polynômes f et g non nuls, il existe un unique couple (q, r) de polynômes tels que $f = gq + r$. L'existence de cette division euclidienne implique la principalité de $\mathbb{Q}[x]$. Nous allons voir que $\mathbb{Z}[i]$ possède également un algorithme euclidien, d'où résultent les propriétés arithmétiques de l'anneau. Il est alors possible de décomposer tout élément de $\mathbb{Z}[i]$ en produit d'irréductibles et cette décomposition est unique (à permutation près des facteurs) si l'on choisit un système de représentants des irréductibles (modulo les inversibles).

L'anneau $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[i]$ et l'on peut se demander quand est-ce qu'un irréductible de $\mathbb{Z}$ reste irréductible dans $\mathbb{Z}[i]$ ou, au contraire, se décompose : par exemple, $5 = 2^2 + 1^2 = (2+i)(2-i)$. La décomposition d'un nombre premier de $\mathbb{Z}$ est liée à son écriture en somme de deux carrés :

Proposition 1. *Si p est un nombre premier vérifiant $p \equiv 1 \mod 4$ ou $p = 2$, alors il existe des entiers naturels x et y tels que $p = x^2 + y^2 = (x+iy)(x-iy)$. Si par contre $p \equiv -1 \mod 4$ alors p reste irréductible dans $\mathbb{Z}[i]$ et cette équation n'admet pas de solution en entiers.*

On en déduit facilement :

***Proposition* 2.** *Les irréductibles de $\mathbb{Z}[i]$ sont les nombres premiers p tels que $p \equiv -1 \mod 4$ et les éléments de norme première.*

(Décomposer $N(z) \in \mathbb{N}$ en irréductibles.) Il en résulte également :

***Théorème* 1.** *Un entier naturel n est somme de deux carrés d'entiers naturels si et seulement si l'exposant de p dans la décomposition en produit d'irréductibles dans $\mathbb{Z}$ est pair pour tout nombre premier $p \equiv -1 \mod 4$.*

Vous verrez par contre au cours du TR.IX.B que tout nombre entier naturel est somme de quatre carrés d'entiers naturels (théorème obtenu en travaillant dans l'anneau non commutatif des quaternions de Hurwitz).

Le but de ce TP est de donner une preuve constructive de la première assertion de la proposition 1 et d'écrire la décomposition en irréductibles sur quelques exemples (le cas général pouvant bien sûr être implémenté en machine par un étudiant qui est à l'aise avec la programmation en Maple). On implémentera un algorithme efficace qui fournit une écriture $p = x^2 + y^2$ et est particulièrement intéressant compte tenu des notions algébriques utilisées.

Division euclidienne dans $\mathbb{Z}[i]$

Comme Maple connaît i (tester `(2+3*I)/(1-I);`), les opérations dans $\mathbb{Z}[i]$ sont directement accessibles par l'utilisateur, un élément de $\mathbb{Z}[i]$ étant vu comme un nombre complexe.

☞ *Quelques commandes* Maple *utiles :* `round, isprime`.

1. Écrire une procedure `znorm` qui calcule la norme d'un élément de $\mathbb{Z}[i]$.

2. Justifier l'assertion faite dans l'introduction sur $\mathbb{U}(\mathbb{Z}[i])$ puis écrire une procédure `znormalize` qui renvoie l'unique représentant de la classe d'un élément de $\mathbb{Z}[i]$ (donné en entrée) modulo les inversibles qui soit dans le premier quadrant (*i.e.*, outre 0, les éléments de la forme $a + bi$ où $a > 0$ et $b \geqslant 0$). Ce sera notre choix de normalisation des irréductibles.

3. Soient a et b deux entiers de Gauss non nuls ; démontrer qu'il existe un couple (q, r) d'éléments de $\mathbb{Z}[i]$ tels que $a = bq + r$ avec $N(r) < N(b)$. (On remarquera que c'est équivalent à trouver $q = x + iy$ tel que $N(a/b - q) < 1$: il suffit donc de poser $a/b = r + is \in \mathbb{Q}(i)$ et prendre pour x et y l'entier le plus proche de r et s respectivement.) En déduire un algorithme de division euclidienne dans

$\mathbb{Z}[i]$ qui sera représenté par une fonction `zdiv` prenant en entrée deux éléments de $\mathbb{Z}[i]$ et qui renvoie un vecteur à deux éléments représentant respectivement le quotient et le reste de la division euclidienne. Tester votre procédure sur les couples $(7+i, 4+3i)$ et $(4+3i, 1+i)$.

4. En mimant l'algorithme classique du pgcd, écrire une procédure `zgcd` qui renvoie le pgcd, normalisé *via* `znormalize`, de deux éléments de $\mathbb{Z}[i]$.

5. Démontrer la propostion 2 (à partir de la proposition 1), puis écrire une procédure `iszprime` renvoyant *true* si l'entier de Gauss donné est premier et *false* sinon. À l'aide de vos procédures, donner (aux inversibles près, *i.e.* en se limitant au premier quadrant) la liste de tous les éléments premiers de $\mathbb{Z}[i]$ de norme inférieure ou égale à 25. En déduire la factorisation des éléments 2, $7+i$, $4+3i$, $5+3i$ et $7+2i$.

La stratégie

Nous allons associer à un nombre premier p (de la forme $4k+1$) un élément premier x_p de $\mathbb{Z}[i]$ tel que $N(x_p) = p$. Pour cela, nous allons faire apparaître x_p comme un générateur d'un idéal premier $\mathfrak{p}$ de $\mathbb{Z}[i]$. En effet, l'anneau $\mathbb{Z}[i]$ est principal. Donc tout idéal premier est principal, et les idéaux premiers non-nuls sont maximaux. Un générateur d'un idéal premier est un élément premier de $\mathbb{Z}[i]$.

Procédons par analyse et synthèse : supposons que $p = N(x_p) = x_p\bar{x_p}$. On vérifie facilement que si $p \neq 2$ alors x_p et $\bar{x_p}$ ne sont pas associés dans $\mathbb{Z}[i]$. Il en résulte un isomorphisme d'anneaux :

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[i]/(x_p) \times \mathbb{Z}[i]/(\bar{x_p}),$$

d'après le théorème chinois. Poursuivons : d'une part, $\mathbb{Z}[i]/(p)$ est de cardinal p^2 (car isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ en tant que groupe abélien) ; d'autre part, les quotients $\mathbb{Z}[i]/(x_p)$ et $\mathbb{Z}[i]/(\bar{x_p})$ sont deux corps car les idéaux premiers (x_p) et $(\bar{x_p})$ sont maximaux. Nécessairement, $\mathbb{Z}[i]/(x_p)$ est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Autrement dit, la projection canonique $\mathbb{Z}[i] \to \mathbb{Z}[i]/(x_p)$ fournit un morphisme d'anneaux $\mathbb{Z}[i] \to \mathbb{F}_p$, de noyau (x_p).

Cela nous amène à construire l'idéal $\mathfrak{p}$ comme le noyau d'un morphisme d'anneaux $f : \mathbb{Z}[i] \to \mathbb{F}_p$. Noter déjà que, puisque $\mathbb{F}_p$ est un corps (donc intègre), le noyau de ce morphisme d'anneaux sera un idéal maximal (donc premier). Un tel morphisme est entièrement caractérisé par l'image de 1 et de i. Néanmoins, étant un morphisme d'anneaux, nous avons nécessairement $f(1) = 1$, et par suite ce morphisme est déterminé par $f(i)$. Or, i est un élément d'ordre 4 dans $\mathbb{U}(\mathbb{Z}[i])$. Il ne peut donc s'envoyer que sur un élément d'ordre 4 de $\mathbb{F}_p^\times$. Ensuite, on obtiendra notre générateur par l'algorithme euclidien de $\mathbb{Z}[i]$.

Cela permet de mettre en évidence les deux ingrédients techniques dont nous aurons besoin :

- la division euclidienne dans $\mathbb{Z}[i]$, déjà implémentée ;
- trouver un élément d'ordre 4 dans $\mathbb{Z}/p\mathbb{Z}$, p étant un nombre premier de la forme $4k+1$.

Enfin, le travail de synthèse consiste à démontrer que x_p ainsi construit est bien de norme p. Ce sera fait en fin de TP.

Élément d'ordre 4 dans $\mathbb{Z}/p\mathbb{Z}$

L'idée est la suivante : *Si p est un nombre premier de la forme $4k+1$, alors en prenant « au hasard » un élément a de $\mathbb{F}_p^*$, il y a de « grande chance » que a^k soit un élément d'ordre 4.*

6. Tester expérimentalement la stratégie proposée en prenant (« au hasard ») des $p \leqslant 1000$ de la forme désirée.

Remarque technique : Pour tirer des nombres « au hasard », on pourra utiliser la fonction

```
RandomTools[Generate](integer(range=m..n))
```

qui renvoie un nombre entre deux entiers m et n. Par exemple, la procédure suivante renvoie un nombre premier pseudo-aléatoire compris entre 3 et n :

```
> randprime:=proc(n);
  RETURN(prevprime(RandomTools[Generate](integer(range=5..n+1))));
  end;
```

7. À partir de vos tests, combien de a faut-il choisir en moyenne pour être sûr d'en avoir un « bon ». Donner des arguments théoriques pour valider vos résultats expérimentaux. (Remarquer que a^k est d'ordre 4 si et seulement si $a^{\frac{p-1}{2}} = -1$; considérer alors l'endomorphisme $x \mapsto x^{\frac{p-1}{2}}$ de $\mathbb{F}_p^*$.)

8. En déduire une procédure `ordre4` qui, étant donné en entrée un nombre premier p de la forme $4k+1$, renvoie un entier c, avec $|c| < p/2$, et tel que sa classe dans $\mathbb{F}_p$ soit un élément d'ordre 4.

Décomposition de p en somme de deux carrés

9. Soit c un élément de $\mathbb{Z}$, tel que $|c| < p/2$ et que sa classe modulo p soit d'ordre 4 dans $\mathbb{F}_p^*$. On considère le morphisme d'anneaux $f : \mathbb{Z}[i] \to \mathbb{F}_p$ défini par $f(1) = 1$ et $f(i) = c \mod p$. Vérifier que c'est bien un morphisme d'anneaux. Montrer que le noyau de f est engendré (en tant que groupe abélien, donc en tant qu'idéal) par p et $i - c$. En déduire, par l'algorithme d'Euclide du calcul du pgcd dans $\mathbb{Z}[i]$, un générateur du noyau de f. Que prend-on comme entiers a et b de façon à avoir $p = a^2 + b^2$?

10. En combinant l'ensemble de votre travail précédent, écrire une procédure `DeuxCarres`, qui prend en entrée un nombre premier p et qui renvoie un couple (a, b) tel que $p = a^2 + b^2$ si p est de la forme $4k + 1$.

11. Question subsidiaire : proposer un algorithme, utilisant la procédure précédente, qui décompose en irréductibles un entier de Gauss quelconque donné.

Remarque. Pour achever la preuve de la proposition 1, il reste à démontrer que si $p \equiv -1 \mod 4$ alors p reste irréductible dans $\mathbb{Z}[i]$ (il ne s'écrit donc pas comme somme de deux carrés). On démontre la contraposée : si p est réductible, il s'écrit $p = \alpha\beta$ ($\alpha \notin \mathbb{U}(\mathbb{Z}[i])$, $\beta \notin \mathbb{U}(\mathbb{Z}[i])$), d'où $N(p) = p^2 = N(\alpha)N(\beta)$. Comme α et β ne sont pas de norme 1, alors $p = N(\alpha)$. Écrivant $\alpha = a + ib$, on obtient $p = a^2 + b^2$, d'où $-b^2 \equiv a^2 \mod p$. On vérifie facilement que p ne divise pas b, donc b est inversible modulo p. La congruence précédente montre alors que -1 est un carré modulo p. Comme les carrés (non nuls) modulo p forment un groupe de cardinal $(p-1)/2$ (c'est l'image de l'endomorphisme $x \mapsto x^2$ de $\mathbb{F}_p^*$), on a $(-1)^{\frac{p-1}{2}} = 1$, ce qui est équivalent à $p \equiv 1 \mod 4$.

Dans la même veine, on peut fournir une preuve, non constructive par contre (à la différence de l'algorithme décrit plus haut), du fait que $p \equiv 1 \mod 4$ s'écrit comme somme de deux carrés : comme -1 est un carré modulo p (les carrés non nuls modulo p sont exactement le noyau de l'endomorphisme $x \mapsto x^{\frac{p-1}{2}}$ de $\mathbb{F}_p^*$), disons $-1 \equiv a^2 \mod p$, le nombre p divise $a^2+1 = (a+i)(a-i)$, mais il ne divise ni $a + i$, ni $a - i$. Il n'est donc pas premier dans $\mathbb{Z}[i]$, donc pas irréductible (c'est une propriété des anneaux principaux). Or on vient de voir qu'il s'écrit alors sous la forme $p = a^2 + b^2$.

This page intentionally left blank

IX

GÉNÉRALITÉS SUR LES EXTENSIONS DE CORPS

Il est bien connu qu'un polynôme $f(X)$ du second degré, à coefficients dans $\mathbb{R}$, dont le discriminant est négatif n'admet pas de racine dans $\mathbb{R}$ mais dans $\mathbb{C}$. Pour résoudre l'équation $f(X) = 0$ on est donc amené à considérer $\mathbb{R}$ comme un sous-corps de $\mathbb{C}$: on dit que $\mathbb{C}$ est une **extension** de $\mathbb{R}$. De manière générale, la théorie des extensions de corps a pour objet de répondre aux questions suivantes :

- Étant donnés un corps K et $f(X)$ un polynôme de $K[X]$, peut-on trouver un corps L dont K soit un sous-corps et dans lequel on puisse résoudre l'équation $f(X) = 0$?
- Étant donné un corps K, peut-on trouver un corps E dont K soit sous-corps et dans lequel on puisse résoudre les équations $f(X) = 0$, pour tous les polynômes $f(X)$ de $K[X]$?

Bien entendu, les propriétés du corps K entrent en jeu, en particulier sa **caractéristique**. Celle-ci caractérise un sous-corps de K, son sous-corps **premier**, dont K est une extension. Ce sous-corps premier est soit isomorphe à $\mathbb{Q}$, soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier, de sorte que tout corps est extension de $\mathbb{Q}$ ou de $\mathbb{Z}/p\mathbb{Z}$.

IX.1. Corps premiers – Caractéristique d'un corps

Définition* IX.1.1.** On dit qu'un sous-ensemble k d'un corps K est un ***sous-corps de K s'il est stable pour les opérations de K et si, muni des opérations induites par celles de K, c'est un corps.

Proposition IX.1.1. *Un sous-ensemble k d'un corps K est un sous-corps de K si c'est un sous-anneau de K stable par inverse.* □

Il est clair qu'une intersection de sous-corps d'un corps K est un sous-corps de K.

Définition IX.1.2. Un corps est dit **premier** s'il ne contient aucun sous-corps distinct de lui-même.

Proposition IX.1.2. *Tout corps K contient un sous-corps premier et un seul.*

Démonstration. C'est l'intersection de tous les sous-corps de K. □

Notons 1_A l'élément unité d'un anneau A et considérons le morphisme d'anneaux $\varphi : \mathbb{Z} \longrightarrow A$ défini par $\varphi(1) = 1_A$, *i.e.* $\varphi(n) = n1_A$. Le noyau $Ker(\varphi)$ de ce morphisme est un idéal de $\mathbb{Z}$, on a donc $Ker(\varphi) = (p)$, avec $p \geqslant 0$.

Définition IX.1.3. L'entier p positif ou nul ainsi défini s'appelle la **caractéristique** de A.

Théorème IX.1.1.

(i) *La caractéristique d'un corps est nulle ou est un nombre premier.*

(ii) *Si K est un corps de caractéristique nulle, son sous-corps premier est isomorphe à $\mathbb{Q}$.*

(iii) *Si K est un corps de caractéristique $p > 0$, son sous-corps premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Soit K un corps : si $p \neq 0$, alors $Im(\varphi) \simeq \mathbb{Z}/(p)$ est un sous-anneau de K, donc intègre. Par conséquent, l'idéal (p) est premier, *i.e.* p est un nombre premier.

Puisque le sous-anneau $Im(\varphi)$ de K est engendré par 1_K, il est contenu dans tout sous-corps de K, en particulier dans le sous-corps premier de K. Par conséquent, le sous-corps premier de K est le corps des fractions de $Im(\varphi)$. Si $p = 0$, $Im(\varphi) \simeq \mathbb{Z}$ et le sous-corps premier de K est isomorphe à $\mathbb{Q}$. Si $p > 0$, alors p est un nombre premier et $Im(\varphi) \simeq \mathbb{Z}/p\mathbb{Z}$ est un corps. □

Proposition IX.1.3. *Soit K un corps de caractéristique $p > 0$.*

(i) *L'application $x \longmapsto x^p$ est un isomorphisme de K sur un de ses sous-corps.*

(ii) *Pour tout entier $n \geqslant 0$, l'application $x \longmapsto x^{p^n}$ est un isomorphisme de K sur un de ses sous-corps.*

Démonstration. Notons φ l'application définie sur K par $\varphi(x) = x^p$. On a $\varphi(xy) = \varphi(x)\varphi(y)$. L'égalité $\varphi(x+y) = \varphi(x) + \varphi(y)$, *i.e.* $(x+y)^p = x^p + y^p$, est une conséquence de la formule du binôme et du fait que p étant premier, C_p^k, $0 < k < p$, est divisible par p. Donc φ est un morphisme d'anneaux de K dans K. Il est injectif, donc bijectif sur son image.

On déduit (ii) de (i) par récurrence sur n. □

Le morphisme défini dans la proposition (IX.1.3.(i)) joue un grand rôle dans l'étude des corps finis et, plus généralement, dans l'étude des corps de caractéristique $p > 0$ (*cf.* TR.IX.A et chapitre XV). C'est le morphisme de ***Frobenius***.

Remarques IX.1.1.

a) On déduit de la définition (IX.1.3) que si un anneau A est de caractéristique $p > 0$, p est le plus petit entier positif tel que, pour tout élément a de A, on ait $pa = 0$.

b) On déduit de la proposition (IX.1.3) que si K est un corps de caractéristique $p > 0$, alors pour tout entier $n > 0$, on a, dans K, l'identité :

$$\left(\sum_{i=1}^{q} x_i\right)^{p^n} = \sum_{i=1}^{q} x_i^{p^n}.$$

c) D'après le théorème (IX.1.1), un corps de caractéristique nulle est infini et un corps fini a une caractéristique $p > 0$.

d) D'après le théorème (IX.1.1), si k et K sont des corps tels que $k \subset K$, ils ont même caractéristique (puisqu'ils ont même sous-corps premier).

Attention. *Les réciproques de c) sont fausses.* (Considérer le corps $(\mathbb{Z}/p\mathbb{Z})(X)$ des fractions rationnelles à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier.)

IX.2. Extensions

Définition IX.2.1. Une **extension** d'un corps K est la donnée d'un corps E et d'un morphisme de corps $i : K \longrightarrow E$.

Un morphisme de corps étant nécessairement injectif, on peut identifier le corps K avec le sous-corps $i(K)$ de E. Dans la suite, cette identification sera toujours supposée faite (sauf mention explicite du contraire) et on considérera

qu'une extension d'un corps K est la donnée d'un corps E contenant K comme sous-corps.

Notation. Une extension E de K sera notée E/K, ou $K \subset E$, ou $K \hookrightarrow E$.

***Exemples* IX.2.1.**

a) Le corps des nombres complexes $\mathbb{C}$ est une extension du corps des nombres réels $\mathbb{R}$.

b) $\mathbb{C}$ et $\mathbb{R}$ sont des extensions de $\mathbb{Q}$. Plus généralement, tout corps est une extension de son sous-corps premier.

c) $E = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ est une extension de $\mathbb{Q}$.

d) Pour tout corps K, le corps $K(X)$ des fractions rationnelles à coefficients dans K est une extension de K.

Soit E une extension d'un corps K. Il est clair que les opérations de E induisent sur E une structure de K-espace vectoriel. Plus précisément, E est une K-algèbre (*cf.* TR.VIII.D).

***Définition* IX.2.2.** Si E/K est une extension, on appelle **degré** de cette extension la dimension du K-espace vectoriel E. Si $\dim_K E = +\infty$, on dit que E est une **extension infinie** de K ; si $\dim_K E$ est finie, on dit que E est une **extension finie** de K et on pose $[E : K] = \dim_K E$.

***Exemples* IX.2.2.**

a) Si E/K est une extension telle que $[E : K] = 1$, alors $E = K$.

b) $[\mathbb{C} : \mathbb{R}] = 2$.

c) $\mathbb{R}$ est une extension infinie de $\mathbb{Q}$, puisque $\mathbb{Q}$ est dénombrable et que $\mathbb{R}$ ne l'est pas.

***Exercice* IX.1.** Soient K un corps et A un anneau intègre contenant K, de dimension finie en tant que K-espace vectoriel. Montrer que A est un corps. (On montrera que, pour tout élément non nul $a \in A$, la multiplication par a est une application K-linéaire bijective de A dans A et on en déduira que a est inversible dans A.)

***Proposition* IX.2.1.** *Soient E/K et F/E des extensions. Si l'un des nombres $[F : K]$ ou $[F : E][E : K]$ est fini, il en est de même pour l'autre et ils sont égaux.*

Démonstration. Soient $(e_i)_{i\in I}$ une K-base de E et $(f_j)_{j\in J}$ une E-base de F. On vérifie qu'alors $(e_i f_j)_{(i,j)\in I\times J}$ est une K-base de F. □

Corollaire IX.2.1. *Si F/K est une extension finie et si E est un corps tel que $K \subset E \subset F$, alors $[E : K]$ et $[F : E]$ sont des diviseurs de $[F : K]$.* □

Remarque IX.2.1. On en déduit que si F/K est une extension finie telle que $[F : K]$ soit un nombre premier, il ne peut exister de corps intermédiaire entre K et F.

Attention. *On prendra garde au fait que si $[F : K]$ n'est pas premier, il n'existe pas nécessairement de corps intermédiaire entre K et F. On trouvera un exemple de cette situation à l'exercice XVI.2 du chapitre XVI.*

Exercice IX.2. *Soient E/K une extension de degré fini et F_1, F_2 des corps intermédiaires, $K \subset F_i \subset E$, $i = 1, 2$. Montrer que si les nombres $[F_1 : K]$ et $[F_2 : K]$ sont premiers entre eux, alors $F_1 \cap F_2 = K$.*

Définition - Proposition IX.2.2. *Soient E un corps et Y un sous-ensemble de E. Le sous-corps de E engendré par Y est le plus petit sous-corps de E contenant Y. C'est l'intersection de tous les sous-corps de E contenant Y.* □

Définition IX.2.3. Soient E/K une extension et A un sous-ensemble de E. Le sous-corps de E engendré par $K \cup A$ est dit obtenu par ***adjonction*** de A à K et est noté $K(A)$.

Exemple IX.2.3. Si $E = \mathbb{R}$, $K = \mathbb{Q}$, $A = \{\sqrt{2}\}$, alors $K(A) = \mathbb{Q}(\sqrt{2})$.

Exercice IX.3. *Avec les notations ci-dessus, montrer que $K(A)$ est le corps des fractions de la sous-algèbre $K[A]$ de E, engendrée par K et A.* (Indication : on rappelle que, en posant $A = \{a_i\}_{i\in I}$, $K[A]$ est l'anneau des polynômes en les indéterminées a_i, $i \in I$ (TR.VIII.D), et utiliser la propriété universelle du corps des fractions d'un anneau intègre, *cf.* VIII.5.)

Définition IX.2.4.

a) Avec les notations ci-dessus, les éléments de A sont appelés des **générateurs** de $K(A)$ sur K.

b) On dit qu'une extension E/K est de **type fini** si elle possède un système fini de générateurs.

c) On dit qu'une extension E/K est **monogène** si elle possède un système de générateurs réduit à un élément. Cet élément est alors appelé **primitif**.

Remarque IX.2.2. Une extension finie est de type fini. Mais la réciproque est fausse. Par exemple, le corps $K(X)$ des fractions rationnelles à coefficients dans K est une extension de type fini de K, mais n'est pas une extension finie. Plus généralement, *cf.* remarque (XI.2.1). Par contre, on a le résultat suivant :

Proposition IX.2.3. *Si E/K est une extension telle que $[E : K]$ soit un nombre premier, alors l'extension est monogène.*

Démonstration. Soit $\alpha \in E \setminus K$; alors $K(\alpha)$ est un corps intermédiaire entre K et E. D'après la remarque (IX.2.1), on a $K(\alpha) = K$ ou $K(\alpha) = E$. Mais puisque l'élément α n'est pas dans K, on ne peut avoir $K(\alpha) = K$. On en déduit que $K(\alpha) = E$. □

On remarque donc que si E/K est une extension telle que $[E : K]$ soit un nombre premier, tout élément de $E \setminus K$ est primitif.

Exercice IX.4. *Soient K un corps et L/K une extension. Montrer que si E_1 et E_2 sont deux corps intermédiaires, $K \subset E_i \subset L$, $i = 1, 2$, il existe un corps intermédiaire maximal parmi ceux contenus dans E_1 et E_2 et un corps intermédiaire minimal parmi ceux contenant E_1 et E_2.* (On montrera que ce sont, respectivement, $E_1 \cap E_2$ et $K(E_1 \cup E_2)$.)

THÈMES DE RÉFLEXION

♡ TR.IX.A. Corps finis

Les corps finis seront étudiés en détail au chapitre XV. Nous allons ici établir quelques propriétés élémentaires, mais fondamentales.

Nous allons d'abord montrer la propriété suivante :

Soient K un corps et K^* le groupe multiplicatif des éléments non nuls de K ; tout sous-groupe fini G de K^* est cyclique, formé de racines de l'unité (*cf.* XV.1).

On rappelle (exercice VI.6) qu'il existe un élément x de G dont l'ordre n est le *ppcm* des ordres des éléments de G.

1. *En déduire que $|G| \leqslant n$, donc que $G = \{1, x, \ldots, x^{n-1}\}$.*

Dans la suite, F est un corps fini à q éléments, de caractéristique $p > 0$. Son sous-corps premier est donc $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

2. *Montrer qu'il existe un entier $n \geqslant 1$ tel que $q = p^n$.*

3. *Montrer que le groupe F^* est cyclique, d'ordre $q - 1$.*

4. *En déduire que pour tout x de F^*, on a $x^{q-1} = 1$ et, pour tout x de F, on a $x^q = x$.*

5. *Soit α un générateur de F^* ; montrer que $F = \mathbb{F}_p(\alpha)$ et que*

$$F = \mathbb{F}_p 1 \oplus \mathbb{F}_p \alpha \oplus \cdots \oplus \mathbb{F}_p \alpha^{n-1}$$

avec $n = [F : \mathbb{F}_p]$.

On considère maintenant un corps K de caractéristique $p > 0$ et $\mathcal{F} : K \longrightarrow K$ le morphisme de Frobenius, $\mathcal{F}(x) = x^p$. D'après la proposition (IX.1.3), c'est un endomorphisme de K.

6. *Montrer que sa restriction à $\mathbb{F}_p$ est l'identité.*

7. *En déduire que pour tout entier $n \in \mathbb{Z}$, on a $n^p \equiv n \, mod(p)$.*

8. *Montrer que si K est un corps fini, $\mathcal{F}$ est un automorphisme.*

9. *En déduire que dans un corps fini de caractéristique p, chaque élément admet une et une seule racine p-ième.*

Nous allons maintenant donner quelques propriétés des ensembles

$$\mathbb{F}_q^2 = \{x \in \mathbb{F}_q | \exists y \in \mathbb{F}_q, x = y^2\}, \quad \mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*,$$

i.e. des éléments qui sont des carrés dans un corps fini, avec $q = p^n$, p premier.

10. *Montrer que si $p = 2$, alors $\mathbb{F}_q^2 = \mathbb{F}_q$ et que si $p > 2$, alors on a $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$.* (Utiliser la suite exacte $1 \longrightarrow \{-1, 1\} \longrightarrow \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^{*2} \longrightarrow 1$. Pour la définition de suite exacte, *cf.* TR.IV.C.)

11. *Montrer que si $p > 2$, alors $x \in \mathbb{F}_q^{*2}$ est équivalent à $x^{\frac{q-1}{2}} = 1$.*

12. *En déduire que, si $p > 2$, $-1 \in \mathbb{F}_q^{*2}$ est équivalent à $q \equiv 1\ mod(4)$.*

♠ TR.IX.B. Corps des quaternions et théorème des quatre carrés

Ce livre est consacré à l'étude des corps commutatifs. Cependant il existe des corps non commutatifs (*i.e.* la multiplication n'est pas commutative) qui, d'après le théorème de Wedderburn (*cf.* chapitre XV), sont nécessairement infinis. Nous allons étudier ici le plus classique d'entre eux, le corps des ***quaternions***.

De plus, cette étude nous permettra de démontrer le théorème suivant :

***Théorème* (des quatre carrés).** *Tout nombre entier naturel est somme de quatre carrés de nombres entiers naturels.*

On désigne par $\mathbb{H}$ l'espace vectoriel $\mathbb{R}^4$, dont on note $\{e, i, j, k\}$ la base canonique, muni de la structure de $\mathbb{R}$-algèbre définie, par linéarité, à partir de la table de multiplication suivante :

$$ee = e, \quad ei = ie = i, \quad ej = je = j, \quad ek = ke = k, \quad i^2 = j^2 = k^2 = -e,$$

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

1. *Vérifier que la multiplication ainsi définie sur $\mathbb{H}$ est associative.*

Un élément de $\mathbb{H}$ est appelé un ***quaternion***. Il s'écrit, de manière unique, $ae + bi + cj + dk$, avec $a, b, c, d \in \mathbb{R}$. Un tel quaternion avec $a = 0$ est appelé un ***quaternion pur***. On note $\mathbb{H}_p$ l'ensemble des quaternions purs.

2. *Vérifier que $\mathbb{H}_p$ est un $\mathbb{R}$-espace vectoriel.*

Soit $z = ae + bi + cj + dk$ un quaternion ; le quaternion ***conjugué*** de z est $\overline{z} = ae - bi - cj - dk$. La ***norme*** de z est le nombre réel $N(z) = z\overline{z} = a^2 + b^2 + c^2 + d^2$.

3. *Montrer que pour tous quaternions z, z', on a $N(zz') = N(z)N(z')$. En déduire que l'ensemble des éléments de $\mathbb{R}$ qui sont sommes de quatre carrés est stable par multiplication.*

4. *Montrer que tout quaternion non nul z admet pour inverse $N(z)^{-1}\overline{z}$. En déduire que $\mathbb{H}$ est un corps non commutatif.*

5. *Soit z un quaternion pur. Montrer que $N(z) = 1$ si et seulement si $z^2 = -1$.*

Deux quaternions purs $z = bi + cj + dk$ et $z' = b'i + c'j + d'k$ sont dits ***orthogonaux*** si $bb' + cc' + dd' = 0$. Autrement dit, les vecteurs (b, c, d) et (b', c', d') de $\mathbb{R}^3$ sont orthogonaux pour le produit scalaire usuel de $\mathbb{R}^3$.

6. *Soient z et z' deux quaternions purs orthogonaux. Montrer que zz' est un quaternion pur orthogonal à z et z'.*

7. *Soit ϵ_1 un quaternion pur de norme 1. Montrer qu'il existe un quaternion pur ϵ_2 orthogonal à ϵ_1 et de norme 1.*

8. *On pose $\epsilon_3 = \epsilon_1\epsilon_2$. Montrer que $(\epsilon_1, \epsilon_2, \epsilon_3)$ est une base de $\mathbb{H}_p$.*

Pour $\alpha \in \mathbb{R}$ et $z \in \mathbb{H}_p$, on pose

$$u_\alpha(z) = (cos(\alpha/2) + \epsilon_1 sin(\alpha/2))z(cos(\alpha/2) - \epsilon_1 sin(\alpha/2)).$$

9. *Montrer que u_α est une application $\mathbb{R}$-linéaire de $\mathbb{H}_p$ dans $\mathbb{H}_p$.*

10. *Calculer les coordonnées de $u_\alpha(z)$ en fonction des coordonnées de z dans la base $(\epsilon_1, \epsilon_2, \epsilon_3)$.*

11. *Interpréter u_α comme la rotation d'angle α et de vecteur directeur ϵ_1.*

12. *Pour un quaternion $z = ae + bi + cj + dk$, on note $v(z)$ le vecteur (b, c, d) de $\mathbb{R}^3$ et on écrit $z = ae + v(z)$. Calculer le produit $(ae + v(z))(a'e + v(z'))$ en fonction de $a, a', v(z), v(z')$, du produit scalaire et du produit vectoriel de $v(z)$ et $v(z')$.*

Si A est un anneau commutatif, un A-***module*** E est la donnée d'un groupe abélien $(E, +)$ muni d'une opération externe $A \times E \longrightarrow E$, ces deux lois satisfaisant aux mêmes axiomes que ceux d'espace vectoriel. L'une des différences fondamentales avec la structure d'espace vectoriel est qu'un A-module E ne possède pas nécessairement de base. S'il en possède une (on dit alors que E est un A-module libre), tout élément de E s'écrit, de manière unique, comme combinaison linéaire finie d'éléments de la base, à coefficients dans A.

Dans la définition des quaternions, on peut remplacer $\mathbb{R}$ par un anneau commutatif A quelconque. Le A-module libre A^4, dont on note $\{e,i,j,k\}$ la base canonique, est muni d'une structure de A-algèbre par les mêmes opérations que ci-dessus. On note $\mathbb{H}(A)$ cette A-algèbre. Il est clair que les notions de conjugué, quaternion pur, norme, définies ci-dessus ont encore un sens dans ce cadre et que pour tout élément $z \in \mathbb{H}(A)$, on a $N(z) \in A$. On en déduit, comme à la question 3, que l'ensemble des éléments de A qui sont sommes de quatre carrés est stable par multiplication. Par conséquent, en prenant $A = \mathbb{Z}$, pour démontrer le théorème des quatre carrés, il suffira de prouver que tout nombre premier est somme de quatre carrés.

Nous allons étudier $\mathbb{H}(\mathbb{Q})$ et son sous-anneau (non commutatif) $\mathbb{H}(\mathbb{Z})$. On note $\mathcal{H}$ l'ensemble des éléments $z \in \mathbb{H}(\mathbb{Q})$, $z = ae+bi+cj+dk$, avec $(a,b,c,d) \in \mathbb{Z}^4$ ou $(a,b,c,d) \in (\frac{1}{2}+\mathbb{Z})^4$. On appelle les éléments de $\mathcal{H}$ les ***quaternions d'Hurwitz***.

13. *Montrer que $\mathcal{H}$ est un sous-anneau de $\mathbb{H}(\mathbb{Q})$ qui contient $\mathbb{H}(\mathbb{Z})$ et qui est stable par passage au conjugué.*

14. *Montrer que pour tout $z \in \mathcal{H}$, on a $z+\overline{z} \in \mathbb{Z}$ et $N(z) \in \mathbb{Z}$.*

15. *Montrer que pour que $z \in \mathcal{H}$ soit inversible, il faut et il suffit que $N(z) = 1$.*

16. *Montrer que pour tout $z \in \mathbb{H}(\mathbb{Q})$, il existe $x \in \mathcal{H}$ tel que $N(x-z) < 1$ (inégalité stricte).* (Soit $z = ae+bi+cj+dk$; il existe $(a',b',c',d') \in \mathbb{Z}^4$ tels que $|a-a'| \leqslant \frac{1}{2}$, $|b-b'| \leqslant \frac{1}{2}$, $|c-c'| \leqslant \frac{1}{2}$, $|d-d'| \leqslant \frac{1}{2}$. Prendre $x = a'e+b'i+c'j+d'k$.)

Pour un anneau non commutatif A, un sous-groupe abélien I de $(A,+)$ est un idéal à gauche (resp. à droite, resp. bilatère) si

$$\forall a \in A,\ \forall x \in I,\ ax \in I, \quad (\text{resp. } xa \in I), \quad (\text{resp. } \forall a,b \in A,\ \forall x \in I,\ axb \in I).$$

Évidemment, si A est un anneau commutatif, ces trois notions coïcident avec celle d'idéal.

17. *Montrer que tout idéal à gauche (resp. à droite) de $\mathcal{H}$ est principal,* i.e. *de la forme $\mathcal{H}z$ (resp. $z\mathcal{H}$).* (Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{H}$: montrer qu'il existe un élément $u \in \mathfrak{a}$ de norme minimale. Montrer que u est inversible. Soient $z \in \mathfrak{a}$ et zu^{-1} : d'après le résultat de la question 16, il existe $x \in \mathcal{H}$ tel que $N(zu^{-1}-x) < 1$. Montrer que $z = xu$.)

Nous allons maintenant démontrer le théorème des quatre carrés pour un nombre premier p. Le théorème est évident si $p = 2$. On peut donc supposer que p est impair.

18. *Montrer que $\mathcal{H}p$ est un idéal bilatère de $\mathcal{H}$ et que l'anneau quotient $\mathcal{H}/\mathcal{H}p$ est isomorphe à $\mathbb{H}(\mathbb{F}_p)$.*

19. *Montrer qu'il existe un élément non trivial* $(a,b,c,d) \in \mathbb{F}_p^4$ *tel que* $a^2+b^2+c^2+d^2=0$. (En prenant $c=1$ et $d=0$, il suffit de montrer que l'équation $b^2+1=-a^2$ a une solution dans $\mathbb{F}_p^2$. En utilisant le TR.IX.A.10, montrer que l'ensemble des éléments de $\mathbb{F}_p$ de la forme b^2+1 (resp. $-a^2$) est de cardinal $\frac{p+1}{2}$. Puisque $\frac{p+1}{2}+\frac{p+1}{2}>p$, en déduire le résultat.)

On en déduit qu'il existe dans $\mathbb{H}(\mathbb{F}_p)$ des éléments non nuls dont la norme est nulle. D'après la question 15, un tel élément n'est pas inversible, il engendre donc un idéal à gauche non trivial.

20. *En déduire qu'il existe deux éléments non inversibles* $z, z' \in \mathcal{H}$ *tels que* $p=zz'$ *et que* $N(z)=N(z')=p$.

Si z (ou z') est un élément de $\mathcal{H}$ dont tous les coefficients sont dans $\mathbb{Z}$, le théorème est démontré. Supposons que z (et z') ont leurs coefficients dans $\frac{1}{2}+\mathbb{Z}$.

21. *Montrer qu'il existe un élément* $u \in \mathcal{H}$ *tel que* $N(u)=1$ *et* $zu \in \mathbb{H}(\mathbb{Z})$. (Le conjugué de la classe de $2z$ dans $\mathbb{H}(\mathbb{Z})/4\mathbb{H}(\mathbb{Z}) \simeq \mathbb{H}(\mathbb{Z}/4\mathbb{Z})$ est la classe d'un quaternion x dont les coefficients sont tous 1. Prendre $u=\frac{1}{2}x$.)

On en déduit que $p=N(zu)$, avec $zu \in \mathbb{H}(\mathbb{Z})$, est la somme de quatre carrés dans $\mathbb{Z}$, donc dans $\mathbb{N}$.

This page intentionally left blank

TRAVAUX PRATIQUES

TP.IX.A. Factorisation des polynômes

Vous avez étudié au sein des TR.VIII.A et TR.VIII.B des critères permettant de vérifier l'irréductibilité de polynômes. Si ces derniers permettent de traiter des cas de degré arbitrairement grand, ils ne s'appliquent cependant pas à n'importe quel polynôme que l'on se donne explicitement. Par contre, MAPLE sait factoriser dans $\mathbb{Q}[x]$ (commande `factor` ou `factors`, selon l'affichage souhaité) tout polynôme, pourvu que le degré ne soit pas tel que l'on dépasse les capacités de la machine. Le but de ce TP est de comprendre et de réimplémenter l'algorithme qui se cache derrière la commande MAPLE (ou du moins un algorithme efficace qui réalise la factorisation).

Quitte à multiplier par un entier suffisamment grand, on peut toujours supposer que le polynôme P appartient à $\mathbb{Z}[x]$. On peut alors réduire P modulo un nombre premier p et se poser la question de la factorisation du polynôme $\overline{P}$ obtenu dans $\mathbb{F}_p[x]$ (où $\mathbb{F}_p$ désigne le corps fini $\mathbb{Z}/p\mathbb{Z}$). La commande MAPLE correspondante est `Factor(P) mod p` (ou `Factors(P) mod p`). Nous allons décrire un algorithme de factorisation sur un corps fini, dû à Berlekamp, qui utilise essentiellement de l'algèbre linéaire et le morphisme de Frobenius (*cf.* TR.IX.A). Pour simplifier, nous nous limiterons à $\mathbb{F}_p$. Signalons également qu'il existe d'autres algorithmes (Cantor-Zassenhaus, etc.) ; le lecteur trouvera dans [28] une description de ces derniers et une comparaison de leur efficacité en fonction des différents paramètres du problème.

L'algorithme de factorisation sur $\mathbb{Q}$ que nous décrirons est de nature « modulaire » : on factorise $\overline{P}$ sur $\mathbb{F}_p$ et l'on reconstruit les facteurs de P dans $\mathbb{Z}[x]$ à partir des facteurs de $\overline{P}$. C'est possible grâce à une borne *a priori* M des coefficients des diviseurs de P (borne de Mignotte) ; on prend alors $p > 2M$. Nous nous limiterons au cas d'un seul grand nombre premier. Il existe d'autres variantes : par exemple, prendre un petit premier p et un entier n tel $p^n > 2M$. On relève

alors la factorisation dans $\mathbb{F}_p$ en une décomposition dans $\mathbb{Z}/p^n\mathbb{Z}$ grâce au « lemme de Hensel ». Le lecteur intéressé trouvera dans [28], chapitre 15, une description de cette seconde méthode modulaire, ainsi qu'une discussion de la pertinence des deux méthodes en fonction des paramètres du problème.

☞ *Quelques remarques concernant la manipulation des polynômes modulo p en* Maple : par rapport aux commandes relatives aux polynômes de $\mathbb{Z}[x]$ et $\mathbb{Q}[x]$, les noms sont en général conservés, mais les commandes commencent par une majuscule et se terminent par `mod p`. On utilisera donc `Expand(P) mod p` pour développer, `Gcd(P,Q) mod p` pour le calcul du pgcd, `Quo(A,B,x) mod p` et `Rem(A,B,x) mod p` pour le quotient et le reste de la division euclidienne. Le degré s'obtient encore par `degree(P,x)`, le coefficient de degré i par `coeff(P,x,i)` et le coefficient dominant simplement *via* `lcoeff`.

Corps finis et irréductibles de $\mathbb{F}_p[x]$

Nous avons besoin, pour effectuer la factorisation dans $\mathbb{F}_p[x]$, d'un test d'irréductibilité. Nous allons donner un tel critère et en profiter pour indiquer comment construire de manière effective les corps finis $\mathbb{F}_{p^n}$ (ils seront étudiés en détail au chapitre XV, où on les définit à l'aide d'une clôture algébrique de $\mathbb{F}_p$, ce qui démontre l'existence et l'unicité de ces corps, mais n'explique pas comment on calcule, en pratique, dans les corps finis). En effet, si P est un polynôme irréductible de degré n, alors l'idéal (P) qu'il engendre est un idéal premier, donc maximal, de $\mathbb{F}_p[x]$ (en vertu de la principalité de $\mathbb{F}_p[x]$). Le quotient $\mathbb{F}_p[x]/(P)$ est donc un corps et un $\mathbb{F}_p$-espace vectoriel de base $\overline{1}, \overline{x}, \dots, \overline{x}^{n-1}$, où $n = \deg P$, c'est-à-dire un corps à p^n éléments.

***Proposition* 1.** *Pour qu'un polynôme $P \in \mathbb{F}_p[x]$ de degré $n \geqslant 1$ soit irréductible, il faut et il suffit qu'il satisfasse aux deux conditions suivantes :*

(i) *P divise $x^{p^n} - x$.*

(ii) *Pour tout diviseur strict d de n, P ne divise pas $x^{p^d} - x$.*

Démonstration. Considérons les degrés des facteurs irréductibles de P. En vertu du lemme ci-dessous, la condition (i) signifie que ce sont tous des diviseurs de n et la condition (ii) qu'aucun d'entre eux n'est un diviseur strict de n. Il n'y a donc qu'un seul facteur irréductible et il est de degré n ; autrement dit, P est irréductible. □

Lemme 1. *Soit $n \geqslant 1$ un entier. Le polynôme $x^{p^n} - x \in \mathbb{F}_p[x]$ est exactement le produit de tous les polynômes irréductibles unitaires de $\mathbb{F}_p[x]$ de degré divisant n.*

Démonstration. Soit tout d'abord P un diviseur irréductible de $\mathbb{F}_p[x]$ de degré un diviseur d de n. Il s'agit de démontrer que P divise $x^{p^n} - x$. On a déjà vu que $\alpha^{p^d} = \alpha$ pour tout élément α d'un corps fini de cardinal p^d (TR.IX.A). Comme $K = \mathbb{F}_p[x]/(P)$ est un tel corps, on peut appliquer ce fait à la classe $\overline{x}$ de x dans K. Ensuite, sachant que d divise n, on en déduit que $\overline{x}^{p^n} = \overline{x}$ (on itère le Frobenius $\varphi_{p^d} : a \mapsto a^{p^d}$ qui est l'identité sur K), donc que P divise $x^{p^n} - x$.

Réciproquement, supposons que P soit un facteur irréductible de $x^{p^n} - x$ et démontrons que le degré d de P divise n. Considérons l'ensemble K' des éléments α du corps $K = \mathbb{F}_p[x]/(P)$ tels que $\alpha^{p^n} = \alpha$. Le fait que K' soit un corps découle directement du fait que φ_{p^n} est un morphisme de corps. De plus, il contient la classe de x modulo P, car P divise $x^{p^n} - x$; c'est donc K tout entier.

D'autre part, on a vu que le groupe des inversibles d'un corps est cyclique (TR.IX.A). Il existe donc un élément α de $K^\times$ d'ordre $p^d - 1$. Comme $\alpha^{p^n} = \alpha$, ou encore $\alpha^{p^n - 1} = 1$, on voit que $p^d - 1$ divise $p^n - 1$. Cela implique que d divise n : écrivons $n = dq + r$; alors $p^n - 1 = p^{dq}p^r - 1 = (p^{dq} - 1)p^r + p^r - 1$. Comme $p^d - 1$ divise $p^{dq} - 1$ et que $p^r - 1 < p^d - 1$, on voit que $p^r - 1$ est le reste de la division euclidienne de $p^n - 1$ par $p^d - 1$. Or ce reste est nul, donc $r = 0$.

Ainsi apparaissent dans la décomposition en irréductibles de $x^{p^n} - x$ tous les polynômes irréductibles unitaires de $\mathbb{F}_p[x]$ de degré divisant n et uniquement ceux-là. Il reste à prouver que ces facteurs sont tous de multiplicité un. On considère pour cela le polynôme dérivé $p^n x^{p^n - 1} - 1 = -1$; il est premier avec $x^{p^n} - x$, d'où le résultat. □

Cela démontre le critère. Existe-t-il pour autant de tels polynômes ?

Proposition 2. *Pour tout nombre premier p et tout entier $n \geqslant 1$, il existe des polynômes irréductibles de degré n dans $\mathbb{F}_p[x]$.*

On a besoin, afin de construire les corps finis, d'une preuve effective. La méthode utilisée en pratique est surprenante au premier abord : on tire au hasard un polynôme unitaire de degré n dans $\mathbb{F}_p[x]$, on teste son irréductibilité, et on recommence en cas d'échec.

En effet, notant $I(n,p)$ le nombre de polynômes irréductibles unitaires de $\mathbb{F}_p[x]$ de degré $n \geqslant 1$, il résulte du lemme précédent que $\sum_{d|n} dI(d,p) = p^n$. On en déduit la majoration $I(n,p) \leqslant p^n/n$ que l'on applique également aux $I(d,p)$ pour $d < n$ divisant n. Ainsi

$$p^n - nI(n,p) \leqslant \sum_{d|n, d<n} p^d \leqslant \sum_{d=1}^{E(n/2)} p^d = p(p^{E(n/2)} - 1)/(p-1) < p^{E(n/2)+1},$$

d'où une minoration de $I(n,p)$. Finalement :

$$\frac{p^n - p^{E(n/2)+1}}{n} \leqslant I(n,p) \leqslant \frac{p^n}{n}.$$

Cela montre que $I(n,p) > 0$. Mieux encore, on en déduit qu'un polynôme irréductible unitaire de grand degré n choisi au hasard a, en gros, une chance sur n d'être irréductible.

Enfin, expliquons comment vérifier le critère d'irréductibilité de manière efficace : on se place dans l'anneau quotient $\mathbb{F}_p[x]/(P)$ et on calcule les puissances x^{p^i} de x modulo P. Puisque $x^{p^{i+1}} = (x^{p^i})^p$, on procède par récurrence et on calcule successivement les restes R_i de la division euclidienne de R_{i-1}^p par P, à partir de $R_0 = x$. La condition (i) s'écrit $R_n = x$ et la condition (ii) est équivalente à $R_i \neq x$ pour $i < n$.

1. Écrire une procédure `irreductible?:=proc(P,p)` testant l'irréductible de P sur $\mathbb{F}_p$ (où P est entré comme un polynôme à coefficients entiers). On utilisera la stratégie exposée ci-dessus.

La fonction suivante permet de tirer au hasard un polynôme unitaire de degré $n \geqslant 1$ dans $\mathbb{F}_p[x]$:

```
>randpol:=(n,p)->sort(x^n+RandomTools[Generate]
(polynom(integer(range=0..p-1), x,degree=n-1))):
```

Vérifier que la probabilité d'obtenir un polynôme irréductible de degré n par un tel tirage au hasard est de l'ordre de $1/n$. On pourra écrire une procédure `test:=proc(N,n,p)` renvoyant la proportion de cas favorables pour N tirages.

Enfin, écrire une procédure `polirreductible:=proc(n,p)` renvoyant un polynôme de $\mathbb{F}_p[x]$ unitaire irréductible de degré n.

Factorisation sur $\mathbb{F}_p$

L'algorithme procède en plusieurs étapes.

La première étape consiste à éliminer les facteurs multiples à l'aide de la dérivation. Écrivant $f = \sum a_i x^i \in \mathbb{F}_p[x]$, le polynôme dérivé est par définition $f' = \sum i a_i x^{i-1}$. Il est nul si et seulement si $f \in \mathbb{F}_p[x^p]$, ou encore, puisque $\sum a_{ip} x^{ip} = (\sum a_{ip} x^i)^p$, si et seulement si $f = g^p$, $g \in \mathbb{F}_p[x]$. En particulier, la dérivée d'un polynôme irréductible est non nulle.

Il s'agit d'écrire la « factorisation sans facteur carré » de f, c'est-à-dire la décomposition $f = \lambda h_1^1 h_2^2 \dots h_s^s$ où λ est le coefficient dominant de f et les h_i sont unitaires sans facteur carré et premiers deux à deux. Si $f = \lambda \prod_{i=1}^r f_i^{e_i}$

est la décomposition de f en facteurs irréductibles (unitaires) dans $\mathbb{F}_p[x]$, alors $h_i = \prod_{e_j=i} f_j$, d'où l'existence et l'unicité de la factorisation sans facteur carré.

Expliquons comment l'obtenir (sans factoriser !). Quitte à diviser par λ, on suppose f unitaire. Partant de $f' = \sum_i i h_i' h_i^{i-1} \prod_{j\neq i} h_j^j$, le lecteur vérifiera que

$$u = \operatorname{pgcd}(f, f') = \prod_{p\nmid i} h_i^{i-1} \prod_{p\mid i} h_i^i.$$

On définit alors deux suites u_k et v_k par récurrence comme suit : $u_1 = u$ et $v_1 = f/u = \prod_{p\nmid i} h_i$. Pour $k \geqslant 1$, on pose $v_{k+1} = \operatorname{pgcd}(u_k, v_k)$ si $p \nmid k$ et $v_{k+1} = v_k$ si $p \mid k$, puis $u_{k+1} = u_k/v_{k+1}$. On vérifie facilement par récurrence que

$$u_k = \prod_{i>k, p\nmid i} h_i^{i-k} \prod_{p\mid i} h_i^i \text{ et } v_k = \prod_{i\geqslant k, p\nmid i} h_i.$$

Il en résulte que $h_k = v_k/v_{k+1}$ si $p \nmid k$. On obtient ainsi des h_k jusqu'à ce que v_k soit un polynôme constant, auquel cas $u_{k-1} = \prod_{p\mid i} h_i^i = g^p$. On remplace alors f par g et l'on recommence.

2. Écrire une procédure `sans2fact:=proc(f,p)` renvoyant la factorisation sans facteur carré de f, formatée comme une liste $[\lambda, [h_1, e_1], \ldots, [h_s, e_s]]$. Tester avec $f(x) = x^{15} + 2x^{14} + 2x^{12} + x^{11} + 2x^{10} + 2x^8 + x^7 + 2x^6 + 2x^4$ et $p = 3$; comparer avec le résultat de la commande Maple `Sqrfree(f) mod 3`.

La deuxième étape consiste à factoriser $P = h$ (sans facteur carré) en un produit d'irréductibles distincts : $P = \prod_{i=1}^r P_i$. D'après le théorème chinois, l'algèbre $A = \mathbb{F}_p[X]/(P)$ est isomorphe au produit $\prod_{i=1}^r \mathbb{F}_p[x]/(P_i)$. Comme les P_i sont irréductibles, chaque $\mathbb{F}_p[X]/(P_i)$ est un corps (à $p^{\deg(P_i)}$ éléments). Le Frobenius $\varphi_p : A \to A$, donné par $a \mapsto a^p$, est un morphisme d'algèbres. Sa matrice, dans la base $\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}$, où $n = \deg P$, s'appelle la matrice de Berlekamp.

☞ *Quelques remarques concernant l'algèbre linéaire sur $\mathbb{F}_p$ en* Maple : on utilise la librairie dédiée : faire `with(LinearAlgebra:-Modular)`. La matrice identité I_n de $\mathrm{M}_n(\mathbb{F}_p)$ se définit alors par la commande

`Create(p,n,n,identity,integer)`.

Déclarant une variable `M:=Mod(p,Matrix(n,n),integer)`, on remplit ensuite la matrice M par des affectations `M[i,j]:=...` Le noyau de M s'obtient *via* `Nullspace(M) mod p` ; l'algorithme sous-jacent est l'algorithme de Gauss-Jordan (appliqué à la transposée de M, *cf.* TP.VI.A).

3. Écrire une procédure `Bmatrice:=proc(P,p)` renvoyant la matrice de Berlekamp B. Tester avec $P = x^4 + 1$ et $p = 3$, par exemple, et calculer

le noyau de $B - I_4$. Comparer la dimension de ce noyau aux nombres de facteurs irréductibles dans la décomposition sur $\mathbb{F}_3$. Tester la conjecture que cela suscite à l'aide d'une procédure `test:=proc(P,p)` et de polynômes tirés au hasard par `randpol`. Enfin, démontrer au papier-crayon, pour tout $P = \prod_{i=1}^{r} P_i$, que la sous-algèbre de Berlekamp N de A, noyau de $\varphi_p - \mathrm{Id}_n$, est isomorphe à $\mathbb{F}_p^r$, *via* le morphisme $a \mapsto (a \mod P_1, \ldots, a \mod P_r)$ du théorème Chinois.

4. Soit S une $\mathbb{F}_p$-base de N. Écrire une procédure `Vect2Pol:=proc(v)` convertissant un vecteur $v = (y_1, \ldots, y_n) \in \mathbb{F}_p^r$ en le polynôme $\sum_{i=1}^{n} y_i x^{i-1}$. En déduire S sur l'exemple $P = x^4 + 1$ et $p = 3$.

On note $S = \{\overline{1}, \overline{v_1}, \ldots, \overline{v_{r-1}}\}$. Si $r \geqslant 2$, démontrer qu'il existe, pour tout $1 \leqslant i, j \leqslant r$, $i \neq j$, un élément $\alpha \in \mathbb{F}_p$ et un indice $1 \leqslant k \leqslant r-1$ tels que $v_k \equiv \alpha \mod P_i$ et $v_k \not\equiv \alpha \mod P_j$ (raisonner par l'absurde : si l'on avait $v_k \equiv \alpha_k \mod P_i$ et $v_k \equiv \alpha_k \mod P_j$ pour tout $1 \leqslant k \leqslant r-1$, exhiber une contradiction en regardant dans la base S un élément $\overline{a}$ tel que $a \equiv 1 \mod P_i$ et $a \equiv 0 \mod P_j$). En déduire que si Q est un diviseur de P non irréductible, alors il existe un élément $\alpha \in \mathbb{F}_p$ et un indice $1 \leqslant k \leqslant r-1$ tels que $\mathrm{pgcd}(v_k - \alpha, Q)$ soit un diviseur strict de Q.

Finalement, démontrer que l'algorithme suivant factorise P :

```
on pose i := 1 ; L := [P] ;        # liste de polynômes dont le produit est P
tant que longueur(L) < r
  on prend Q := L[i] ;
  pour tout k ⩽ r − 1, α ∈ F_p
    on pose D := pgcd(v_k − α, Q) ;
    si 0 < degré(D) < degré(Q),
      remplacer Q par D dans L et rajouter Q/D à la fin
      recommencer au début de la boucle extérieure
  poser i := i+1 ;    # Q est irréductible, on n'y touche plus
renvoyer L
```

L'implémenter (on écrira une procédure `Berlekamp1:=proc(P,p)` renvoyant la liste formatée $[\lambda, [P_1, 1], \ldots, [P_r, 1]]$ des facteurs irréductibles unitaires de multiplicité 1, précédés du coefficient dominant) et le tester avec $P = x^4 + 1$ et $p = 3, 17$. Comparer avec le résultat de la commande `Factors`.

5. On va maintenant introduire une variante probabiliste de l'algorithme précédent qui améliore le temps de calcul. Pour simplifier, on suppose $p \neq 2$ (l'algorithme est différent dans ce cas particulier ; voir [28]).

L'idée est la suivante : on choisit au hasard une combinaison linéaire $\overline{a}$ des éléments de la base S (les coefficients étant choisis par des tirages indépendants). Les $a \mod P_i$ sont donc des éléments aléatoirement uniformément distribués sur $\mathbb{F}_p$, indépendamment pour tout i. Alors, si cette combinaison est non nulle, soit $\text{pgcd}(a, P)$ est un facteur non trivial de P et l'on a gagné, soit $a^{\frac{p-1}{2}} \equiv \pm 1 \mod P_i$ pour tout i et chaque cas se produit avec la probabilité $1/2$, indépendamment pour chaque indice i (résultat classique sur les carrés dans le corps $\mathbb{F}_p$, *cf.* TR.IX.A). Il y a beaucoup de chances pour que $\text{pgcd}(a^{\frac{p-1}{2}} - 1, P)$ soit un facteur non trivial de P : il faut et suffit pour cela qu'il existe deux indices distincts i et j tels que $a^{\frac{p-1}{2}} - 1 \equiv 0 \mod P_i$ et $a^{\frac{p-1}{2}} - 1 \not\equiv 0 \mod P_j$.

Écrire une procédure `test:=proc(P,p,S,N)` renvoyant, pour N tirages, la proportion q_1 de cas où $\text{pgcd}(a, P)$ est un facteur non trivial de P et la proportion q_2 de cas où $\text{pgcd}(a^{\frac{p-1}{2}} - 1, P)$ est un facteur non trivial de P parmi les cas où $\text{pgcd}(a, P) = 1$. Tester avec $P = x^4 + 1$ et $p = 17$. Enfin, calculer les probabilités théoriques correspondantes et comparer sur l'exemple avec les proportions obtenues.

6. Même si la probabilité d'obtenir un facteur irréductible est élevée, il est nécessaire de vérifier qu'il en est bien ainsi : c'est là qu'intervient la procédure `irreductible?` de la première partie. Écrire une procédure `Berlekamp2` renvoyant la factorisation obtenue par cette variante probabiliste. On modifiera `Berlekamp1`, les facteurs D de la liste L étant cette fois de la forme $\text{pgcd}(a, P) = 1$ ou $\text{pgcd}(a^{\frac{p-1}{2}} - 1, P)$.

Remarque. Il est difficile de mettre en évidence avec Maple que la variante probabiliste est meilleure car l'arithmétique élémentaire (pour les entiers et les polynômes) n'est pas implémentée de façon optimale dans Maple. De plus, il faudrait optimiser l'exponentiation.

Factorisation sur $\mathbb{Q}$

On suppose P à coefficients entiers. Comme pour $\mathbb{F}_p$, la première étape consiste à écrire la décomposition sans facteur carré de P, *i.e.* $P = \lambda h_1^1 h_2^2 \dots h_s^s$ où λ est le coefficient dominant de P et les $h_i \in \mathbb{Q}[x]$ sont unitaires sans facteur carré et premiers deux à deux.

7. La situation est plus simple qu'en caractéristique p : sur l'exemple

$$f = x^{12} + x^{11} - x^9 - 2x^8 + x^5 + x^4$$

calculer $u = f/\operatorname{pgcd}(f, f')$, factoriser en irréductibles f/u, puis recommencer en remplaçant f par u, etc. Observer les facteurs des quotients f/u successifs et en déduire un algorithme donnant la décomposition sans facteur carré. L'implémenter au sein d'une procédure `Sans2Fact0:=proc(f)`, tester et comparer avec la commande `sqrfree` de Maple.

Remarque. En fait, la commande `sqrfree` renvoie la décomposition sans facteur carré de P dans $\mathbb{Z}[x]$, *i.e.* l'écriture $P = \lambda h_1^1 h_2^2 \dots h_s^s$ où $\lambda \in \mathbb{Z}$ et les $h_i \in \mathbb{Z}[x]$ sont primitifs sans facteur carré et premiers deux à deux. La décomposition en irréductibles dans $\mathbb{Z}[x]$ (*cf.* chapitre VIII) assure l'existence et l'unicité de cette décomposition.

8. Nous allons réduire P modulo un nombre premier p. Pour appliquer l'algorithme de Berlekamp, il faut s'assurer que la réduction $\overline{P}$ est sans facteur carré. Le but de cette question est d'expliquer quels nombres p conviennent, c'est-à-dire comment choisir p sans avoir à calculer $\operatorname{pgcd}(\overline{P}, \overline{P}')$ et recommencer avec un nouveau p si l'on ne trouve pas un polynôme constant.

Calculer `gcd(2*x,2); gcd(-2*x,2); gcd(x/2,1/2); Gcd(2*x,2) mod 3;` Quelle normalisation du pgcd Maple utilise-t-il ?

Calculer `gcd(f,g) mod 3; Gcd(f,g) mod 3;` pour $f = 18x^3 - 42x^2 + 30x - 6$ et $g = -12x^2 + 10x - 2$. Calculer également les résultants suivants :

`resultant(f,g,x) mod 2; Resultant(f,g,x) mod 2;` pour $f = 4x^3 - x$ et $g = 2x + 1$ (voir TR.VIII.C pour une définition du résultant, ou la partie du TP.XI qui y est consacrée).

Le pgcd et le résultant de deux polynômes ne se comportent donc pas bien *a priori* vis-à-vis de la réduction modulo p. Cependant, on voit facilement que si p ne divise pas le coefficient dominant des deux polynômes, alors le résultant réduit modulo p coïncide avec le résultant des réductions modulo p. On voit également que si p ne divise pas le coefficient dominant de l'un des polynômes, alors le résultant réduit modulo p n'est pas nul si et seulement si le résultant n'est pas divisible par p.

D'autre part, on a vu que le résultant de f et g (tous les deux non nuls), calculé sur un corps ($\mathbb{Q}$ ou $\mathbb{F}_p$), est nul si et seulement si $\operatorname{pgcd}(f, g)$ est non constant (TR.VIII.C). Ainsi, si p ne divise pas le coefficient dominant de l'un des polynômes f et g, alors $\operatorname{pgcd}(f, g)$ est non constant si et seulement si

$\mathrm{pgcd}(\overline{f},\overline{g})$ est non constant. En prenant $f = P$ et $g = P'$, on voit que, si p ne divise pas le coefficient dominant de P, alors $\overline{P}$ est sans facteur carré si et seulement p ne divise pas le résultant de P et P'. En particulier, il n'y a qu'un nombre fini de mauvais p. Par définition, le *discriminant* de f est $D(f) = \frac{(-1)^{\frac{n-1}{2}} Res(f,f')}{a}$, où a désigne le coefficient dominant de f. On l'obtient avec la commande Maple `discrim(f,x)`. La définition du résultant montre que a^{2n-2} divise $D(f)$, donc *a fortiori* a. En définitive, si p ne divise pas $D(P)$ alors $\overline{P}$ est sans facteur carré. Tester en prenant $P = x^9+x^6+x^5-2x^4-2x-2$.

Remarque. Si p ne divise pas le coefficient dominant de f et g, on peut montrer que $\mathrm{pgcd}(\overline{f},\overline{g}) = \overline{c}\,\overline{\mathrm{pgcd}(f,g)}$, où c est le coefficient dominant de $\mathrm{pgcd}(f,g)$ calculé dans $\mathbb{Z}[x]$ (voir [28], chapitre 6.4).

9. Avant de poursuivre avec la description de l'algorithme à proprement parlé, faisons une petite digression au sujet des tests modulaires d'irréductibilité : il s'agit d'exploiter au maximum les factorisations de P modulo différents nombres premiers (puisque nous savons déjà tester l'irréductibilité et factoriser sur $\mathbb{F}_p$).

On se donne la liste

$L = (x^7 + 2x^5 + 1,\ x^8 + 2x^5 + 1,\ x^9 + x^4 + x^3 + 5x^2 + 11,\ x^4 + 3x^2 + 7x + 4,$
$x^6 + 2x^3 + 4x^2 + 15,\ x^7 + x + 1).$

- Appliquer le critère par réduction du TR.VIII.B : pour quels polynômes de la liste L peut-on conclure à l'aide des premiers p inférieur à 20 (obtenus par exemple *via* `select(isprime([$1..20])`) ? On écrira une procédure `test1:=proc(f)` que l'on appliquera aux éléments de la liste.
- Écrire une procédure `test2:=proc(f)` renvoyant la liste des degrés des facteurs dans la décomposition en irréductibles sur $\mathbb{F}_p$, pour les différents p premiers inférieurs à 20 tels que cette décomposition soit sans facteur carré (et que p ne divise pas le coefficient dominant de P). Peut-on conclure, à l'aide de ces renseignements, pour tous les cas non tranchés par le test précédent ?
- Proposer un argument pour le cas restant.

La factorisation des polynômes sur $\mathbb{Q}[x]$ est possible par des méthodes modulaires grâce au théorème suivant (consulter [20] pour une preuve) :

***Théorème* 1.** *Soit $P = QR$ avec $P = \sum_i a_i x^i$, $Q = \sum_i b_i x^i$ et R des polynômes de $\mathbb{Z}[x]$. On note d le degré de Q et $\|P\|$ la norme euclidienne de P, c'est-à-dire $\|P\| = (\sum_i |a_i|^2)^{1/2}$. Alors $|b_i| \leqslant \binom{d}{i}\|P\|$.*

Soit alors $M = \|P\| \sup_{1\leqslant d\leqslant \deg(P)/2} \sup_{1\leqslant i\leqslant d} \binom{d}{i}$, appelée borne de Mignotte (ou toute autre constante dont l'on sache que si Q est un diviseur non trivial de P, alors les coefficients de l'un parmi Q et P/Q sont majorés en valeur absolue par M). Choisissons un nombre premier $p > 2M$ ne divisant pas le coefficient dominant de P et tel que la réduction $\overline{P}$ modulo p soit sans facteur carré. On écrit la décomposition $\overline{P} = \overline{\lambda}\prod_{i=1}^{r} \overline{P_i}$ en irréductibles dans $\mathbb{F}_p[x]$ (où λ désigne le coefficient dominant de P).

Si S est un sous-ensemble de $\{1,\dots,r\}$, on note P_S le polynôme congru à $\prod_{i\in S} P_i$ modulo p dont tous les coefficients sont compris entre $-p/2$ et $p/2$ (choisir les représentants de $\mathbb{Z}/p\mathbb{Z}$ symétriques par rapport à 0, que l'on obtient en Maple avec l'opérateur `mod` en définissant au préalable `mod:='mods'`). Si P n'est pas irréductible, il s'écrit $P = \lambda QR$ et on a donc $QR \equiv \prod_{i=1}^{r} P_i \mod p$. Il existe donc une partition de $\{1,\dots,r\}$ en deux sous-ensembles I et J tels que $Q \equiv P_I \mod p$ et $R \equiv P_J \mod p$. L'un des deux, par exemple Q, est de degré $\deg(Q) \leqslant \deg(P)/2$. En vertu du théorème précédent et du choix de p, Q est égal à P_I dans $\mathbb{Z}[x]$.

☞ *Autres commandes* Maple *utiles* :

`floor` (partie entière), `binomial`, `norm(f,2)` (pour calculer $\|f\|$), `convert(S,'*')` (pour multiplier entre eux tous les polynômes de la liste S) ; enfin, si S est une liste de polynômes, `combinat[choose](S,i)` renvoie la liste des parties de S à i éléments.

10. Écrire une procédure `trouve_p:=proc(f)` renvoyant un nombre premier (de préférence le plus petit) supérieur strictement à 2 fois la borne de Mignotte, ne divisant pas le coefficient dominant de f et tel que $\overline{P}$ soit sans facteur carré.

Traiter les exemples suivants :

$$P = x^6 + 2x^3 + 4x^2 + 15,\ P = x^9 + x^6 + x^5 - 2x^4 - 2x - 2.$$

On déterminera p puis l'on testera la divisibilité par des P_S, avec S de cardinal 1, puis 2, 3, etc., jusqu'à $|S|/2$. Lorsqu'un facteur non trivial $Q = P_S$ est obtenu, ne pas oublier d'éliminer les indices correspondants de S avant de recommencer avec P/Q. En déduire la factorisation en irréductibles dans $\mathbb{Q}[x]$ de ces polynômes.

11. Écrire une procédure `FactQ:=proc(P)` renvoyant la décomposition en produit d'irréductibles dans $\mathbb{Q}[x]$. On automatisera les calculs de la question précédente, la décomposition modulo p étant obtenue *via* `Factors(P) mod p`. On éliminera d'emblée les cas triviaux où P est de degré inférieur ou égal à un, cas où la borne de Mignotte n'est pas définie.

TP.IX.B. Les quaternions de Hamilton

Ce TP propose une construction géométrique du corps (non commutatif) $\mathbb{H}$ des quaternions de Hamilton. On y étudie la structure algébrique de $\mathbb{H}$, puis l'on interprète géométriquement l'action de $\mathbb{H}^\times$ par automorphisme intérieur sur $\mathbb{H}$. Il en résulte un isomorphisme entre $\mathrm{SO}_3(\mathbb{R})$ et le quotient $\mathbb{H}^\times/\mathbb{R}^\times$. Cela permet d'interpréter algébriquement la composition de deux rotations de l'espace, de manière similaire au cas de la dimension 2, où il est bien connu que la composition de rotations correspond au produit de nombres complexes de norme 1. Telle était d'ailleurs l'une des motivations à l'introduction des quaternions par Hamilton.

Ce TP reprend et complète une partie des notions rencontrées au cours du TR.IX.B : on regarde les coordonnées cartésiennes comme des variables formelles et on donne des preuves analytiques formelles de certains résultats démontrés au papier-crayon dans le thème de réflexion (notamment l'associativité du produit des quaternions et la description des automorphismes intérieurs comme rotations de l'espace E). Une telle méthode, sans l'aide de l'ordinateur pour effectuer les calculs, serait fastidieuse. Cependant, Maple travaillant dans des corps de fractions rationnelles, il s'agit d'être rigoureux lorsque l'on évalue en des réels donnés.

On rappelle que l'ensemble $\mathbb{H}$ des quaternions de Hamilton est l'ensemble des couples $(r,u) \in \mathbb{R}\times E$, où E désigne l'espace euclidien orienté de dimension 3. On dit que r est la composante réelle et u est appelée composante quaternionique pure. L'ensemble $\mathbb{H}$ hérite de manière canonique d'une structure d'espace vectoriel de dimension 4 sur le corps des réels. Après identification naturelle de $\mathbb{R}$ et E avec des sous-espaces de $\mathbb{H}$, on note $\mathbb{H} = \mathbb{R}\oplus E$. Choisissant une base orthonormée directe (i,j,k) de E, ainsi identifié à $\mathbb{R}^3$, et avec les identifications précédentes, tout quaternion s'écrit $q = r + xi + yj + zk$.

On définit le *conjugué* q^* du quaternion $q=(r,u)$, sa *norme* $N(q)$ et sa *trace* $Tr(q)$ comme suit :

$$q^* = (r,-u), \quad N(q) = qq^* = r^2 + \|u\|^2, \quad Tr(q) = q + q^* = 2r.$$

D'autre part, on munit $\mathbb{H}$ d'une multiplication notée $\cdot$ par la formule suivante :

$$(r,u)\cdot(s,v) = (rs - u.v, rv + su + u\wedge v).$$

☞ *Remarques concernant la manipulation des vecteurs et matrices sous* Maple : nous utiliserons la librairie *LinearAlgebra* de Maple (faire `with(LinearAlgebra);`). Les opérations sur les vecteurs s'effectuent avec les commandes `VectorAdd`, `VectorScalarMultiply`.

Les produits scalaire et vectoriel de deux vecteurs q_1 et q_2 s'obtiennent respectivement par `DotProduct(q1,q2,conjugate=false)` et `CrossProduct(q1,q2)` (l'option `conjugate=false` est nécessaire car Maple travaille par défaut avec des espaces hermitiens).

La norme $\|u\|$ s'obtient par `VectorNorm(u,2,conjugate=false)`.

Utilisant la syntaxe concise de la librairie *LinearAlgebra*, on peut définir le vecteur $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ par `<x,y,z>`. Un quaternion $q = r+xi+yj+zk$ sera donc représenté sous Maple par la liste `q:=[r,<x,y,z>]`.

☞ *Remarques concernant la simplification des expressions sous* Maple : la fonction `normal` permet de comparer deux expressions symboliques en les indéterminées $x_1, \ldots, x_r$ *via* la « représentation normale des expressions rationnelles ». Lorsque $f \in \mathbb{Q}(x_1, \ldots, x_r)$, la commande `normal(f)` renvoie un quotient de deux polynômes premiers entre eux (on divise par le pgcd dans l'anneau factoriel $\mathbb{Q}[x_1, \ldots, x_r]$) et trie les monômes selon un ordre spécifique. L'ordre de Maple est un peu surprenant au premier abord ; on peut demander l'ordre du degré lexicographique en appliquant par la suite la commande `ord`). Pour simplifier les coefficients d'une matrice M (ou d'un vecteur, ou d'une liste de vecteurs, etc.), on est amené à combiner cette fonction avec l'opérateur `Map` comme suit : `Map(normal,M)`. Maple met alors chaque coefficient sous forme normale, ce qui permet la comparaison. Parfois, on a recours à `Map(simplify,M)`, mais il est difficile de voir clair dans les multiples règles de simplification appliquées par Maple. S'il s'agit uniquement de simplifier des racines carrées, on peut appliquer `Map(simplify[sqrt],M)` qui est une commande moins obscure.

La commande `simplify(expr,trig)` fait appel à la règle de simplification `trig` (consulter au besoin l'aide en ligne) afin de simplifier l'expression `expr`. Tester également la commande `combine(expr,trig)`.

Enfin, il peut être utile de remplacer dans une expression `expr` une sous-expression `expr1` par `expr2` : on utilise pour cela `subs(expr1=expr2,expr)` ou la commande plus élaborée `algsubs(expr1=expr2,expr)`. Par exemple, `subs({x=0,y=1},x^2+y^2+z^2)` ou encore `algsubs(a+b=1,a-b)`. Noter, sur le second exemple, qu'on a le choix entre $2a-1$ ou $-2b+1$ et Maple donne aléatoirement l'une ou l'autre de ces réponses. Si l'on spécifie `algsubs(a+b=1,a-b,[a])`, Maple effectue la division euclidienne de $a-b$ par $a+b$ dans $\mathbb{Q}(b)[a]$ et en renvoie le reste, en l'occurence $-2b+1$.

Structure algébrique de $\mathbb{H}$

1. Écrire des fonctions `Hadd(q1,q2)`, `Hscal(lambda,q)` et `Hmul(q1,q2)` calculant respectivement $q_1 + q_2$, λq et $q_1.q_2$ (où $q, q_1, q_2 \in \mathbb{H}$ et $\lambda \in \mathbb{R}$). Tester sur des exemples de votre choix. Quels axiomes de la structure de $\mathbb{R}$-algèbre sont vérifiés par $\mathbb{H}$ de façon évidente ? En fait, seule l'associativité du produit pose quelques difficultés que nous surmonterons plus loin.

2. Écrire une fonction `egal?(q1,q2)` renvoyant `true` ou `false` selon que $q_1 = q_2$ ou non. Notant $e = 1$, la structure multiplicative sur la $\mathbb{R}$-algèbre $\mathbb{H}$ est donc définie par les produits de deux éléments de la base (e, i, j, k) de $\mathbb{H}$ (par linéarité). Vérifier que e est l'unité de $\mathbb{H}$ et que les relations suivantes sont vérifiées : $i^2 = j^2 = k^2 = -e$, $i.j = -j.i = k$, $j.k = -k.j = i$, $k.i = -i.k = j$.

3. On désire démontrer que le produit des quaternions est associatif. Pour cela, on utilise des variables formelles et l'on définit des quaternions `qi:=[ri,<xi,yi,zi>]` pour $i = 1, 2, 3$. Mathématiquement, ce sont trois éléments de $\mathbb{H}(\mathbb{Q}[r_i, x_i, y_i, z_i; 1 \leqslant i \leqslant 3])$, où, pour tout anneau commutatif A, $\mathbb{H}(A)$ désigne le A-module libre A^4 de base (e, i, j, k) muni d'une structure de A-algèbre par les relations de la question précédente. Calculer $res_1 = q_1.(q_2.q_3)$ et $res_2 = (q_1.q_2).q_3$. Que donne `egal?(res1,res2)` ? Réitérer après mise sous forme normale. Cela démontre l'associativité de la multiplication dans $\tilde{\mathbb{H}} = \mathbb{H}(\mathbb{Q}[r_i, x_i, y_i, z_i; 1 \leqslant i \leqslant 3])$, donc dans $\mathbb{H} = \mathbb{H}(\mathbb{R})$ après application du morphisme d'évaluation $\tilde{\mathbb{H}} \to \mathbb{H}$ en un 12-uplet de réels quelconques.

Pour s'entraîner à ce type de raisonnement, démontrer formellement la distributivité de la multiplication par rapport à l'addition.

4. En exploitant l'analogie avec les complexes, où l'inverse s'exprime $z^{-1} = \frac{\bar{z}}{|z|^2}$, démontrer que tout quaternion q non nul est inversible pour la multiplication : $\mathbb{H}$ est donc un corps non commutatif. Puis écrire des fonctions `Conj`, `N` et `Inv` renvoyant respectivement le conjugué, la norme, et l'inverse d'un quaternion. Noter que la conjugaison est un anti-automorphisme de $\mathbb{H}$ (*i.e.* elle est $\mathbb{R}$-linéaire et vérifie $(q_1 q_2)^* = q_2^* q_1^*$) et que la norme $N : \mathbb{H}^\times \to]0, +\infty[$ est un morphisme de groupes.

5. On s'intéresse au groupe non abélien $(\mathbb{H}^\times, \cdot)$. Soit q un quaternion fixé ; déterminer le centralisateur Z_q de q, c'est-à-dire le sous-groupe de $\mathbb{H}^\times$ constitué des quaternions h qui commutent avec q ? Quel est le centre Z de $\mathbb{H}^\times$, c'est-à-dire le sous-groupe constitué des quaternions qui commutent avec tous les éléments de $\mathbb{H}^\times$?

Quaternions et groupe orthogonal

On s'intéresse maintenant à l'action de $\mathbb{H}^\times$ sur $\mathbb{H}$ par automorphismes intérieurs : autrement dit, on s'intéresse aux applications $\phi_q : \mathbb{H} \to \mathbb{H},\ h \mapsto qhq^{-1}$, où q appartient à $\mathbb{H}^\times$.

6. Écrire une procédure `phi:=proc(q,h)` renvoyant $\phi_q(h)$ (et un message d'erreur si $q = 0$). Vérifier avec Maple (à l'aide de la commande `subs`) que $\phi_q \mid_{\mathbb{R}} = \mathrm{Id}_{\mathbb{R}}$ et que E est laissé stable par ϕ_q. En comparant $Tr(\phi_q(h))$ et $Tr(h)$, retrouver au papier-crayon cette dernière assertion.

7. Démontrer que $\rho : q \mapsto \phi_q \mid_E$ définit un morphisme $\rho : \mathbb{H}^\times \to \mathrm{O}_3(\mathbb{R})$ de noyau $\mathbb{R}^\times$. Déterminer le sous-espace des points fixes de $\rho(q) = \phi_q \mid_E$. En déduire que $\rho(q)$ est une rotation d'axe $\mathbb{R}u$, où l'on a posé $q = (r, u)$, et d'angle θ_q que l'on déterminera plus loin en fonction de q.

Écrire la matrice de $\rho(q)$ dans la base (i, j, k). Vérifier avec Maple qu'il s'agit bien d'une matrice orthogonale de déterminant 1. On posera `q:=[r,<a,b,c>]` et l'on travaillera dans $\mathbb{Q}[r, a, b, c]$.

8. Déterminer une base orthonormée directe $\mathcal{B} = (u_1, u_2, u_3)$ de E dont le premier vecteur est $u_1 = \frac{u}{\|u\|}$. Enfin, donner la matrice M_q de $\rho(q)$ dans la nouvelle base $\mathcal{B}$. On effectuera les calculs avec Maple en notant qu'il s'agit d'un changement de base dans un K-espace vectoriel, où K est une extension de corps de $\mathbb{Q}(r, a, b, c)$ obtenue en « rajoutant » $\|u\| = \sqrt{a^2 + b^2 + c^2}$ et une seconde racine pour la construction de u_2. Ce changement de base a-t-il toujours un sens dans le $\mathbb{R}$-espace E ?

9. Soit $q' = \frac{q}{\sqrt{N(q)}}$; que dire de ϕ_q et $\phi_{q'}$? En déduire que l'on peut supposer $N(q) = 1$. Sous cette hypothèse, vérifier que la matrice M_q se réécrit :

$$M_q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2r^2-1 & -2r\sqrt{1-r^2} \\ 0 & 2r\sqrt{1-r^2} & 2r^2-1 \end{pmatrix}.$$

En déduire que $\cos\theta_q = 2r^2 - 1$ et $\sin\theta_q = 2r\sqrt{1-r^2}$. Posant $r = \cos t$ et $\|u\| = \sin t$, quelle relation lie t et θ_q ? Si l'on choisit d'effectuer la substitution $r = \cos t$ et les simplifications d'expressions trigonométriques avec Maple, il est utile d'indiquer au système de calcul formel que $t \in [0, \pi]$ avec la commande `assume(t>=0,t<=Pi)`. Finalement, démontrer que les groupes $\mathbb{H}^\times/\mathbb{R}^\times$ et $\mathrm{SO}_3(\mathbb{R})$ sont isomorphes.

10. Caractériser la rotation $\rho_1 = \rho(j)$. Réciproquement, déterminer q_2 tel que $\rho_2 = \rho(q_2)$ soit une rotation d'angle $\frac{\pi}{2}$ et d'axe $\mathbb{R}(i + j)$. Enfin, caractériser la composée $\rho_1 \circ \rho_2$.

X

K-MORPHISMES ET GROUPE DE GALOIS D'UNE EXTENSION

L'idée fondamentale et profonde de Galois a été d'associer à chaque équation $f(X) = 0$, où $f(X) \in K[X]$, un groupe dont la structure permet de décider de la résolubilité par radicaux, ou non, de l'équation. Les éléments de ce groupe permutent les racines de l'équation en laissant invariants les coefficients. Cette construction peut être généralisée à n'importe quelle extension L/K : c'est la notion de K-**automorphisme** de L, qui conduit au **groupe de Galois** de l'extension.

Cette notion est si importante – par exemple par les relations qu'elle donne entre le degré de l'extension et l'ordre du groupe de Galois, ou encore celles qu'elle induit entre les corps intermédiaires de l'extension et les sous-groupes du groupe de Galois – que nous lui consacrons un chapitre, si court soit-il. Nous la suivrons tout au long des chapitres suivants et nous verrons comment des propriétés supplémentaires sur les extensions se traduisent au niveau de l'action du groupe de Galois.

X.1. K-morphismes

***Définitions* X.1.1.** Soient E/K et F/K des extensions.

a) On appelle K-**morphisme** de E dans F, un morphisme de corps $f : E \longrightarrow F$ qui prolonge l'identité de K (*i.e.* $f_{|K} = id_K$).

b) Un K-morphisme bijectif est un K-**isomorphisme**.

c) Un K-morphisme de E dans lui-même est un K-**endomorphisme** de E.

d) Un K-endomorphisme bijectif est un K-**automorphisme**.

Exemples X.1.1.

a) La conjugaison complexe est un $\mathbb{R}$-automorphisme de $\mathbb{C}$.

b) L'application $\sigma : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ définie par $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ est un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\sqrt{2})$.

Remarques X.1.1.

a) Si E/K et F/K sont des extensions, un K-morphisme de E dans F est un morphisme de K-algèbres. En particulier, c'est un morphisme de K-espaces vectoriels.

b) Nous avons rappelé (exercice VIII.7) qu'un morphisme de corps est toujours injectif. Il est donc bijectif si et seulement s'il est surjectif.

c) Soient E/K et F/K des extensions, f un K-morphisme de E dans F, alors $f(E)$ est un sous-corps de F isomorphe à E. On peut donc considérer que F est une extension de E.

d) Si E/K est une extension finie, tout K-endomorphisme de E est un K-automorphisme, puisque c'est un endomorphisme injectif d'un espace vectoriel de dimension finie.

e) Si $E = K(a)$ (ou, plus généralement, $E = K(a_1, \ldots, a_n)$), tout K-morphisme f de E dans une extension F/K est entièrement déterminé par la donnée de $f(a)$ (ou, plus généralement, par la donnée de $f(a_1), \ldots, f(a_n)$). (Le justifier en utilisant le fait que tout élément de $K(a)$ est une fraction rationnelle en a et que f est injectif.)

f) Soient E/K une extension et $P(X) \in K[X]$ un polynôme dont les racines sont dans E. Si f est un K-endomorphisme de E et si $a \in E$ est une racine de $P(X)$, il est clair, puisque f laisse invariant les coefficients de $P(X)$, que $f(a)$ est aussi racine de $P(X)$. Autrement dit, dans cette situation, tout K-automorphisme de E opère sur les racines de $P(X)$ comme une permutation. Par conséquent, si $E = K(a_1, \ldots, a_n)$, où $a_1, \ldots, a_n$ sont les racines d'un polynôme $P(X) \in K[X]$, d'après la remarque précédente, tout K-automorphisme de E peut être identifié à un élément du groupe S_n.

X.2. Groupe de Galois

Proposition X.2.1. *Soit E/K une extension. L'ensemble des K-automorphismes de E est un groupe pour la composition des applications.*

Démonstration. Il est très facile de vérifier que l'ensemble $Aut(E)$ des automorphismes de corps de E est un groupe pour la composition des applications. On vérifie que l'ensemble des K-automorphismes de E est un sous-groupe de $Aut(E)$. □

Pour cette raison, dans la suite de ce livre, nous écrirons les compositions de K-automorphismes d'une extension de K sous forme de produit, en omettant le signe de composition.

Définition X.2.1. Si E/K est une extension, on note $Gal(E/K)$ le groupe (pour la composition des applications) des K-automorphismes de E et on l'appelle le **groupe de Galois** de l'extension E/K.

Exemples X.2.1.

a) Les $\mathbb{R}$-automorphismes de $\mathbb{C}$ sont l'identité ou la conjugaison complexe, d'où $Gal(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$.

b) On pose $\alpha = \sqrt[3]{2}$ (*i.e.* $\alpha \in \mathbb{R}$, $\alpha^3 = 2$). Alors un $\mathbb{Q}$-automorphisme s de $\mathbb{Q}(\alpha)$ vérifie $s(\alpha)^3 = s(\alpha^3) = s(2) = 2$, donc s est l'identité de $\mathbb{Q}(\alpha)$. On a $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$.

c) On pose $\alpha = \mathrm{e}^{2i\pi/5}$: un $\mathbb{Q}$-automorphisme s de $\mathbb{Q}(\alpha)$ vérifie $s(\alpha)^5 = s(\alpha^5) = s(1) = 1$, donc $s(\alpha)$ est une racine cinquième de l'unité, $s(\alpha) = \alpha$, α^2, α^3, α^4 (on ne peut avoir $s(\alpha) = 1$). Si on note s_i le $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\alpha)$ engendré par $s_i(\alpha) = \alpha^i$, $i = 1, 2, 3, 4$, et si on note $x = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4$ un élément générique de $\mathbb{Q}(\alpha)$ (cette écriture sera rigoureusement justifiée au chapitre XI), on a

$s_1(x) = x$,
$s_2(x) = a + d\alpha + b\alpha^2 + e\alpha^3 + c\alpha^4$,
$s_3(x) = a + c\alpha + e\alpha^2 + b\alpha^3 + d\alpha^4$,
$s_4(x) = a + e\alpha^4 + d\alpha^2 + c\alpha^3 + b\alpha^4$.

En écrivant la table de composition de ces éléments, on voit que $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ (engendré par s_2).

Exercice X.1.

1. Soient K un corps et P son sous-corps premier. Montrer que $Gal(K/P) = Aut(K)$.

2. Montrer que $Gal(\mathbb{R}/\mathbb{Q}) = \{1\}$. (Indication : utiliser le fait que tout nombre réel positif est un carré dans $\mathbb{R}$.)

3. Montrer que $\bigcup_{n\geqslant 1}\mathbb{Q}(2^{1/n})$ est une extension de $\mathbb{Q}$ et que

$$Gal\left(\bigcup_{n\geqslant 1}\mathbb{Q}(2^{1/n})/\mathbb{Q}\right)=\{id\}.$$

(Indication : on pourra commencer par étudier le cas $\mathbb{Q}(2^{1/n})/\mathbb{Q}$.)

X.3. Degré d'une extension et ordre du groupe de Galois

Théorème X.3.1. *Soient K et L deux corps. Toute famille de morphismes de corps de K dans L, distincts deux à deux, est linéairement libre sur L.*

Démonstration. Il suffit de montrer que pour toute famille finie $u_1,...,u_n$ de morphismes distincts deux à deux, l'égalité $\sum_{i=1}^{n}\lambda_i u_i=0$, $\lambda_i\in L$, implique $\lambda_i=0$, $i=1,\dots,n$. Considérons une expression $\sum_{i=1}^{n}\lambda_i u_i=0$ telle que tous les λ_i soient non nuls et que n soit minimal pour cette propriété. Puisque $u_1\neq u_n$, il existe $y\neq 0\in K$ tel que $u_1(y)\neq u_n(y)$. Alors :

$$\forall x\in K,\ 0=\sum_{i=1}^{n}\lambda_i u_i(xy)=\sum_{i=1}^{n}\lambda_i u_i(x)u_i(y).$$

On en déduit que :

$$0=u_1(y)\sum_{i=1}^{n}\lambda_i u_i(x)-\sum_{i=1}^{n}\lambda_i u_i(x)u_i(y)=\sum_{i=2}^{n}\lambda_i(u_i(x)u_1(y)-u_i(x)u_i(y)).$$

Dans cette expression, le coefficient de $u_n(x)$ est $\lambda_n(u_1(y)-u_n(y))$, qui est non nul. D'où la contradiction avec la minimalité de n. □

Proposition - Définition X.3.1. *Soient E un corps et G un groupe d'automorphismes de E. L'ensemble E^G des éléments de E invariants sous l'action de G,*

$$E^G=\{x\in E,\forall s\in G, s(x)=x\}$$

est un sous-corps de E, appelé le corps des invariants de G. On note aussi ce corps $Inv(G)$. □

Théorème X.3.2. *Soient K un corps, G un sous-groupe fini du groupe des automorphismes de K, K_0 le corps des invariants de G. Alors K/K_0 est une extension telle que $[K : K_0] = |G|$.*

Démonstration. Soit n l'ordre de G et notons $G = \{g_1 = 1, g_2, \ldots, g_n\}$. Supposons que $[K : K_0] = m < n$ et soit $\{x_1, \ldots, x_m\}$ une base de K sur K_0. Le système d'équations $g_1(x_j)y_1 + \ldots + g_n(x_j)y_n = 0, j = 1, \ldots, m$, ayant plus d'inconnues que d'équations, a une solution $z_1, \ldots, z_n$ dans K, les $z_i, i = 1, \ldots, n$ étant non tous nuls. On obtient donc une combinaison linéaire des g_i, $1 \leqslant i \leqslant n$, nulle sur la base. On en déduit que la famille g_i, $i = 1, \ldots, n$, de morphismes distincts de K dans K est liée, ce qui est en contradiction avec le théorème (X.3.1). D'où $m \geqslant n$.

Supposons que la dimension du K_0-espace vectoriel K soit strictement supérieure à n. Il existe une famille $\{x_1, \ldots, x_{n+1}\}$ d'éléments de K, libre sur K_0. Pour les mêmes raisons que ci-dessus le système d'équations

$$g_j(x_1)y_1 + \ldots + g_j(x_{n+1})y_{n+1} = 0, \quad j = 1, \ldots, n$$

admet une solution non triviale $(z_1, \ldots, z_{n+1})$. On peut supposer que $z_1, \ldots, z_r$ sont non nuls, $z_{r+1} = \ldots = z_{n+1} = 0$, et que r est minimal pour cette propriété. On a alors

$$g_j(x_1)z_1 + \ldots + g_j(x_r)z_r = 0, \quad j = 1, \ldots, n. \tag{X.1}$$

Soit g un élément de G. On a :

$$gg_j(x_1)g(z_1) + \ldots + gg_j(x_r)g(z_r) = 0, \quad j = 1, \ldots, n.$$

Mais, si j varie de 1 à n, les éléments gg_j parcourent G et le système ci-dessus s'écrit

$$g_j(x_1)g(z_1) + \ldots + g_j(x_r)g(z_r) = 0, \quad j = 1, \ldots, n. \tag{X.2}$$

D'où, en multipliant (X.1) par $g(z_1)$ et (X.2) par z_1, on obtient par soustraction,

$$g_j(x_2)(z_2g(z_1) - g(z_2)z_1) + \ldots + g_j(x_r)(z_rg(z_1) - g(z_r)z_1) = 0.$$

Ceci est un système d'équations analogue à (X.1), avec un nombre de termes strictement inférieur à r. Tous les coefficients sont donc nuls, ce qui est équivalent à

$$\forall g \in G, \ \forall i = 1, \ldots, r, \ z_iz_1^{-1} = g(z_iz_1^{-1}),$$

et donc, $z_iz_1^{-1}$ appartient à K_0. Autrement dit, il existe $u_1, \ldots, u_r$ dans K_0 et k dans K tels que $z_i = ku_i$, $i = 1, \ldots, r$. D'où, pour $j = 1$, on tire de (X.1) que :

$$x_1ku_1 + \ldots + x_rku_r = 0,$$

d'où :

$$x_1u_1 + \ldots + x_ru_r = 0,$$

avec $u_1, \ldots, u_r$ non tous nuls. C'est en contradiction avec le fait que $\{x_1, \ldots, x_{n+1}\}$ est libre sur K_0. D'où $[K : K_0] = n =\mid G \mid$. □

Corollaire X.3.1. *Soient E/K une extension finie et H un sous-groupe fini de $Gal(E/K)$. Alors $[E^H : K] = [E : K]/|H|$.*

Démonstration. On a :

$$[E^H : K] = [E : K]/[E : E^H] = [E : K]/ \mid H \mid . \qquad \square$$

Exercice X.2. Soient K un corps de caratéristique nulle et $K(X)$ le corps de fractions rationnelles à coefficients dans K. Montrer que le groupe de Galois $G = Gal(K(X)/K)$ est infini et que le corps des invariants de G est K.

X.4. Corps intermédiaires et sous-groupes du groupe de Galois

Soient K un corps, E/K une extension et $G = Gal(E/K)$.

Soit L un corps intermédiaire entre K et E, $K \subset L \subset E$. On lui associe $G(L) = Gal(E/L)$. Puisque tout L-automorphisme de E est un K-automorphisme, il est clair que $G(L)$ est un sous-groupe de G. De plus, si L' est un autre corps intermédiaire, tel que $L \subset L'$, alors $G(L) \supset G(L')$.

Soit H un sous-groupe de G. Il est clair que E^H contient K, donc E^H est un corps intermédiaire, $K \subset E^H \subset E$. De plus, si H' est un autre sous-groupe de G, tel que $H \subset H'$, alors $E^H \supset E^{H'}$.

En résumé, si on note $\mathcal{K}(E/K)$ l'ensemble des corps intermédiaires entre K et E, et $\mathcal{G}(G)$ l'ensemble des sous-groupes de G, on a deux applications décroissantes (pour la relation d'ordre définie par l'inclusion)

$$\Phi : \ \mathcal{K}(E/K) \longrightarrow \mathcal{G}(G), \qquad L \longmapsto Gal(E/L)$$

$$\Psi : \ \mathcal{G}(G) \longrightarrow \mathcal{K}(E/K), \qquad H \longmapsto E^H.$$

De plus, pour tout $L \in \mathcal{K}(E/K)$ et tout $H \in \mathcal{G}(G)$, on a

$$L \subset E^{Gal(E/L)} \quad \text{et} \quad H \subset Gal(E/E^H).$$

Autrement dit, on a $L \subset \Psi \circ \Phi(L)$ et $H \subset \Phi \circ \Psi(H)$.

X.4.1. Question

Les applications Φ et Ψ sont-elles des applications bijectives, réciproques l'une de l'autre ?

Les exemples ci-dessous montrent que c'est possible, mais que ce n'est pas toujours vrai.

Exemples X.4.1.

a) On considère le polynôme $f(X) = X^4 - 4X^2 - 5$ de $\mathbb{Q}[X]$. On a $f(X) = (X^2+1)(X^2-5)$, dont les racines sont i, $-i$, $\sqrt{5}$, $-\sqrt{5}$: on se place donc dans $\mathbb{Q}(i,\sqrt{5})$. D'après la décomposition de $f(X)$ donnée ci-dessus, un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(i,\sqrt{5})$ envoie i sur i et $\sqrt{5}$ sur $\sqrt{5}$. Par conséquent, le groupe $Gal(\mathbb{Q}(i,\sqrt{5})/\mathbb{Q})$ a quatre éléments, chaque élément distinct de l'identité étant d'ordre 2. On a donc $Gal(\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Notons $s_0 =$ identité, s_1, s_2, s_3 les $\mathbb{Q}$-automorphismes définis par $s_0(i) = i$, $s_0(\sqrt{5}) = \sqrt{5}$; $s_1(i) = i$, $s_1(\sqrt{5}) = -\sqrt{5}$; $s_2(i) = -i$, $s_2(\sqrt{5}) = \sqrt{5}$; $s_3(i) = -i$, $s_3(\sqrt{5}) = -\sqrt{5}$.

Les sous-groupes de $G = Gal(\mathbb{Q}(i,\sqrt{5})/\mathbb{Q})$ sont $H_0 = \{s_0\}$, $H_1 = \{s_0, s_1\}$, $H_2 = \{s_0, s_2\}$, $H_3 = \{s_0, s_3\}$ et G. D'autre part, on vérifiera que les corps intermédiaires sont $L_0 = \mathbb{Q}(i,\sqrt{5})$, $L_1 = \mathbb{Q}(i)$, $L_2 = \mathbb{Q}(\sqrt{5})$, $L_3 = \mathbb{Q}(i\sqrt{5})$, $L_4 = \mathbb{Q}$. Il est facile de vérifier que $L_j = \mathbb{Q}(i,\sqrt{5})^{H_j}$ et $\mathrm{Gal}(\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i,\sqrt{5})^{H_j}) = H_j$, $j = 0, \ldots, 4$. Par conséquent, pour l'extension $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}$, les applications Φ et Ψ ci-dessus sont bijectives et réciproques l'une de l'autre.

b) Pour l'extension $\mathbb{Q}(i,\sqrt[3]{2})/\mathbb{Q}$, on montre que Φ n'est pas injective en vérifiant que $\Phi(\mathbb{Q}(i)) = \Phi(\mathbb{Q}(i,\sqrt[3]{2}))$ et que Ψ n'est pas surjective, car $\mathbb{Q}(i)$ n'est pas dans l'image de Ψ.

La théorie de Galois (*cf.* chapitre XIV) montre que, sous certaines hypothèses sur l'extension E/K, la réponse à la question X.4.1 est positive.

Cependant, en toute généralité, on a les propriétés suivantes.

Proposition X.4.1. *Soient E/K une extension et $G = Gal(E/K)$.*

(i) *Soient L un corps intermédiaire et s un K-automorphisme de E. Alors $\Phi(s(L)) = s\Phi(L)s^{-1}$.*

(ii) *Soient H et H' deux sous-groupes de G et $s \in G$ tels que $H' = sHs^{-1}$. Alors $\Psi(H') = s(\Psi(H))$.*

Démonstration. (i). Posons $L' = s(L), g \in Gal(E/L), y \in L'$. Alors $y = s(x), x \in L$. D'où :

$$sgs^{-1}(y) = sg(x) = s(x) = y,$$

i.e. $s\Phi(L)s^{-1} \subset \Phi(L')$. De la même manière, $s^{-1}\Phi(L')s \subset \Phi(L)$. Donc $\Phi(L') \subset s\Phi(L)s^{-1}$, d'où l'égalité.

(ii). Soient $x \in \Psi(H)$ et $t \in H$. Alors $sts^{-1}(s(x)) = s(t(x)) = s(x)$. Donc $s(x) \in \Psi(H')$ et $s(\Psi(H)) \subset \Psi(H')$. D'autre part, soit $y \in \Psi(H')$, *i.e.*

$$\forall t \in H, sts^{-1}(y) = y.$$

On pose $x = s^{-1}(y)$; alors $s(t(x)) = y = s(x)$. Comme s est un isomorphisme, on en déduit que $t(x) = x$, d'où $y \in s(\Psi(H))$. On a donc $\Psi(H') \subset s(\Psi(H))$, d'où l'égalité. □

XI

EXTENSIONS ALGÉBRIQUES EXTENSIONS TRANSCENDANTES

Comme cela a été rappelé dans l'introduction du chapitre IX, l'un des objectifs de la théorie des corps est la résolution des équations polynomiales. Inversement, on peut se poser la question suivante : étant donnée une extension L/K, tout élément de L est-il racine d'un polynôme à coefficients dans K ? Si la réponse est affirmative, on dit que l'extension L/K est **algébrique**. C'est par exemple le cas de l'extension $\mathbb{C}/\mathbb{R}$. Par contre, ce n'est pas le cas de l'extension $\mathbb{R}/\mathbb{Q}$ puisque Liouville en 1844, Hermite en 1873, Lindemann en 1882 ont, respectivement, montré que les nombres réels $\sum_{n>0} 10^{-n!}$, e, π, sont irrationnels (*i.e.* n'appartiennent pas à $\mathbb{Q}$) et sont **transcendants** sur $\mathbb{Q}$ (*i.e.* ne peuvent être racine d'un polynôme à coefficients dans $\mathbb{Q}$). On dit que l'extension $\mathbb{R}/\mathbb{Q}$ est **transcendante**.

D'après ce qui précède, on remarque que l'extension $\mathbb{C}/\mathbb{Q}$ est une extension algébrique d'une extension transcendante de $\mathbb{Q}$.

L'objet de ce chapitre est d'introduire et d'étudier les extensions algébriques ou transcendantes et de montrer que la remarque ci-dessus correspond à une situation générale.

XI.1. Extensions algébriques

Définition XI.1.1. Soit E/K une extension. Un élément α de E est **algébrique** sur K s'il existe $P(X) \in K[X]$ tel que $P(\alpha) = 0$.

Considérons $K(\alpha)$, l'extension de K obtenue par adjonction de α à K, et le morphisme d'anneaux $\varphi : K[X] \longrightarrow K(\alpha)$ défini par $\varphi(X) = \alpha$. Alors, dire que α

est algébrique sur K est équivalent à dire que le noyau $\mathrm{Ker}(\varphi)$ de φ est non nul, ou encore que les éléments α^n $(n \in \mathbb{N})$ sont linéairement dépendants sur K.

Théorème XI.1.1. *Soient E/K une extension et $\alpha \in E$ un élément algébrique sur K.*

(i) *Il existe un unique polynôme irréductible unitaire $M_\alpha(X) \in K[X]$ tel que $M_\alpha(\alpha) = 0$.*

(ii) *Tout polynôme $P(X) \in K[X]$ tel que $P(\alpha) = 0$ est divisible par $M_\alpha(X)$.*

(iii) *Le corps $K(\alpha)$ est isomorphe à $K[X]/(M_\alpha(X))$ et $[K(\alpha) : K]$ est égal au degré du polynôme $M_\alpha(X)$. En posant ce degré égal à n, les éléments $1, \alpha, \ldots, \alpha^{n-1}$ forment une base du K-espace vectoriel $K(\alpha)$.*

Démonstration. On a $Im(\varphi) \simeq K[X]/Ker(\varphi)$; puisque l'anneau $K[X]$ est principal, l'idéal $Ker(\varphi)$ est engendré par un polynôme $P(X)$. Puisque $Im(\varphi)$ est contenu dans E, c'est un anneau intègre, par conséquent l'idéal $(P(X))$ est premier. Il est donc engendré par un polynôme irréductible, qui est unique si on le suppose unitaire. Soit $M_\alpha(X)$ ce polynôme. Puisque $M_\alpha(X)$ est irréductible et $K[X]$ est principal, l'idéal $Ker(\varphi)$ est maximal, donc $Im(\varphi)$ est un corps contenant K et α, $Im(\varphi) = K(\alpha)$. On a

$$dim_K(K[X]/(M_\alpha(X))) = deg(M_\alpha(X))$$

et l'isomorphisme

$$K[X]/(M_\alpha(X)) \longrightarrow K(\alpha)$$

envoie la base $1, \overline{X}, \ldots, \overline{X}^{n-1}$ de $K[X]/(M_\alpha(X))$ sur $1, \alpha, \ldots, \alpha^{n-1}$. □

Définitions XI.1.2. Avec les notations ci-dessus, le polynôme $M_\alpha(X)$ est appelé le ***polynôme minimal*** de α sur K. L'entier $deg(M_\alpha(X)) = [K(\alpha) : K]$ est appelé le ***degré*** de α sur K.

Exercice XI.1. Soient E/K une extension et un élément α de E. Montrer que les assertions suivantes sont équivalentes :

(i) α est algébrique sur K.

(ii) Le corps $K(\alpha)$ est isomorphe à $K[\alpha]$.

(iii) $K[\alpha]$ est un K-espace vectoriel de dimension finie.

Exercice XI.2.

1. Soient E/K une extension de degré n et x un élément de E. Montrer que le degré du polynôme minimal de x sur K divise n.

2. Soient K un corps, E/K une extension et x un élément de E algébrique de degré impair sur K. Montrer que x^2 est algébrique sur K et que $K(x^2) = K(x)$.

3. Soient K un corps, E/K une extension, α et β des éléments de E algébriques sur K, $M_\alpha(X)$ et $M_\beta(X)$ leurs polynômes minimaux respectifs. Montrer que si les degrés de $M_\alpha(X)$ et $M_\beta(X)$ sont étrangers, alors $M_\beta(X)$ est irréductible dans $K(\alpha)[X]$.

Définition XI.1.3. Une extension E/K est ***algébrique*** si tout élément de E est algébrique sur K.

Proposition XI.1.1. *Une extension finie est algébrique.*

Démonstration. Soient E/K une extension finie et $\alpha \in E$; puisque $dim_K(K(\alpha)) \leqslant dim_K(E)$, il existe un entier n tel que $1, \alpha, \ldots, \alpha^n$ soient linéairement dépendants. Il existe donc des éléments $a_0, \ldots, a_n$ de K tels que $a_0 + \ldots + a_n\alpha^n = 0$. Autrement dit, il existe un polynôme $P(X) \in K[X]$ tel que $P(\alpha) = 0$. □

Attention. *La réciproque est fausse (*cf. *théorème XI.1.3 ci-dessous).*

Proposition XI.1.2. *Soient E/K une extension algébrique. Alors*

$$Card(E) \leqslant Card(K[X] \times \mathbb{N}).$$

Démonstration. Soit $\Gamma = \{(P, \alpha) \,|\, P \in K[X], \alpha \in E \text{ et } P(\alpha) = 0\}$. L'application $\Gamma \longrightarrow K[X]$ définie par $(P, \alpha) \mapsto P$ est telle que l'image réciproque de tout élément de $K[X]$ est finie, puisque tout polynôme n'a qu'un nombre fini de racines. Donc $Card(\Gamma) \leqslant Card(K[X] \times \mathbb{N})$. L'application $E \to \Gamma$ définie par $\alpha \mapsto (P, \alpha)$, où P est le polynôme minimal de α, est injective. Donc $Card(E) \leqslant Card(\Gamma)$. □

Remarque XI.1.1. Puisque $\mathbb{R}$ et $\mathbb{C}$ ont la puissance du continu et que $\mathbb{Q}$ est dénombrable (donc aussi $\mathbb{Q}[X]$), on en déduit que $\mathbb{R}$ et $\mathbb{C}$ ne sont pas des extensions algébriques de $\mathbb{Q}$ (*cf.* aussi l'appendice en fin de chapitre).

Proposition XI.1.3. *Pour qu'une extension E/K soit algébrique, il faut et il suffit que tout anneau A, tel que $K \subset A \subset E$, soit un corps.*

Démonstration. Soient E/K une extension algébrique et A un anneau tel que $K \subset A \subset E$. Tout élément non nul $\alpha \in A$ étant algébrique, le sous-anneau de A engendré par K et α est égal au corps $K(\alpha)$, donc α est inversible dans A. Réciproquement, supposons que tout anneau A vérifiant $K \subset A \subset E$ soit un corps. Pour tout élément $\alpha \in E$ on a $K \subset K[\alpha] \subset E$, donc $K[\alpha]$ est un corps et α est inversible dans $K[\alpha]$, *i.e.* il existe $f(x) \in K[X]$ tel que $\alpha^{-1} = f(\alpha)$. On a donc $\alpha f(\alpha) - 1 = 0$, *i.e.* α est algébrique. □

Proposition XI.1.4. *Soient E/K une extension et $\alpha_1, \ldots, \alpha_n \in E$ des éléments algébriques sur K. Alors $K(\alpha_1, \ldots, \alpha_n)$, le corps obtenu par adjonction à K des α_i, $i = 1, ..., n$, est une extension finie (donc algébrique) de K.*

Réciproquement, toute extension finie de K est de cette forme.

Démonstration. On fait un raisonnement par récurrence sur n. L'extension $K \subset K(\alpha_1)$ est finie. Supposons que $K(\alpha_1, \ldots, \alpha_{n-1})$ soit une extension finie de K : puisque $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$, $K(\alpha_1, \ldots, \alpha_n)$ est une extension finie de $K(\alpha_1, \ldots, \alpha_{n-1})$, donc de K. La réciproque est évidente. □

Théorème XI.1.2. *Soient E/K et L/E des extensions. L'extension L/K est finie (resp. algébrique) si et seulement si E/K et L/E sont des extensions finies (resp. algébriques).*

Démonstration. Le cas des extensions finies a déjà été vu à la proposition (IX.2.1). Il est clair que si L/K est une extension algébrique, alors E/K et L/E sont des extensions algébriques. On suppose que L/E et E/K sont des extensions algébriques. Soit $\alpha \in L$: il existe des éléments de E, $a_0, \ldots, a_n$, tels que $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Considérons $E_0 = K(a_0, \ldots, a_n)$; puisque les a_i sont dans E, ils sont algébriques sur K. Par conséquent, d'après la proposition (XI.1.4), E_0/K est une extension finie, donc $E_0(\alpha)/K$ également, d'où α est algébrique sur K. □

Les extensions algébriques possèdent la propriété suivante, fondamentale pour la théorie de Galois.

Proposition XI.1.5. *Si E/K est une extension algébrique, tout K-endomorphisme de E est un K-automorphisme.*

Démonstration. Pour tout polynôme $P(X) \in K[X]$, on note R_P l'ensemble des racines de $P(X)$ dans E. L'extension E/K étant algébrique, on a

$$E = \bigcup_{P(X) \in K[X]} R_P.$$

Soit f un K-endomorphisme de E : la restriction de f à R_P est une application de R_P dans R_P, qui est injective puisque restriction d'un morphisme de corps, donc surjective puisque le cardinal de R_P est fini. On en déduit que $f : E \to E$ est surjective. □

Définition* XI.1.4.** On appelle ***nombre algébrique tout nombre complexe algébrique sur $\mathbb{Q}$.

***Théorème* XI.1.3.** *L'ensemble $\mathbb{A}$ des nombres algébriques est un corps et c'est une extension algébrique de $\mathbb{Q}$, de degré infini.*

Démonstration. Un nombre complexe α appartient à $\mathbb{A}$ si et seulement si $[\mathbb{Q}(\alpha) : \mathbb{Q}] < +\infty$. Soient α et β des éléments de $\mathbb{A}$: alors,

- comme $\mathbb{Q}(-\alpha) = \mathbb{Q}(\alpha)$, on en déduit que $-\alpha$ appartient à $\mathbb{A}$;
- comme $\mathbb{Q}(\alpha+\beta) \subseteq \mathbb{Q}(\alpha,\beta)$ et $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, on en déduit que $[\mathbb{Q}(\alpha+\beta) : \mathbb{Q}] < +\infty$, donc que $(\alpha+\beta)$ appartient à $\mathbb{A}$.

On démontre de la même manière que $(\alpha\beta)$ et α^{-1}, si $\alpha \neq 0$, appartiennent à $\mathbb{A}$. Autrement dit, $\mathbb{A}$ est stable par somme, produit et inverse, c'est donc un sous-corps de $\mathbb{C}$.

Montrons que le degré de $\mathbb{A}$ sur $\mathbb{Q}$ ne peut être fini. En effet, le polynôme $X^{p-1} + X^{p-2} + \ldots + X + 1$, où p est un nombre premier, est irréductible sur $\mathbb{Q}$ (*cf.* exemple VIII.9.1) et toute racine α de ce polynôme appartient à $\mathbb{A}$. Ceci étant vrai pour p aussi grand que l'on veut, $[\mathbb{A} : \mathbb{Q}]$ ne peut être fini. □

***Remarque* XI.1.2.** L'extension $\mathbb{A}/\mathbb{Q}$ étant algébrique, d'après la proposition (XI.1.2) $\mathbb{A}$ est dénombrable.

On remarque que tout polynôme irréductible unitaire de $K[X]$ est polynôme minimal de ses racines dans une extension E de K (s'il admet des racines dans E). Une question, importante dans la suite, est de savoir, lorsque ce polynôme admet des racines dans E, si elles sont simples.

***Proposition* XI.1.6.** *Soient K un corps de caractéristique p, E une extension de K et $\alpha \in E$ un élément algébrique sur K. Pour que α soit racine simple de son polynôme minimal $M_\alpha(X)$ sur K, il faut et il suffit que $M_\alpha(X)$ n'appartienne pas à $K[X^p]$.*

Démonstration. Pour que α soit racine multiple de $M_\alpha(X)$, il faut et il suffit que $M'_\alpha(\alpha) = 0$, où M' désigne le polynôme dérivé de M, donc, d'après le théorème (XI.1.1.(ii)), que $M'_\alpha(x)$ soit un multiple de $M_\alpha(X)$. Comme $deg(M'_\alpha(X)) < deg(M_\alpha(X))$, ceci implique que $M'_\alpha(X) = 0$. Mais $M'_\alpha(X) = 0$ est équivalent à $M_\alpha(X) \in K[X^p]$. En effet, si on écrit $M_\alpha(X) = \sum_k a_k X^k$, alors $M'_\alpha(X) = \sum_k k a_k X^{k-1}$ et $M'_\alpha(X) = 0$ est équivalent à $ka_k = 0$ pour tout k, *i.e.* $a_k = 0$ pour tout k non multiple de p. □

Corollaire XI.1.1. *Soient K un corps de caractéristique nulle, E une extension de K et $P(X) \in K[X]$ un polynôme irréductible. Toute racine de $P(X)$ appartenant à E est simple.* □

Exercice XI.3. Étude des extensions de degré deux

1. On étudie d'abord les extensions K de degré 2 de $\mathbb{Q}$, $K \subset \mathbb{R}$.

a) Montrer que toute extension de degré 2 de $\mathbb{Q}$ est de la forme $\mathbb{Q}(\sqrt{d})$, où d est un entier relatif, $d \neq 0, 1$, sans facteur carré.

b) Montrer que si d et d' sont deux tels éléments, avec $d \neq d'$, les extensions $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt{d'})/\mathbb{Q}$ ne sont pas $\mathbb{Q}$-isomorphes.

c) Soient d un entier relatif, $d \neq 0, 1$, sans facteur carré et $r \in \mathbb{Q}$. Montrer que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{r})$ si et seulement si r/d est un carré non nul de $\mathbb{Q}$.

2. Soient K un corps de caractéristique différente de 2 et L/K une extension.

a) Montrer que $[L : K] = 2$ si et seulement s'il existe $\Delta \in K \setminus K^2$ et $\delta \in L$ tels que $\delta^2 = \Delta$ et $L = K(\delta)$.

b) On suppose que $[L : K] = 2$. Déduire de ce qui précède que le groupe $Gal(L/K)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, engendré par l'application σ définie par $\sigma(a + b\delta) = a - b\delta$.

XI.2. Extensions transcendantes

Définition XI.2.1. Soit E/K une extension. Un élément de E qui n'est pas algébrique sur K est dit ***transcendant*** sur K. Si l'extension E n'est pas algébrique, elle est dite ***transcendante*** (sur K).

Remarque XI.2.1. Un élément $\alpha \in E$ est transcendant sur K si et seulement si les éléments α^n, $n \in \mathbb{N}$, sont linéairement indépendants sur K. Dans ce cas, $\dim_K K(\alpha) = +\infty$: il en est donc de même pour $\dim_K E$.

***Proposition* XI.2.1.** *Soit K un corps. Le corps des fractions rationnelles $K(X)$ est une extension transcendante sur K.*

Démonstration. Le seul polynôme de $K[X]$ annulé par X est le polynôme nul. □

***Définition* XI.2.2.** Soit E/K une extension. Une famille d'éléments $(\alpha_i)_{i\in I}$ est dite **algébriquement libre** sur K si l'idéal des relations algébriques entre les α_i à coefficients dans K (*i.e.* le noyau du morphisme $K[X_i]_{i\in I} \longrightarrow K(\alpha_i)_{i\in I}$ défini par $X_i \mapsto \alpha_i$, $i \in I$) est nul. Si une famille d'éléments de E n'est pas algébriquement libre sur K, on dit qu'elle est **algébriquement liée**.

***Remarques* XI.2.2.**

a) La famille $(\alpha_i)_{i\in I}$ est algébriquement libre sur K si et seulement si les monômes $\prod_i \alpha_i^{n_i}$ sont linéairement indépendants sur K, ou encore, si et seulement si la relation $f(\alpha_i) = 0$, où $f \in K[X_i]_{i\in I}$, entraîne $f = 0$.

b) On en déduit que, pour qu'une famille $(\alpha_i)_{i\in I}$ d'éléments de E soit algébriquement libre sur K, il faut et il suffit que toute sous-famille finie soit algébriquement libre sur K.

c) Il est clair que si $(\alpha_i)_{i\in I}$ est une famille d'éléments de E algébriquement libre sur K, elle est linéairement libre sur K. La réciproque est fausse, car si E/K est une extension algébrique, toute famille non vide (y compris une famille linéairement libre) n'est jamais algébriquement libre, puisque tout élément de cette famille possède un polynôme minimal.

***Définitions* XI.2.3.** Une extension E/K est dite extension **transcendante pure** de K s'il existe une famille $(\alpha_i)_{i\in I}$ d'éléments de E, algébriquement libre sur K et telle que $E = K(\alpha_i)_{i\in I}$. Une telle famille est appelée **base pure** de E sur K.

***Théorème* XI.2.1.** *Pour qu'une extension E/K soit transcendante pure, de base pure $(\alpha_i)_{i\in I}$, il faut et il suffit que E soit isomorphe au corps $K(X_i)_{i\in I}$ des fractions rationnelles sur K.*

Démonstration. Si $I = \emptyset$, K est une extension transcendante pure de K. Si $I \neq \emptyset$, alors $\varphi : K[X_i]_{i\in I} \to K[\alpha_i]_{i\in I}$ définie par $f \mapsto f(\alpha_i)$ est un isomorphisme, car surjective par définition de $K[\alpha_i]_{i\in I}$ et injective puisque les $(\alpha_i)_{i\in I}$ sont algébriquement libres. La propriété universelle du corps des fractions d'un anneau intègre (*cf.* exercice VIII.12) montre que le corps des fractions de $K[\alpha_i]_{i\in I}$ est $E = K(\alpha_i)_{i\in I}$, d'où $K(\alpha_i)_{i\in I} \simeq K(X_i)_{i\in I}$. La réciproque est évidente. □

Proposition XI.2.2. *Soient E/K une extension, A et B deux parties de E. Les assertions suivantes sont équivalentes :*

(i) *$A \cup B$ est algébriquement libre sur K et $A \cap B = \emptyset$*

(ii) *A (resp. B) est algébriquement libre sur K et B (resp. A) est algébriquement libre sur $K(A)$ (resp. $K(B)$).*

Démonstration. (i) $\Longrightarrow$ (ii) : Les propriétés $A \subset A \cup B$ et $A \cup B$ algébriquement libres sur K impliquent que A est algébriquement libre sur K. Si B est non algébriquement libre sur $K(A)$, alors il existe une famille finie $(\beta i)_{i=1,\ldots,n}$ d'éléments de B algébriquement liée sur $K(A)$ (*cf.* remarque (XI.2.2.b)). D'où, il existe un polynôme non nul $f \in K(A)[X_1, \ldots, X_n]$ tel que $f(\beta_1, \ldots, \beta_n) = 0$. En conséquence, (par exemple en multipliant f par le produit des dénominateurs des coefficients de f), il existe $g \in K[A][X_1, \ldots, X_n]$ tel que $g(\beta_1, \ldots, \beta_n) = 0$. Mais g s'exprime en fonction d'un nombre fini d'éléments $\alpha_1, \ldots, \alpha_m$ de A ; d'où $g \neq 0$ appartient à $K[\alpha_1, \ldots, \alpha_m, X_1, \ldots, X_n]$ et $g(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n) = 0$, ce qui est contraire à l'hypothèse.

(ii) $\Longrightarrow$ (i) : Si B est algébriquement libre sur $K(A)$, alors $B \cap K(A) = \emptyset$, d'où $B \cap A = \emptyset$. Soient $\alpha_1, \ldots, \alpha_m, \in A$, $\beta_1, \ldots, \beta_n \in B$ et $f \in K[X_1, \ldots, X_m, X_{m+1}, \ldots, X_{m+n}]$ tels que $f(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n) = 0$. Alors le polynôme g défini par $g(Y_1, \ldots, Y_n) = f(\alpha_1, \ldots, \alpha_m, Y_{m+1}, \ldots, Y_{m+n}) \in K[A][Y_1, \ldots, Y_n]$ est tel que $g(\beta_1, \ldots, \beta_n) = 0$. Puisque B est algébriquement libre sur $K(A)$, on a $g = 0$, *i.e.* tous ses coefficients sont nuls. Ces coefficients sont de la forme $g_i(\alpha_1, \ldots, \alpha_m)$, où $g_i \in K[X_1, \ldots, X_m]$. Les éléments $\alpha_1, \ldots, \alpha_m$ sont algébriquement libres, donc tous les g_i sont nuls. D'où $f = 0$ et $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ sont algébriquement libres. □

Corollaire XI.2.1. *Soient E/K une extension, $B \subset E$ une partie algébriquement libre sur K, $x \in E$ un élément transcendant sur $K(B)$. Alors $B \cup \{x\}$ est une partie algébriquement libre sur K.* □

Proposition XI.2.3. *Soient E/K une extension et $L \subset E$. Pour que L soit algébriquement libre sur K, il faut et il suffit que tout $x \in L$ soit transcendant sur $K(L \setminus \{x\})$.*

Démonstration. La condition est nécessaire d'après la proposition (XI.2.2), (prendre $A = L \setminus \{x\}, B = \{x\}$). Supposons que pour tout $x \in L$, x est transcendant sur $K(L \setminus \{x\})$ et que L est algébriquement liée sur K. Alors, il existe une partie finie $A \subset L$ algébriquement liée sur K. Soit B une partie de A algébriquement libre maximale et soit $C = A \setminus B$. Par hypothèse $C \neq \emptyset$ et tout $x \in C$ est

algébrique sur $K(B)$. Par conséquent, x est algébrique sur $K(L \setminus \{x\})$, ce qui est contraire à l'hypothèse. □

Définition* XI.2.4.** Soit E/K une extension. On appelle ***base de transcendance de E sur K un élément maximal de l'ensemble, ordonné par inclusion, des parties de E algébriquement libres sur K.

***Remarque* XI.2.3.** D'après le lemme de Zorn (*cf.* l'appendice en fin de cet ouvrage), un tel élément maximal existe.

***Proposition* XI.2.4.** *Soit E/K une extension. Une partie B de E est une base de transcendance de E sur K si et seulement si B est algébriquement libre sur K et E est algébrique sur $K(B)$.*

Démonstration. Supposons que B soit algébriquement libre sur K et que E soit algébrique sur $K(B)$: alors B est algébriquement libre maximale. En effet, tout élément $x \in E$, $x \notin B$, est algébrique sur $K(B)$. Donc d'après la proposition (XI.2.3), $L = B \cup \{x\}$ ne peut être algébriquement libre sur K.

Réciproquement, soit $B \subset E$ une partie algébriquement libre maximale. Alors tout élément $x \notin B$, $x \in E$, ne peut être transcendant sur $K(B)$, sinon $B \cup \{x\}$ serait algébriquement libre sur K d'après le corollaire (XI.2.1). □

On en déduit le résultat suivant :

***Théorème* XI.2.2.** *Toute extension E/K est une extension algébrique d'une extension transcendante pure de K* (cf. *remarque XI.2.5 ci-dessous).* □

Attention. *Une base pure d'une extension transcendante pure de K est une base de transcendance. Mais une extension transcendante E de K n'est pas nécessairement une extension transcendante pure, même si tous les éléments de $E \setminus K$ sont transcendants sur K,* (cf. *exercice XI.4 ci-dessous).*

***Exercice* XI.4.** (¶) Soient u un nombre réel transcendant sur $\mathbb{Q}$, $K = \mathbb{Q}(u)$, α une racine de $X^2 + u^2 + 1$ dans $\mathbb{C}$ et $E = K(\alpha)$.

a) Montrer que le polynôme $X^2 + u^2 + 1$ est irréductible dans $K[X]$.

b) Montrer que tout élément de $E \setminus \mathbb{Q}$ est transcendant sur $\mathbb{Q}$.

c) Montrer que E n'est pas une extension transcendante pure de $\mathbb{Q}$. (Indication : d'après la proposition (XI.2.4), $\mathbb{Q}(u)/\mathbb{Q}$ est une extension transcendante pure et utiliser la dernière remarque de (XI.2.5).)

Nous allons maintenant montrer, suivant un scénario analogue à celui utilisé dans le cadre des espaces vectoriels, que toutes les bases de transcendance d'une extension ont le même cardinal.

***Proposition XI.2.5* (théorème d'échange).** *Soient E/K une extension, A une partie de E telle que E soit algébrique sur $K(A)$ et B une partie de E algébriquement libre sur K. Alors, il existe une partie C de A telle que $B \cup C$ soit une base de transcendance de E sur K et que $B \cap C = \emptyset$.*

Démonstration. Si E est algébrique sur $K(A)$, alors E est algébrique sur $K(A \cup B)$. Or B est contenu dans $A \cup B$ et B est algébriquement libre sur K ; on en déduit qu'il existe dans $A \cup B$ une partie algébriquement libre maximale contenant B. □

Théorème XI.2.3. *Si une extension E/K a une base de transcendance sur K qui est finie, toutes les bases de transcendance de E sur K ont même cardinal.*

Démonstration. Soit B une base de transcendance de E sur K, avec $card(B) = n$.

Si $n = 0$, alors E est algébrique sur K et toutes les bases de transcendance de E sur K sont vides.

Si $n \neq 0$, supposons le résultat vrai pour les extensions dont une base est de cardinal inférieur ou égal à $n - 1$. Soit B' une autre base de transcendance de E sur K. Supposons que B' ne soit pas contenue dans B (sinon $B' = B$) et soit $x \in B'$, $x \notin B$. D'après le théorème d'échange (XI.2.5), il existe $C \subset B$ telle que $C \cup \{x\}$ soit une base de transcendance de E sur K et $x \notin C$. Puisque B est algébriquement libre maximale, on a $C \neq B$, *i.e.* $Card(C) \leqslant n - 1$. On considère $K' = K(x)$ et $C' = B' \setminus \{x\}$. Alors C et C' sont algébriquement libres sur K' (d'après la proposition XI.2.2) et, comme $K'(C') = K(B')$, E est algébrique sur $K'(C)$ et $K'(C')$. Autrement dit, C et C' sont deux bases de transcendance de E sur K'. Comme $Card(C) \leqslant n - 1$, il en est de même pour C', par hypothèse de récurrence. Donc B' a au plus n éléments. On a donc montré que $Card(B) = n$ implique $Card(B') \leqslant n$. Cela donne le résultat, car si $Card(B') < n$, le même raisonnement appliqué dans l'autre sens donne $Card(B) < n$. □

Remarque XI.2.4. Ce résultat est encore vrai pour les bases infinies, mais la démonstration dans ce cas est beaucoup plus compliquée.

Définition XI.2.5. Soit E/K une extension ayant une base de transcendance sur K qui est finie. On appelle **degré de transcendance** de E sur K le cardinal d'une base de transcendance de E sur K.

Remarques XI.2.5. Il résulte de ce qui précède que si E/K est une extension de degré de transcendance n, alors :

a) Tout système de générateurs a au moins n éléments. S'il en existe un ayant n éléments, c'est une base pure (et E est donc une extension pure de K).

b) Toute partie de E algébriquement libre sur K a au plus n éléments. S'il en existe une ayant n éléments, c'est une base de transcendance de E sur K.

Le théorème (XI.2.3) et la remarque qui le suit montrent que l'extension transcendante pure évoquée dans le théorème (XI.2.2) est unique, à isomorphisme près.

Attention. *La notion d'extension transcendante pure n'est pas stable par sous-extension* (cf. *TR.XI.B).*

XI.3. Appendice

Théorème. *Le nombre π est irrationnel et transcendant sur $\mathbb{Q}$.*

Démonstration (cf. [27]). On remarquera que si $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ est une fonction telle que

$$lim_{n\to+\infty} f(n) = 0,$$

alors il existe N tel que pour tout $n > N$, $f(n) = 0$.

Montrons que π est irrationnel.

On considère

$$I_n = \int_{-1}^{1} (1-x^2)^n cos(\alpha x)dx.$$

Une intégration par parties donne, pour $n \geqslant 2$

$$\alpha^2 I_n = 2n(2n-1)I_{n-1} - 4n(n-1)I_{n-2},$$

d'où, par récurrence,

$$\alpha^{2n+1} I_n = n![P(\alpha)sin\alpha + Q(\alpha)cos\alpha]$$

où $P, Q \in \mathbb{Z}[x]$, avec $d^\circ P < 2n+1$ et $d^\circ Q < 2n+1$. Supposons que $\pi = \frac{a}{b}$ avec $(a,b) = 1$, $a, b \in \mathbb{Z}$. On pose $\alpha = \frac{\pi}{2}$. Alors

$$J_n = \frac{a^{2n+1} I_n}{n!} \in \mathbb{Z}.$$

On a $J_n = \frac{a^{2n+1}}{n!} \int_{-1}^{1} (1-x^2)^n (cos\frac{\pi}{2}x)dx$.

Pour $-1 < x < 1$, la fonction $(1-x^2)^n cos(\frac{\pi}{2}x)$ est strictement positive, donc $J_n > 0$ pour tout n.

Mais $\mid J_n \mid \leqslant \frac{|a|^{2n+1}}{n!} \int_{-1}^{1} cos(\frac{\pi}{2}x)dx \leqslant C\frac{|a|^{2n+1}}{n!}$. D'où $lim_{n\to+\infty} J_n = 0$. Donc, il existe N tel que pour tout $n > N$, $J_n = 0$. Contradiction.

Montrons que π est transcendant sur $\mathbb{Q}$.

Supposons que π soit algébrique sur $\mathbb{Q}$. Comme i ($i^2 = -1$) est algébrique, $i\pi$ est algébrique. Donc il existe un polynôme $P_1(X) \in \mathbb{Q}[X]$ ayant pour racines $\alpha_1 = i\pi, \alpha_2, \ldots, \alpha_n$. Mais, $e^{i\pi} + 1 = 0$, donc

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1)\ldots(e^{\alpha_n} + 1) = 0. \tag{XI.1}$$

On va construire un polynôme appartenant à $\mathbb{Z}[X]$ dont les racines seront toutes les sommes $\alpha_{i_1} + \ldots + \alpha_{i_r}$ qui apparaissent comme puissances de e dans le développement de l'expression $(XI.1)$.

Considérons tous les éléments $\alpha_s + \alpha_t$, $1 \leqslant s \leqslant n$, $1 \leqslant t \leqslant n$. Les polynômes symétriques élémentaires en les $\alpha_s + \alpha_t$ sont des polynômes symétriques en les $\alpha_1, \ldots, \alpha_n$. Ils s'expriment donc en fonction des polynômes symétriques élémentaires en les $\alpha_1, \ldots, \alpha_n$, (*cf.* VIII.11). Ces polynômes α_t sont racines d'un polynôme $P_2(X) \in \mathbb{Q}[X]$. De la même façon, les $\alpha_{i_1} + \ldots + \alpha_{i_k}$ sont racines d'un polynôme $P_k(X) \in \mathbb{Q}[X]$.

On considère le polynôme

$$P_1(X)P_2(X)\ldots P_n(X) \in \mathbb{Q}[X]$$

dont les racines sont les exposants des puissances de e dans l'expression développée de $(XI.1)$. En multipliant par un entier, on obtient un polynôme de $\mathbb{Z}[X]$, et en divisant par une puissance de X convenable, on obtient un polynôme $Q(X)$ dont les racines sont les exposants non nuls $\beta_1, \ldots, \beta_r$ qui apparaissent dans le développement de (XI.1),

$$e^{\beta_1} + e^{\beta_2} + \ldots + e^{\beta_r} + e^0 + \ldots + e^0 = e^{\beta_1} + \ldots + e^{\beta_r} + k = 0,$$

avec $k > 0$. Supposons que

$$Q(X) = cX^r + c_1X^{r-1} + \ldots + c_r.$$

Alors $c_r \neq 0$ puisque $Q(0) \neq 0$. On pose

$$f(x) = \frac{c^s x^{p-1} Q(x)^p}{(p-1)!} \quad \text{avec } s = rp - 1,\ p \text{ premier}$$

et on considère

$$F(x) = f(x) + f'(x) + \ldots + f^{(s+p+r-1)}(x)$$

(on a $f^{(s+p+r)}(x) = 0$). Alors

$$\frac{d}{dx}(e^{-x}F(x)) = e^{-x}(F'(x) - F(x)) = -e^{-x}f(x),$$

d'où

$$e^{-x}F(x) - F(0) = -\int_0^x e^{-y}f(y)dy.$$

On fait le changement de variable $y = tx$ et on trouve

$$F(x) - e^x F(0) = -x\int_0^1 e^{(1-t)x}f(tx)dt.$$

On fait prendre à x les valeurs $\beta_1, \ldots, \beta_r$ et on fait la somme. Puisque

$$e^{\beta_1} + \ldots + e^{\beta_r} + k = 0,$$

on trouve

$$\sum_{j=1}^r F(\beta_j) + kF(0) = -\sum_{j=1}^r \beta_j \int_0^1 e^{(1-t)\beta_j} f(t\beta_j)dt. \tag{XI.2}$$

On va montrer que le premier membre est un entier non nul pour p assez grand.

Puisque $Q(\beta_j) = 0$, on a $\sum_{j=1}^r f^{(q)}(\beta_j) = 0$, pour $0 < q < p$. Pour $q \geqslant p$, $f^{(q)}(\beta_j)$ a un facteur p. Pour tout q, $\sum_{j=1}^r f^{(q)}(\beta_j)$ est un polynôme symétrique en les β_j de degré inférieur à s. C'est donc un polynôme de degré inférieur à s en les $\frac{c_i}{c}$. Le facteur c^s fait que ces expressions sont dans $\mathbb{Z}$. D'où, si $q \geqslant p$,

$$\sum_{j=1}^r f^{(q)}(\beta_j) = pk_q \in \mathbb{Z}.$$

On regarde maintenant $F(0)$. On a :

$$f^{(q)}(0) = \begin{cases} 0 & q \leqslant p-2 \\ c^s c_r^p & q = p-1 \\ l_q p & q \geqslant p \end{cases}$$

avec $l_q \in \mathbb{Z}$. Donc le premier membre de (XI.2) est du type $Kp + kc^s c_r^p$, $K \in \mathbb{Z}$. Comme $k \neq 0, c \neq 0, c_r \neq 0$, si on considère $p > sup(k, \mid c \mid, \mid c_r \mid)$, le premier membre de (XI.2) est un entier non divisible par p, donc non nul.

On examine maintenant le second membre de (XI.2) :

$$|f(t\beta_j)| \leqslant \frac{|\ c\ |^s|\ \beta_j\ |^{p-1}\ m(j)^p}{(p-1)!}, \quad \text{où } m(j) = sup_{0\leqslant t\leqslant 1}\ |\ Q(t\beta_j)\ |\ .$$

D'où

$$\left| -\sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-t)\beta_j} f(t\beta_j)dt \right| \leqslant \sum_{j=1}^{r} \frac{|\ \beta_j\ |^p|\ c\ |^s\ m(j)^p B}{(p-1)!}$$

avec

$$B = sup_j \left| \int_0^1 e^{(1-t)\beta_j} dt \right|.$$

Donc cette expression tend vers 0 quand p tend vers $+\infty$. Comme c'est une fonction de p, à valeurs dans $\mathbb{Z}$, elle devrait être nulle pour p assez grand. Or le premier membre est non nul pour p assez grand. Contradiction. □

THÈMES DE RÉFLEXION

♡ TR.XI.A. Constructions à la règle et au compas

Nous allons voir dans ce TR que, malgré le caractère très élémentaire des notions algébriques introduites dans les chapitres qui précèdent, ces notions permettent de résoudre des problèmes géométriques – quadrature du cercle, trisection de l'angle, duplication du cube – qui étaient restés sans réponse pendant des siècles. Ceci est un exemple de la puissance des méthodes algébriques en géométrie. Nous compléterons cette étude au chapitre XVII en montrant comment la théorie de Galois permet de déterminer les polygônes qui sont constructibles à la règle et au compas.

Nous allons tout d'abord donner un formalisme algébrique qui permet de décrire les constructions géométriques à la règle et au compas.

Soit $\mathcal{P}_0$ un ensemble de points du plan euclidien $\mathbb{R}^2$. On considère deux types de constructions géométriques :

(α) Tracer une droite passant par deux points de $\mathcal{P}_0$.

(β) Tracer un cercle de centre un point de $\mathcal{P}_0$ et de rayon égal à la distance entre deux points de $\mathcal{P}_0$.

Tout point de $\mathbb{R}^2$ obtenu comme intersection de deux droites ou cercles distincts au moyen des opérations (α) ou (β) est dit ***constructible en une étape***.

Un point M de $\mathbb{R}^2$ est dit ***constructible*** à partir de $\mathcal{P}_0$ s'il existe une suite finie de points M_1, $M_2, \ldots, M_n = M$ de $\mathbb{R}^2$, tels que M_{i+1}, $1 \leqslant i \leqslant n-1$, soit un point constructible en une étape à partir de $\mathcal{P}_0 \cup \{M_1, \ldots, M_i\}$.

On suppose $\mathbb{R}^2$ rapporté à un système de coordonnées et on repère un point par ses coordonnées (x, y). On note K_0 le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points de $\mathcal{P}_0 = \{P_i(x_i, y_i)\}_{i \in I_0}$, $K_0 = \mathbb{Q}(x_i, y_i)_{i \in I_o}$.

Soit M_n un point constructible de $\mathbb{R}^2$, par une suite $M_1, \ldots, M_i, \ldots, M_n$: en notant (x_i, y_i), $1 \leqslant i \leqslant n$, les coordonnées du point M_i, on définit par récurrence

le sous-corps K_i de $\mathbb{R}$ par $K_i = K_{i-1}(x_i, y_i)$. On obtient donc une suite d'extensions

$$K_0 \subset K_1 \subset \ldots \subset K_i \subset \ldots \subset K_n \subset \mathbb{R}.$$

1. *Avec les notations ci-dessus, montrer que*

$$[K_{i-1}(x_i) : K_{i-1}] = 1 \text{ ou } 2$$

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

(En écrivant les équations des droites ou cercles dont le point M_i est intersection, on montrera que les polynômes minimaux de x_i et y_i sont de degré 1 ou 2.)

2. *Soit $M = (x, y)$ un point de $\mathbb{R}^2$ constructible à partir de $\mathcal{P}_0$. Montrer que les extensions $K_0(x)/K_0$ et $K_0(y)/K_0$ ont un degré qui est une puissance de 2.*

Duplication du cube

Le problème est : ***« Peut-on construire à la règle et au compas l'arête d'un cube dont le volume soit le double de celui d'un cube donné ? »***.

On peut supposer que le cube donné est le cube unité et on pose $\mathcal{P}_0 = \{(0,0),(1,0)\}$.

3. *Montrer que le problème posé revient à construire un segment de longueur a, avec a racine du polynôme $X^3 - 2$.*

4. *En déduire que la duplication du cube est impossible.*

Trisection de l'angle

Le problème est : ***« Peut-on construire à la règle et au compas deux droites qui divisent un angle donné quelconque θ en trois angles égaux ? »***.

On considère le cas $\theta = \frac{\pi}{3}$. Le problème posé revient alors à construire $\alpha \in [0,1]$ tel que $\alpha = cos\frac{\pi}{9}$, donc aussi $\beta = 2\alpha$.

5. *Montrer que le polynôme minimal de β est $X^3 - 3X - 3$.* (On utilisera la formule $cos(3a) = 4cos^3(a) - 3cos(a)$.)

6. *En déduire que la trisection de l'angle est impossible.*

Quadrature du cercle

Le problème est : ***« Peut-on construire à la règle et au compas un carré ayant même aire qu'un disque donné ? »***.

Supposons que le disque donné soit le disque unité, d'aire π. Le problème posé revient donc à construire le point de coordonnées $(0, \sqrt{\pi})$ à partir de $\mathcal{P}_0 = \{(0,0),(1,0)\}$.

7. *Montrer que si la construction du point $(0, \sqrt{\pi})$ était possible, $[\mathbb{Q}(\pi) : \mathbb{Q}]$ serait fini.*

8. *Déduire de ce résultat et de la transcendance de π que la quadrature du cercle est impossible.*

♠ TR.XI.B. Théorème de Lüroth

Les résultats concernant les extensions transcendantes établis dans ce chapitre conduisent à la question suivante :

Soit E/K une extension transcendante pure : toute sous-extension de E/K est-elle une extension transcendante pure de K ?

Nous allons voir ci-dessous que c'est bien le cas lorsque l'extension E/K est de degré de transcendance égal à 1.

Un théorème, dû à Castelnuovo, dont la démonstration dépasse largement le niveau de ce livre, affirme que c'est encore vrai pour les extensions transcendantes pures de $\mathbb{C}$ dont le degré de transcendance est égal à 2. Il existe des contre-exemples pour les extensions de $\mathbb{C}$ de degré de transcendance égal à 3.

Soient k un corps, $K = k(X)$, $f(X) \neq 0$ et $g(X) \neq 0$ des éléments distincts premiers entre eux de $k[X]$ et $\alpha = \frac{f(X)}{g(X)}$. Soit T une indéterminée : on peut exprimer X comme racine du polynôme $h(T) = \alpha g(T) - f(T)$.

1. *Montrer que le polynôme $h(T)$ est non nul.*

2. *En déduire que K est algébrique sur $k(\alpha)$ et que α est transcendant sur k.*

3. *Montrer que le polynôme $h(T)$ est irréductible dans $k(\alpha)[T]$.* (Faire un raisonnement par l'absurde.)

4. *Montrer que $[K : k(\alpha)] = sup(deg(f), deg(g))$.*

Ce qui précède est une application explicite du théorème (XI.2.2), dans le cas de l'extension $k(X)/k$.

5. *Déduire de ce qui précède que tout k-automorphisme de $k(X)$ est de la forme $f(X) \mapsto f(aX+bcX+d)$, avec $a,b,c,d \in k$ et $ad-bc \neq 0$.*

La suite de ce TR est consacrée à la démonstration du théorème de Lüroth :

Soient k un corps, $K = k(X)$, L un sous-corps de K contenant strictement k. Il existe $y \in L$ transcendant sur k tel que $L = k(y)$.

6. *Montrer que X (donc $k(X)$) est algébrique sur L. En déduire que l'extension L/k n'est pas de degré fini.*

On note $F(T) = T^n + a_1(X)T^{n-1} + \ldots + a_n(X)$ le polynôme minimal de X sur L.

7. *Montrer qu'on peut écrire les coefficients $a_i(X)$ (qui sont des fractions rationnelles que l'on suppose irréductibles) sous la forme $b_i(X)/b_0(X)$, avec $b_0(X)$ de degré minimal.* ($b_0(X)$ est le *ppcm* des dénominateurs des $a_i(X)$).

On considère alors le polynôme $G(X,T) = b_0(X)T^n + b_1(X)T^{n-1} + \ldots + b_n(X)$ et on note n' le degré de G par rapport à la variable X.

8. *Montrer que :*

- *Pour tout i, $b_i(X)/b_0(X)$ appartient à L.*
- *Les $b_i(X)$ sont premiers entre eux dans leur ensemble.*
- *Il existe $i \neq 0$ tel que $b_i(X)/b_0(X)$ n'appartienne pas à k.*

On note y un élément $b_i(X)/b_0(X) \notin k$ et on pose

$$H(X,T) = b_0(X)b_i(T) - b_i(X)b_0(T).$$

9. *Montrer qu'il existe $f(X,T) \in k[X,T]$ tel que $H(X,T) = f(X,T)G(X,T)$.*

10. *Montrer que le polynôme $f(X,T)$ est constant et en déduire que $n' = n$.* (Utiliser l'antisymétrie en X et T de $H(X,T)$ et raisonner sur les degrés.)

11. *Montrer que $[K : k(y)] \leqslant n$ et en déduire que $L = k(y)$.*

TRAVAUX PRATIQUES

TP.XI. Nombres algébriques et polynôme minimal

On se propose de manipuler, avec MAPLE, les nombres algébriques (c'est-à-dire les nombres complexes définis comme zéros a de polynômes P de $\mathbb{Q}[x]$, ou, de façon équivalente, de $\mathbb{Z}[x]$). On travaille donc dans des corps de nombres $\mathbb{Q}(a) \simeq \mathbb{Q}[x]/(P)$ (on suppose P irréductible). On va voir comment définir en MAPLE de telles extensions et calculer dans $\mathbb{Q}(a)$.

L'un des problèmes est de trouver le polynôme minimal de $b \in \mathbb{Q}(a)$. L'ingrédient essentiel est le résultant, qui permet de calculer la *norme* d'un polynôme de $\mathbb{Q}(a)[x]$ (voir plus loin). En effet, la norme de $x-b$ est liée au « polynôme caractéristique » de b, donc au polynôme minimal. Nous étudierons en détail le résultant puis la norme, qui est cruciale également dans l'algorithme de factorisation d'un polynôme sur un corps de nombres. Ainsi MAPLE est-il capable de factoriser un polynôme Q de $\mathbb{Q}[x]$ sur $\mathbb{Q}(a)$. Bien entendu, on utilise la factorisation sur $\mathbb{Q}$ (algorithme décrit au TP.IX.A). Nous donnons pour finir quelques applications.

Familiarisation

1. Manipulons.

– Tester les commandes `irreduc(P)` et `solve(P)` sur différents polynômes $P \in \mathbb{Z}[x]$ de bas degré. Par quel type de formules MAPLE exprime-t-il les racines ? Pourquoi n'obtient-on pas de telles formules dans tous les cas ? (Vous en saurez plus au chapitre XVI.) MAPLE renvoie alors un « `RootOf` » (tester $x^5 - x + 1$ par exemple).

– Quel est l'intérêt de la commande `alias` ?

– Que fait `evala` ? Que fait `allvalues` ?

```
> P:=x^5-x+1: irreduc(P); solve(P);
> a:=RootOf(P,x); a^10; evala(a^10);
> alias(b=RootOf(P,x)): b^10; evala(b^10);
> rac:=allvalues(a);
```

– Tester la commande `factor(P)` sur différents polynômes ; enfin, reprendre l'exemple de la question précédente :

```
> factor(P);
> factor(P, real);
> factor(P, complex);
> rac1:=map(evalf,[rac]);
> map(r->convert(r,polar),rac1);
```

Quel type d'algorithme Maple utilise-t-il pour factoriser dans les réels et les complexes ? Essayer de comprendre comment les racines stockées dans `rac` sont ordonnées, en consultant au besoin l'aide de la commande `RootOf,indexed`.

– Calculer à la main les expressions suivantes :

```
> sum(x,x=RootOf(P,x)), sum(x^5,x=RootOf(P,x)),
  sum(1/x,x=RootOf(P,x));
```

(Utiliser les relations entre coefficients et racines, *cf.* chapitre VIII, paragraphe 11.)

– Les degrés 3 et 4 :

```
>alias(a=RootOf(x^3+x-1)): allvalues(a);
>a:='a': alias(a=RootOf(x^3+x-1)): allvalues(a);
>alias(b=RootOf(x^3+x-1)): allvalues(b);
>P:=sort(x^3+add(c[i]*x^i,i=0..2),x);allvalues(RootOf(P,x));
>P:=sort(x^4+add(c[i]*x^i,i=0..3),x);allvalues(RootOf(P,x));
```

2. Soit a une racine du polynôme $P(x) = x^5 + x^2 + 4$ et soit $R(x) = x^9 + x^6 + 1$. Définir P, R et a sous Maple ; que donne `evala(subs(x=a,R));` ? Vérifier qu'il s'agit de la valeur en a du reste de la division euclidienne de R par P, conformément à l'isomorphisme $\mathbb{Q}[a] \simeq \mathbb{Q}[x]/(P)$ qui fait correspondre à $R(a)$ la classe de $R(x)$ dans le quotient $\mathbb{Q}[x]/(P)$. On utilisera la commande Maple `rem`.

Comme $\mathbb{Q}[a] \simeq \mathbb{Q}[x]/(P)$ est un corps, a^{-1} s'exprime également comme un polynôme en a (de degré au plus 4). Tester `evala(subs(x=a,R));` et vérifier que le polynôme obtenu est l'inverse de x modulo P (plus exactement l'inverse de la classe de x dans $\mathbb{Q}[x]/(P)$). Maple a donc appliqué l'algorithme d'Euclide (semi-)étendu (commande `gcdex`) pour calculer le coefficient souhaité d'une relation de Bezout $xu(x) + P(x)v(x) = 1$. Tout élément non nul de $\mathbb{Q}[a]$ est inversible : le polynôme (en a) correspondant est premier avec P, donc on peut écrire l'identité de Bezout. Calculer $R(a)^{-1}$.

Remarque. L'idée de l'algorithme euclidien est que si $a = bq + r$ (où $b \neq 0$) alors ou bien $r = 0$ auquel cas le pgcd est b, ou bien $\text{pgcd}(a, b) = \text{pgcd}(b, r)$ à une unité près. En effet, si d divise a et b, alors il divise $r = a - bq$ (et b) ; réciproquement, s'il divise b et r, il divise $a = bq+r$ (et b). Ainsi le pgcd est le dernier reste non nul. Finalement, l'algorithme d'Euclide est le suivant : à partir de $a_0 = a$ et $b_0 = b$, on effectue les divisions euclidiennes $a_n = b_n q_n + r_n$ puis l'on définit $a_{n+1} = b_n$ et $b_{n+1} = r_n$ tant que $r_n \neq 0$.

Pour l'algorithme étendu, on cherche à construire deux suites u_n et v_n telles que $r_n = au_n + bv_n$ pour tout n, jusqu'au dernier reste non nul où l'on obtient les coefficients de Bezout. On utilise le fait que $a_n = r_{n-2}$ et $b_n = r_{n-1}$: on effectue alors la division euclidienne $r_{n-2} = r_{n-1}q_n + r_n$ et l'on définit $u_n = u_{n-2} - u_{n-1}q_n$ et $v_n = v_{n-2} - v_{n-1}q_n$. Pour initialiser, on part de $r_{-2} = a = a.1 + b.0$ et $r_{-1} = b = a.0 + b.1$.

La problématique qui nous concerne maintenant est la suivante : soit a une racine (dans $\mathbb{C}$) d'un polynôme irréductible P de $\mathbb{Q}[x]$. Cela définit une extension $L = \mathbb{Q}(a)$ de $\mathbb{Q}$. Le polynôme minimal de a est P, à une constante près, et la structure algébrique de $\mathbb{Q}(a)$ est définie par l'isomorphisme $\mathbb{Q}(a) \simeq \mathbb{Q}[x]/(P)$. En particulier, cela ne dépend pas de la racine complexe choisie ; en notation Maple, `a:=RootOf(P,x)` n'en dit pas plus : on travaille dans $\mathbb{Q}[x]/(P)$.

Un autre élément b de $\mathbb{Q}(a)$ s'exprime comme un polynôme $b = R(a)$ en a. Il s'agit de calculer son polynôme minimal sur $\mathbb{Q}$, en fonction de R et P. L'ingrédient essentiel est le *résultant*.

La théorie du résultant

Soit A un anneau intègre. Pour tout entier n, on note $A[x]_n$ le A-module des polynômes de degré strictement plus petit que n. C'est donc un A-module libre de rang n.

Si $f = \sum_{i=0}^{m} a_i x^i$ et $g = \sum_{i=0}^{n} b_i x^i$ sont deux éléments de $A[x]$, on peut définir le résultant $Res(f,g)$ comme le déterminant de la matrice de Sylvester

$$\begin{pmatrix} a_m & \dots & a_1 & a_0 & & \\ & a_m & \dots & a_1 & a_0 & \\ & & \ddots & & \ddots & \ddots \\ & & a_m & \dots & a_1 & a_0 \\ b_n & \dots & \dots & b_1 & b_0 & \\ & \ddots & & & \ddots & \ddots \\ & & b_n & \dots & \dots & b_1 & b_0 \end{pmatrix}$$

où les n premières lignes correspondent à f et les m suivantes à g : c'est donc une matrice de $\mathrm{M}_{mn}(\mathbb{Q})$. On l'obtient en Maple comme suit (pour des polynômes « généraux ») :

```
>sylvester:=proc(m,n) local f,g;
  f:=add(a[i]*x^i,i=0..m); g:=add(b[i]*x^i,i=0..m);
  return(LinearAlgebra[SylvesterMatrix](f,g,x));
 end;
```

La matrice de Sylvester est, à la transposée près (ce qui ne change pas le déterminant), la matrice de l'application linéaire $\phi_{f,g} : (u,v) \mapsto uf + vg$ de $A[x]_n \times A[x]_m$ dans $A[x]_{m+n}$, par rapport aux bases

$$((x^{n-1},0),\dots,(1,0),(0,x^{m-1}),\dots,(0,1)) \text{ et } (x^{m+n-1},\dots,1).$$

Utilisant la relation $\det(S)\,\mathrm{Id} = ST$, où T est la transposée de la comatrice de S, appliquée à la matrice de Sylvester S, puis en multipliant par le vecteur correspondant à $1 \in A[x]_{m+n}$, on voit que $Res(f,g)$ appartient à l'image de $\phi_{f,g}$. Cela démontre :

Proposition 1. *Si f et g sont deux polynômes non constants, il existe u et v dans $A[x]$ avec $\deg(u) < \deg(g)$ et $\deg(v) < deg(f)$ tels que $uf + vg = Res(f,g)$.*

On en déduit :

Proposition 2. *Si A est un anneau principal et si f et g sont deux polynômes non constants de $A[x]$, alors f et g ont un facteur commun non constant dans $A[x]$ si seulement si $Res(f,g) = 0$.*

En effet, on commence par montrer que f et g ont un facteur commun non constant si et seulement s'il existe u et v dans $A[x]$, avec $\deg(u) < \deg(g)$ et $\deg(v) < deg(f)$, tels que $uf + vg = 0$. Dans ce cas, $\phi_{f,g}$ n'est pas injective, donc son déterminant est nul ; la réciproque résulte de la proposition précédente.

Le résultant vérifie les propriétés suivantes, qui le caractérisent :

(a) $Res(g, f) = (-1)^{mn} Res(f, g)$.

(b) Si f et g sont non constants et r est le reste de la division euclidienne de f par g, alors $Res(f, g) = (-1)^{mn} b_n^{m-\deg(r)} Res(g, r)$.

(c) Si $g = b \in A$ alors $Res(f, g) = b^m$ (en particulier, $Res(0, b) = 0$, $Res(a, b) = 1$ si $a, b \in A \setminus \{0\}$).

On a également, notant $f = a_m \prod_{i=1}^{m}(x - r_i)$ et $g = b_n \prod_{i=1}^{n}(x - s_i)$ (dans un corps de décomposition contenant les racines r_i et s_i) :

$$Res(f, g) = a_m^n b_n^m \prod_{i,j}(r_i - s_j). \tag{2}$$

C'est d'ailleurs ainsi que le résultant a été défini au TR.VIII.C.

Nous allons vérifier formellement, pour des petits degrés, les propriétés (a), (b) et (c), écrire un algorithme de calcul du déterminant basé sur ces propriétés (c'est ainsi qu'il est implémenté dans Maple, car cette méthode est bien meilleure que le calcul d'un déterminant). Enfin, nous expliquerons comment démontrer la formule (2) en travaillant dans le corps des séries formelles $K(r_i, s_j)$ (où K désigne le corps des fractions de A), ce qui se prête encore à des vérifications à l'aide du système de calcul formel.

☞ *Quelques remarques concernant la simplification des expressions sous* Maple : La fonction `normal` permet de comparer deux expressions symboliques en les indéterminées $x_1, \ldots, x_r$ *via* la « représentation normale des expressions rationnelles ». Lorsque $f \in \mathbb{Q}(x_1, \ldots, x_r)$, la commande `normal(f)` renvoie un quotient de deux polynômes premiers entre eux (on divise par le pgcd dans l'anneau factoriel $\mathbb{Q}[x_1, \ldots, x_r]$) et trie les monômes selon un ordre spécifique. L'ordre de Maple est un peu surprenant au premier abord ; on peut demander l'ordre du degré lexicographique en appliquant par la suite la commande `ord`. Le degré total en les x_i s'obtient par `degree(P,{seq(x[i],i=1..n)})`.

3. Tester `sylvester(3,4)` et `LinearAlgebra[SylvesterMatrix](f,g,x)` avec $f = 2x^2 + 3x + 1$ et $g = 7x^2 + x + 3$. Puis écrire une procédure `resultant1:=proc(f,g)` calculant $Res(f, g)$ comme un déterminant (pour deux polynômes non tous les deux de degré 0, sans quoi la matrice de Sylvester « dégénère »). On utilisera la commande `LinearAlgebra[Determinant]`. Tester sur l'exemple précédent et comparer avec le résultat de la commande `resultant` de Maple.

Écrire ensuite des procédures de test destinées à vérifier les propriétés (a), (b) et (c). Par exemple :

```
>test2:=proc(m,n)
   f:=add(a[i]*x^i,i=0..m); g:=add(b[i]*x^i,i=0..m);
   r:=rem(f,g,x);
   return(evalb(-1)^(m*n)*b[n]^(m-degree(r,x))*
    normal(resultant(g,r,x)/resultant(f,g,x))=1);
 end:
```

Les démontrer au papier-crayon (commencer par remplacer f par $f - b_n/a_m x^{m-n} g$, effectuer des opérations sur les lignes de la matrice de Sylvester et utiliser les propriétés du déterminant).

Remarque. On a un peu triché : il faudrait utiliser la procédure `resultant1`. Or Maple ne parvient pas à écrire la matrice de Sylvester lorsque les coefficients des polynômes sont dans $\mathbb{Q}(a_i, b_j)$. Il y parvient uniquement pour $\mathbb{Q}[a_i, b_j]$. Pour bien faire, il faudrait donc réécrire une procédure `SylvesterMatrix`.

Par contre, on utilisera `resultant1` pour les tests relatifs à (a) et (c) où ce problème ne se pose pas.

Enfin, écrire une procédure `resultant2` calculant le résultant à partir de ces trois formules. Noter la ressemblance avec l'algorithme d'Euclide. Tester sur les exemples habituels. Prendre également $f = xy - 1$ et $g = x^2 + y^2 - 4$: le résultant appartient à $A = \mathbb{Z}[y]$.

4. Écrivons $f = a_m \prod_{i=1}^{m}(t - x_i)$ et $g = b_n \prod_{i=1}^{n}(t - y_i)$: les racines sont donc des paramètres formels, autrement dit, on travaille dans l'anneau $\mathbb{Z}[x_i, y_j, a_m, b_n]$ qui contient le résultant. Vérifier pour $m = 3$ et $n = 4$ que $Res(f, g)$ est un polynôme homogène de degré $m + n$ (les différents monômes s'obtiennent en appliquant `op`). Il s'agit de remplacer les a_i et b_j par leur expression en fonction des x_i et y_j. La procédure ci-dessous y pourvoit :

```
>remplace:=proc(n,a,x) local P,t,i;
```

```
  if n=1 then return({a[1]=x[1]});
    else P:=collect(expand(a[n]*mu(t+x[i],i=1..n)),t);
    return({seq(a[i]=coeff(P,t,i),i=0..n-1)});
  fi;
end:
```

La commande `subs(remplace(m,a,x) union remplace(n,b,y),R)` exprime alors le résultant R comme un élément de $\mathbb{Z}[x_i, y_j]$. Le tester pour $m = 3$ et $n = 4$. Vérifier qu'il s'agit d'un polynôme homogène de degré mn. Le démontrer pour tout m et n à l'aide de la formule

$$\det M = \sum_{\sigma \in S_d} \varepsilon(\sigma) m_{\sigma(1),1} \dots m_{\sigma(d),d},$$

sachant que les fonctions symétriques élémentaires s_i (donc les a_i) sont homogènes de degré $n - i$ en les x_i.

D'autre part, si l'on remplace x_i par y_j, on obtient un résultant nul. Ainsi $Res(f, g)$ est divisible par $x_i - y_j$ dans $\mathbb{Q}(\widetilde{x_i}, y_j, a_m, b_n)[x_i]$ (où $\widetilde{x_i}$ signifie que l'on omet x_i), donc dans $\mathbb{Z}[x_i, y_j, a_m, b_n]$ car $x_i - y_j$ est unitaire. Les $x_i - y_j$ étant premiers entre eux, $Res(f, g)$ est divisible par $\prod_{i,j}(x_i - y_j)$. Le vérifier sur l'exemple. Quel facteur reste-t-il ? Démontrer finalement la formule (2) (examiner la contribution de la diagonale, *i.e.* $\sigma = \mathrm{Id}$). Noter que l'on utilise le fait que l'évaluation est un morphisme d'anneaux qui « commute » avec le déterminant : on peut remplacer les x_i par les r_i.

Calcul du polynôme minimal

Soient $L = \mathbb{Q}(a)$ l'extension de $\mathbb{Q}$ définie par la racine a d'un polynôme irréductible $P \in \mathbb{Z}[x]$ et $b = R(a) \in L$, où $R \in \mathbb{Q}[x]$. On désire calculer le polynôme minimal de b sur $\mathbb{Q}$.

Pour cela, soit m_b la multiplication par b, vue comme endomophisme du $\mathbb{Q}$-espace vectoriel L. Le déterminant $P_{b,L/\mathbb{Q}}(x) = \det(x\,\mathrm{Id}_L - m_b)$ est par définition le polynôme caractéristique de b par rapport à l'extension $L/\mathbb{Q}$. De plus, on verra (*cf.* chapitre XIII) :

***Proposition* 3.** *Soient L/K une extension finie de degré n, b un élément de L, μ_b le polynôme minimal de b sur K et $r = [L : K(b)]$. Le polynôme caractéristique de b par rapport à l'extension L/K est alors $P_{b,L/K} = \mu_b^r$.*

5. Soit $P = x^4 + x^3 + x^2 + x + 1$, a une racine de P et $b \in \mathbb{Q}(a)$. On va voir que la commande `evala(Norm(x-b));` de Maple calcule le polynôme caractéristique de b par rapport à l'extension $\mathbb{Q}(a)/\mathbb{Q}$.

– On prend $b = a$; vérifier que la commande `evala(Norm(x-b))` donne le polynôme minimal. Écrire la matrice A de m_a dans la base $(1, a, \ldots, a^3)$ (commencer par définir `ma:=(i,j)->...;` puis `A:=Matrix(4,ma);`). Calculer enfin le polynôme caractéristique de a par rapport à l'extension $\mathbb{Q}(a)/\mathbb{Q}$ à l'aide de la commande

```
LinearAlgebra[CharacteristicPolynomial](A,x);
```

et comparer.

– On prend $b = a + a^{-1}$. Refaire les mêmes calculs et déterminer μ_b.

Nous allons maintenant expliquer le nom de la commande Maple. Si $a_1 = a, \ldots, a_m$ sont les m racines complexes distinctes du polynôme irréductible P de degré m et si A est un polynôme donné de $\mathbb{Q}(a)[x]$, la norme $N_{\mathbb{Q}(a)/\mathbb{Q}}(A)$ est par définition :

$$N_{\mathbb{Q}(a)/\mathbb{Q}}(A) = \prod_{i=1}^{n} \sigma_i(A)$$

où $\sigma_i : \mathbb{Q}(a) \hookrightarrow \mathbb{C}$ est définie par $\sigma_i(a) = a_i$ et σ_i opère sur A en agissant sur chaque coefficient. Notant $M = \mathbb{Q}(a_1, \ldots, a_m)$ le corps de décomposition de P, d'après la théorie de Galois, on a $M^{Gal(M/\mathbb{Q})} = \mathbb{Q}$ (cela a été annoncé au chapitre X et sera démontré rigoureusement au chapitre XIV). On voit donc que $N_{\mathbb{Q}(a)/\mathbb{Q}}(A)$ appartient à $\mathbb{Q}[x]$.

Proposition 4. *Si A est irréductible dans $\mathbb{Q}(a)[x]$, alors $N_{\mathbb{Q}(a)/\mathbb{Q}}(A)$ est égal à une puissance d'un polynôme irréductible de $\mathbb{Q}[x]$.*

Corollaire 1. *On a $N_{\mathbb{Q}(a)/\mathbb{Q}}(x - b) = \mu_b^r$, où $r = [\mathbb{Q}(a) : \mathbb{Q}(b)]$.*

Démonstration. Soit $N_{\mathbb{Q}(a)/\mathbb{Q}}(A) = \prod_i N_i^{e_i}$ la factorisation en irréductibles sur $\mathbb{Q}$. Comme A divise $N_{\mathbb{Q}(a)/\mathbb{Q}}(A)$ dans $\mathbb{Q}(a)[x]$ et est irréductible dans $\mathbb{Q}(a)[x]$, il divise l'un des facteur, disons N_1. Alors $\sigma_i(A)$ divise $\sigma_i(N_1) = N_1$ pour tout i. Donc $N_{\mathbb{Q}(a)/\mathbb{Q}}(A)$ divise N_1^n dans $M[x]$, donc dans $\mathbb{Q}[x]$. Cela démontre la proposition. □

Le corollaire montre que $N_{\mathbb{Q}(a)/\mathbb{Q}}(x - b)$ coïncide avec le polynôme caractéristique de b. Enfin, faisons le lien avec la théorie du résultant, ce qui fournira une méthode efficace de calcul du polynôme caractéristique, donc du polynôme minimal.

On écrit $A(x) = \sum_i g_i(a)x^i$ et l'on définit $g_A(x, y) = \sum_i g_i(y)x^i$.

Proposition 5. *Avec les notations précédentes,*

$$N_{\mathbb{Q}(a)/\mathbb{Q}}(A) = Res_y(\mu_a(y), g_A(x, y)).$$

Démonstration. Considérons $g_A(x,y)$ comme un polynôme de $\mathbb{Q}(x)[y]$ et écrivons $g_A(x,y) = \lambda(x)\prod_{i=1}^{n}(y-r_i)$, où $n = \deg_y g$, dans un corps de décomposition. Comme $\mu_a(y) = \prod_{i=1}^{m}(y-a_i)$, le résultant s'exprime par

$$Res_y(\mu_a(y), g_A(x,y)) = \lambda(x)^m \prod_{i,j}(a_i - r_i) = \prod_{i=1}^{m}\lambda(x)\prod_{j=1}^{n}(a_i - r_i) = \prod_{i=1}^{m} g_A(x,a_i).$$

L'égalité en découle, puisque $g_A(x,a_i) = \sigma_i(A)$. □

6. Écrire une procédure `Norme:=proc(A,a,P)` calculant, par la méthode du résultant, la norme d'un polynôme A de $\mathbb{Q}(a)[x]$, où a est défini par une commande `alias(a=RootOf(P,x))`. Tester avec l'exemple $P = x^4 + x^3 + x^2 + x + 1$, $b = a + a^{-1}$ de la question précédente.

7. Enfin, écrire une procédure `minimal:=proc(b,a,P)` faisant appel à `Norme` et renvoyant le polynôme minimal de b (on pourra utiliser le polynôme dérivé obtenu avec la commande `diff`). Tester sur l'exemple habituel.

Factorisation dans une extension algébrique

La clef est encore la norme.

Proposition 6. *Supposons que $A \in \mathbb{Q}(a)[x]$ et $N_{\mathbb{Q}(a)/\mathbb{Q}}(A) \in \mathbb{Q}[x]$ soient tous les deux sans facteur carré. Soit $N_{\mathbb{Q}(a)/\mathbb{Q}}(A) = \prod_{j=1}^{s} N_j$ la factorisation en irréductibles dans $\mathbb{Q}[x]$. Alors $A = \prod \mathrm{pgcd}(A, N_j)$ est la factorisation de A en irréductibles dans $\mathbb{Q}(a)[x]$.*

Démonstration. Soit $A = \prod_{i=1}^{t} A_i$ la factorisation en irréductibles dans $\mathbb{Q}(a)[x]$. Comme $N_{\mathbb{Q}(a)/\mathbb{Q}}(A)$ est sans facteur carré, il en est de même de $N_{\mathbb{Q}(a)/\mathbb{Q}}(A_i)$. Ce dernier est donc un polynôme irréductible de $\mathbb{Q}(x)$ (en vertu de la proposition 4), c'est-à-dire un N_{j_i}. De plus, comme $N_{\mathbb{Q}(a)/\mathbb{Q}}(A_iA_j)$ divise $N_{\mathbb{Q}(a)/\mathbb{Q}}(A)$ pour $i \neq j$, donc est sans facteur carré, on voit que les $N_{\mathbb{Q}(a)/\mathbb{Q}}(A_i)$, donc les N_{j_i}, sont premiers entre eux deux à deux. Finalement, $s = t$ et l'on peut supposer que $N_{\mathbb{Q}(a)/\mathbb{Q}}(A_i) = N_i$, quitte à réordonner les facteurs. Enfin, N_i est premier avec $N_{\mathbb{Q}(a)/\mathbb{Q}}(A_j)$ donc avec A_j pour $i \neq j$. Ainsi $A_i = \mathrm{pgcd}(A, N_i)$ (à une unité près), ce qui démontre la proposition. □

Le lemme suivant permet de se ramener à la situation de la proposition.

Lemme 1. *Si $A \in \mathbb{Q}(a)[x]$ est sans facteur carré, alors il n'existe qu'un nombre fini de $k \in \mathbb{Q}$ tels que $N_{\mathbb{Q}(a)/\mathbb{Q}}(A(x-ka))$ ne soit pas sans facteur carré.*

Démonstration. Appelons $r_{i,j}$ les différentes racines de $\sigma_i(A)$. Alors $N_{\mathbb{Q}(a)/\mathbb{Q}}(A(x-ka))$ possède une racine multiple si et seulement s'il existe i_1, i_2, j_1 et j_2 tels que $r_{i_1,j_1}+ka_{j_1} = r_{i_2,j_2}+ka_{j_2}$, c'est-à-dire $k = (r_{i_1,j_1}-r_{i_2,j_2})/(a_{j_2}-a_{j_1})$. Il n'y a qu'un nombre fini de tels éléments k. □

8. Factoriser $P = x^4+x^3+x^2+x+1$ dans $\mathbb{Q}(a)[x]$, où a est une racine de P, en suivant la stratégie explicitée ci-dessus. On utilisera

```
collect(evala(Expand(P)),x)
```

pour développer une expression de $\mathbb{Q}(a)[x]$ et l'écrire comme un polynôme en x. Comparer avec le résultat de la commande `factor(P,a)` de Maple.

9. Sur cet exemple et notant toujours $b = a+a^{-1}$, quel est le polynôme minimal de a sur $\mathbb{Q}(b)$? (Il est nécessaire de définir proprement b avec une commande `RootOf` avant de pouvoir factoriser dans $\mathbb{Q}(b)[x]$.)

10. Justifier que $L = \mathbb{Q}(b)$ contient un sous-corps isomorphe à $K = \mathbb{Q}(a)$ si et seulement si μ_a possède une racine dans L. Écrire une procédure

```
test:=proc(P,Q)
```

renvoyant `true` or `false` et répondant à cette question pour $\mu_a = P$ et $\mu_b = Q$. Tester avec $P = x^4+x^3+x^2+x+1$ et $Q = x^2-5$, puis $Q = x^2+5$.

Remarque. Cet exemple est un cas particulier de la situation suivante : on a $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right) \subset \mathbb{Q}(\zeta_p)$, où $\mathbb{Q}(\zeta_p)$ désigne l'extension cyclotomique engendrée par une racine ζ_p primitive p-ième de l'unité.

XII

DÉCOMPOSITION DES POLYNÔMES CLÔTURES ALGÉBRIQUES

L'objet de ce chapitre est de répondre, par l'affirmative, aux questions posées dans l'introduction du chapitre IX. Précisément, on montre que, pour tout corps K et tout polynôme $f(X) \in K[X]$, il existe une extension « minimale » L/K dans laquelle le polynôme $f(X)$ se décompose en facteurs du premier degré. Autrement dit, L contient toutes les racines de l'équation $f(X) = 0$. Ce corps L est un **corps de décomposition** du polynôme $f(X)$ sur K.

De plus, on montre qu'il existe une extension algébrique E/K, unique à isomorphisme près, vérifiant la propriété ci-dessus pour tous les polynômes de $K[X]$, et aussi pour tous les polynômes de $E[X]$. Le corps E est une **clôture algébrique** de K.

XII.1. Corps de rupture et corps de décomposition d'un polynôme

Définition XII.1.1. Soient k un corps et $f(X)$ un polynôme non constant à coefficients dans k. Un **corps de rupture** K de f est une extension K/k telle que $f(X)$ admette une racine α dans K et $K = k(\alpha)$.

Quitte à remplacer $f(X)$ par l'un des ses facteurs irréductibles, **on supposera dans toute la suite que le polynôme $f(X)$ est irréductible dans $k[X]$.**

Proposition XII.1.1. *Pour tout corps k et tout polynôme $f(X)$ de $k[X]$, il existe un corps de rupture.*

Démonstration. On pose $K = k[X]/(f(X))$. Puisque $f(X)$ est irréductible, l'idéal $(f(X))$ est maximal, d'où K est un corps. On considère l'application $k \hookrightarrow k[X] \longrightarrow K$ qui permet d'identifier k à un sous-corps de K et donc de considérer l'extension K/k. On note α la classe de X dans K : alors dans K, $f(\alpha) = 0$, *i.e.* α est une racine de f. D'après le théorème (XI.1.1), $K = k(\alpha)$. □

***Exemples* XII.1.1.**

a) $k = \mathbb{Q}$, $f(X) = X^2 - 2$; $K = \mathbb{Q}(\sqrt{2})$.

b) $k = \mathbb{R}$, $f(X) = X^2 + 1$; $K = \mathbb{C}$.

***Proposition* XII.1.2 (prolongement des isomorphismes).** *Soient k et k' deux corps et $s : k \longrightarrow k'$ un isomorphisme de corps. On note $\overline{s} : k[X] \longrightarrow k'[X]$ l'isomorphisme d'anneaux prolongeant s ($\overline{s}(\sum_i a_i X^i) = \sum_i s(a_i)X^i$). Soit $f(X)$ un polynôme irréductible de $k[X]$.*

(i) *Le polynôme $\overline{s}(f)(X)$ est irréductible dans $k'[X]$.*

(ii) *Soient K (resp. K') une extension de k (resp. k') et α (resp. α') une racine de $f(X)$ (resp. $\overline{s}(f)(X)$) dans K (resp. K'). Il existe un unique isomorphisme de corps $\sigma : k(\alpha) \longrightarrow k'(\alpha')$ prolongeant s et tel que $\sigma(\alpha) = \alpha'$.*

Démonstration. L'assertion (i) est évidente.

Pour l'assertion (ii), montrons d'abord l'unicité : un élément y de $k(\alpha)$ s'écrit $y = a_o + \ldots + a_{n-1}\alpha^{n-1}$, où n est le degré de f. Donc

$$\sigma(y) = \sigma(a_o) + \ldots + \sigma(a_{n-1})\sigma(\alpha)^{n-1} = s(a_o) + \ldots + s(a_{n-1})\alpha'^{n-1},$$

d'où l'unicité.

Pour montrer l'existence, considérons le diagramme suivant, où Θ et Θ' sont les isomorphismes établis au théorème (XI.1.1) :

$$\begin{array}{ccc} k(\alpha) & \xrightarrow{\ \sigma\ } & k'(\alpha') \\ {\scriptstyle\Theta}\downarrow & & \downarrow{\scriptstyle\Theta'} \\ k[X]/(f(X)) & \xrightarrow[\ \overline{\overline{s}}\ ]{} & k'[X]/(\overline{s}(f)(X)) \end{array}$$

où $\overline{\overline{s}}$ est obtenu à partir de $\overline{s}$ par passage au quotient. On pose

$$\sigma = \Theta'^{-1} \circ \overline{\overline{s}} \circ \Theta.$$ □

***Proposition* XII.1.3.** *Soient k un corps et $f(X)$ un polynôme irréductible de $k[X]$. Deux corps de rupture de $f(X)$ sont k-isomorphes.*

Démonstration. On applique la proposition XII.1.2 avec $k' = k$ et $s = id_k$. □

Corollaire XII.1.1. *Soient K/k une extension et α et α' deux éléments de K algébriques sur k. Les assertions suivantes sont équivalentes :*

(i) *Les polynômes minimaux respectifs de α et α' sont égaux*

(ii) *Il existe un (unique) k-isomorphisme de $k(\alpha)$ sur $k(\alpha')$ appliquant α sur α'.*

Démonstration. L'assertion (i) implique (ii) car :

$$k(\alpha) \simeq k[X]/(M_\alpha(X)) = k[X]/(M_{\alpha'}(X)) \simeq k(\alpha').$$

D'autre part, l'assertion (ii) implique (i) : en effet, en notant σ le k-isomorphisme dont l'assertion (ii) suppose l'existence, pour tout polynôme $P(X) \in k[X]$ on a $\sigma(P(\alpha)) = P(\sigma(\alpha)) = P(\alpha')$. D'où $P(\alpha) = 0$ si et seulement si $P(\alpha') = 0$. On en déduit que $M_\alpha(X) = M_{\alpha'}(X)$. □

Définition XII.1.2. Lorsque les conditions équivalentes ci-dessus sont vérifiées, les éléments α et α' sont dits **conjugués**.

Remarque XII.1.1. On précisera cette notion au chapitre suivant.

Définition XII.1.3. Soient k un corps, $f(X)$ un polynôme non constant de $k[X]$ et K/k une extension. Le polynôme $f(X)$ se **décompose** dans K (ou est **scindé** dans K) si $f(X) = c(X-\alpha_1)\dots(X-\alpha_n)$, où $c, \alpha_1, \dots, \alpha_n$ sont dans K.

Autrement dit, dans $K[X]$ le polynôme s'écrit comme produit de facteurs de degré 1.

Exemples XII.1.2.

a) Le polynôme $X^3 - 1$ de $\mathbb{Q}[X]$ est scindé dans $\mathbb{C}$.

b) Le polynôme $X^4 - X^2 - 2$ de $\mathbb{Q}[X]$ est scindé dans $\mathbb{Q}(i, \sqrt{2})$ $(X^4 - X^2 - 2 = (X + i)(X - i)(X + \sqrt{2})(X - \sqrt{2}))$, mais pas dans $\mathbb{Q}(i)$ $(X^4 - X^2 - 2 = (X + i)(X - i)(X^2 - 2))$.

***Définition* XII.1.4.** Soient k un corps et $f(X)$ un polynôme non constant de $k[X]$. On appelle **corps de décomposition** de $f(X)$ sur k, une extension (algébrique) K/k telle que $f(X)$ est scindé dans K, de racines $\alpha_1, \ldots, \alpha_n$ et $K = k(\alpha_1, \ldots, \alpha_n)$.

***Théorème* XII.1.1.** *Soient k un corps et $f(X)$ un polynôme non constant de $k[X]$.*

(i) *Il existe un corps de décomposition de $f(X)$ sur k.*

(ii) *Deux corps de décomposition de $f(X)$ sur k sont k-isomorphes.*

Démonstration. (i). On fait un raisonnement par récurrence sur le degré de f.

– Si $d^\circ f = 1$, le résultat est évident.

– Supposons le résultat vrai pour tout corps k et tout polynôme de $k[X]$ de degré inférieur ou égal à $n-1$ ($n > 1$). Soit $f(X) \in k[X]$ de degré n. Si $f(X)$ n'est pas scindé dans k, il possède un facteur irréductible $g(X)$ avec $d^\circ g > 1$. Soit $k(\alpha_1)$ un corps de rupture de $g(X)$. Dans $k(\alpha_1)[X]$, on a $f(X) = (X - \alpha_1)h(X)$ et $d^\circ h = n - 1$. Donc $h(X)$ admet un corps de décomposition $k(\alpha_1)(\alpha_2, \ldots, \alpha_n) = K$, qui est donc un corps de décomposition de $f(X)$ sur k.

(ii). On démontre plus généralement le lemme suivant :

***Lemme* XII.1.1.** *Soient $s : k \longrightarrow k'$ un isomorphisme de corps, $f(X)$ un polynôme de $k[X]$, K (resp. K') un corps de décomposition de $f(X)$ (resp. $\overline{s}(f)(X)$). Alors, il existe un isomorphisme de corps $\sigma : K \longrightarrow K'$ qui prolonge s.*

Démonstration. – Si $d^\circ f = 1$, c'est évident.

– Supposons le résultat vrai pour tout corps et tout polynôme de degré inférieur ou égal à $n-1$ et soit f un polynôme de degré n. On considère

$$K = k(\alpha_1, \ldots, \alpha_n), \quad K' = k'(\alpha'_1, \ldots, \alpha'_n)$$

et

$$f(X) = c(X - \alpha_1)\ldots(X - \alpha_n), \quad \overline{s}(f)(X) = c'(X - \alpha'_1)\ldots(X - \alpha'_n).$$

Soit $g(X)$ un facteur irréductible de $f(X)$ admettant α_1 comme racine dans K. En renumérotant les α'_i, on peut supposer que $\overline{s}(g)(X)$ admet α'_1 comme racine

dans K'. D'après la proposition (XII.1.2), il existe $s_1 : k(\alpha_1) \longrightarrow k'(\alpha'_1)$, isomorphisme de corps qui prolonge s. D'où, par hypothèse de récurrence, il existe

$$\sigma : K = k(\alpha_1)(\alpha_2, \ldots, \alpha_n) \longrightarrow K' = k'(\alpha'_1)(\alpha'_2, \ldots, \alpha'_n)$$

qui prolonge s_1, donc aussi s. □

Pour démontrer l'assertion (ii) du théorème XII.1.1, on applique ce lemme avec $k' = k$ et $s = id_k$. □

Remarques XII.1.2.

a) Deux corps de décomposition d'un polynôme ne sont pas canoniquement isomorphes. En effet l'isomorphisme dépend de l'ordre dans lequel on écrit les racines du polynôme.

b) Deux polynômes irréductibles distincts peuvent avoir le même corps de décomposition (*cf.* exemples ci-dessous).

Exemples XII.1.3.

a) $f(X) = (X^2 - 3)(X^3 + 1)$ se décompose dans $\mathbb{C}$ en

$$f(X) = (X + \sqrt{3})(X - \sqrt{3})(X + 1)\left(X + \frac{1 + i\sqrt{3}}{2}\right)\left(X - \frac{1 - i\sqrt{3}}{2}\right).$$

On a donc un corps de décomposition de $f(X)$ qui est $\mathbb{Q}(i, \sqrt{3})$.

b) Les polynômes $f(X) = X^2 - 3$ et $g(X) = X^2 - 2X - 2$ sont irréductibles sur $\mathbb{Q}$ et admettent un corps de décomposition sur $\mathbb{Q}$ qui est $\mathbb{Q}(\sqrt{3})$.

c) On considère le polynôme $f(X) = X^2 + X + 1$ dans $\mathbb{Z}/2\mathbb{Z}[X]$. Ce polynôme est irréductible. Pour fabriquer un corps de décomposition sur $\mathbb{Z}/2\mathbb{Z}$ de $f(X)$, on doit adjoindre à $\mathbb{Z}/2\mathbb{Z}$ un élément α admettant $f(X)$ comme polynôme minimal. On a $\alpha^2 + \alpha + 1 = 0$, *i.e.* $\alpha^2 = -(\alpha + 1) = \alpha + 1$ (caractéristique 2). On considère $K = \{0, 1, \alpha, \alpha + 1\}$. On a alors

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

(pour le tableau de la multiplication, on a $\alpha(\alpha+1) = \alpha^2+\alpha = \alpha+1+\alpha = 2\alpha+1 = 1$). On en déduit que K est un corps et que

$$X^2+X+1 = (X-\alpha)(X+\alpha+1).$$

Autrement dit, le polynôme $f(X) = X^2+X+1 \in \mathbb{Z}/2\mathbb{Z}[X]$ est scindé dans $\mathbb{Z}/2\mathbb{Z}(\alpha)$, mais n'est pas scindé sur $\mathbb{Z}/2\mathbb{Z}$ qui est l'unique corps strictement contenu dans $\mathbb{Z}/2\mathbb{Z}(\alpha)$. Donc $\mathbb{Z}/2\mathbb{Z}(\alpha)$ est un corps de décomposition de X^2+X+1 sur $\mathbb{Z}/2\mathbb{Z}$.

Exercice XII.1.

1. Soient K un corps, $P(X)$ un polynôme de degré n de $K[X]$, E un corps de décomposition de $P(X)$. Montrer que $[E:K]$ divise $(n!)$.

2. Soient $K \subset \mathbb{C}$ un corps et $P(X) = X^3+pX+q$ un polynôme irréductible dans $K[X]$, dont on note a,b,c les racines dans $\mathbb{C}$. On pose $d = (a-b)(b-c)(c-a)$.

a) Écrire les relations entre coefficients et racines pour $P(X)$. En déduire que $b+c = -a$ et $(b-c)(-2q^2+\frac{q}{a}) = d$.

b) Montrer que $K(a,d)$ est un corps de décomposition de $P(X)$ sur K.

c) Montrer que $[K(a,d):K] = 3$ ou 6, suivant que le discriminant $D(P) = -4p^3-27q^2$ de P est un carré ou non dans K. (Indication : on remarquera que d^2 est symétrique en a,b,c ; il s'exprime donc en fonction des polynômes symétriques élémentaires, donc en fonction de p et q. Vérifier que $d^2 = D(P)$.)

XII.2. Clôtures algébriques

L'étude du paragraphe précédent consistait à construire, pour un polynôme non constant donné $f(X) \in k[X]$, une extension de k dans laquelle le polynôme $f(X)$ se décompose en un produit de polynômes du premier degré (corps de décomposition de $f(X)$ sur k).

L'objectif de ce paragraphe est de faire une construction analogue, valable pour tous les polynômes de $k[X]$.

Proposition XII.2.1. *Soit k un corps. Les assertions suivantes sont équivalentes :*

(i) *Tout polynôme non constant de $k[X]$ se décompose, dans $k[X]$, en un produit de polynômes du premier degré*

(ii) *Tout polynôme irréductible de $k[X]$ est du premier degré*

(iii) *Tout polynôme non constant de $k[X]$ a au moins une racine dans k*

(iv) *Toute extension algébrique de k est triviale (*i.e. *égale à k).*

Démonstration. Il est évident que (i) implique (ii).

Montrons que (ii) implique (iii) : puisque $k[X]$ est principal, tout polynôme $f(X)$ s'écrit comme produit de polynômes irréductibles, donc du premier degré. Un polynôme du premier degré a une racine dans k.

Pour montrer que (iii) implique (i), on procède par récurrence sur le degré de f :

- le résultat est vrai si $d^\circ f = 1$,
- supposons le résultat vrai si $d^\circ f \leqslant n-1$ et soit f un polynôme de degré n ; il existe $\alpha \in k$ tel que $f(\alpha) = 0$, d'où $f(X) = (X-\alpha)g(X)$ et le résultat en découle par hypothèse de récurrence.

Montrons que (ii) implique (iv) : soit α un élément algébrique sur k. Le polynôme minimal de α est de degré 1, donc $dim_k k(\alpha) = 1$, *i.e.* α appartient à k.

Montrons que (iv) implique (ii) : soit $f(X) \in k[X]$ un polynôme irréductible. Alors $k[X]/(f)$ est un corps qui est une extension finie, donc algébrique, de k. D'où $k[X]/(f) = k$ et $dim_k k[X]/(f) = 1 = d^\circ f$. □

Définition* XII.2.1.** Un corps k qui vérifie les conditions équivalentes ci-dessus est dit ***algébriquement clos.

***Théorème* XII.2.1.** *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

On va donner deux démonstrations de ce théorème.

Première démonstration. Soit $f(X)$ un polynôme non constant de $\mathbb{C}[X]$. Si $f(X)$ n'admet pas de racine dans $\mathbb{C}$, la fonction $\frac{1}{f(z)}$ est holomorphe dans $\mathbb{C}$. Puisque $\lim_{|z|\to+\infty} \frac{1}{f(z)} = 0$, la fonction $\frac{1}{f(z)}$ est bornée. Donc, d'après le théorème de Liouville, elle est constante, d'où une contradiction. □

Cette élégante démonstration analytique d'un résultat purement algébrique, comme les très nombreuses interactions de l'algèbre en analyse, est un exemple de l'unité des mathématiques que l'on a grandement tort de découper en « rondelles » !!

Deuxième démonstration (*cf.* [25]). Cette démonstration « essentiellement » algébrique utilise les ingrédients suivants :

a) Tout polynôme de $\mathbb{R}[X]$ de degré impair admet une racine dans $\mathbb{R}$ (c'est une conséquence du théorème des valeurs intermédiaires, seul ingrédient analytique de la démonstration).

b) Tout polynôme de $\mathbb{C}[X]$ de degré 2 a ses racines dans $\mathbb{C}$.

c) L'existence, pour tout polynôme, d'un corps de décomposition.

d) Les relations entre coefficients et racines d'un polynôme.

e) Le fait qu'un polynôme symétrique est un polynôme en les polynômes symétriques élémentaires.

On va montrer que tout polynôme non constant $P(X) \in \mathbb{C}[X]$ admet une racine dans $\mathbb{C}$.

Soit $\overline{P}(X)$ le polynôme dont les coefficients sont les conjugués de ceux de $P(X)$. Le polynôme $F(X) = P(X)\overline{P}(X)$ appartient à $\mathbb{R}[X]$. Si $F(X)$ a une racine $\alpha \in \mathbb{C}$, alors soit $P(\alpha) = 0$ et on a le résultat, soit $\overline{P}(\alpha) = 0$, mais alors $P(\overline{\alpha}) = 0$ et on a le résultat. Il suffit donc de montrer que tout polynôme non constant $f(X) \in \mathbb{R}[X] \subset \mathbb{C}[X]$ admet une racine dans $\mathbb{C}$. Posons $d = d^\circ f$ et écrivons $d = 2^n q$, q impair. On fait un raisonnement par récurrence sur n.

Si $n = 0$, le degré de f est impair, d'où le résultat d'après a).

Supposons le résultat vrai pour $d = 2^{n-1}q$ (et $f(X)$ unitaire). Dans un corps K de décomposition sur $\mathbb{C}$ de $f(X)$, $(\mathbb{C} \subset K)$, on a

$$f(X) = \prod_{i=1}^{d}(X - \alpha_i), \quad \alpha_1, \ldots, \alpha_d \in K.$$

Soit c un élément quelconque de $\mathbb{R}$. On pose

$$\beta_{ij} = \alpha_i + \alpha_j + c\alpha_i\alpha_j, \quad i \leqslant j.$$

Il y a $\frac{1}{2}d(d+1)$ éléments β_{ij}. Mais

$$\frac{1}{2}d(d+1) = 2^{n-1}q(d+1),$$

et $q(d+1)$ est impair.

On considère le polynôme

$$g(X) = \prod_{i \leqslant j}(X - \beta_{ij}).$$

Ce polynôme a pour coefficients les polynômes symétriques élémentaires en les β_{ij}, donc des polynômes symétriques en les α_i, à coefficient réels (puisque $c \in \mathbb{R}$). Donc, d'après e), ce sont des polynômes à coefficients réels en les polynômes symétriques élémentaires en les α_i. Par conséquent, d'après d), les coefficients de $g(X)$ sont réels. Comme son degré est de la forme $2^{n-1}q'$, avec q' impair, par hypothèse

de récurrence, il admet une racine $z_c \in \mathbb{C}$. Cette racine est nécessairement l'un des β_{ij}. Donc il existe $i(c)$ et $j(c)$ tels que

$$\alpha_{i(c)} + \alpha_{j(c)} + c\alpha_{i(c)}\alpha_{j(c)} = z_c.$$

Ceci est vrai pour tout $c \in \mathbb{R}$. Or $\mathbb{R}$ est infini et l'ensemble des couples $(i, j), i \leqslant j$, est fini. Donc il existe $c' \neq c$ tel que $i(c) = i(c')$ et $j(c) = j(c')$. Notons r et s ces indices. On a

$$\alpha_r + \alpha_s + c\alpha_r\alpha_s = z_c \quad \in \mathbb{C}$$
$$\alpha_r + \alpha_s + c'\alpha_r\alpha_s = z_{c'} \quad \in \mathbb{C}.$$

D'où $\alpha_r + \alpha_s$ et $\alpha_r\alpha_s$ appartiennent à $\mathbb{C}$ et on en déduit que α_r et α_s sont racines d'une équation du second degré à coefficients dans $\mathbb{C}$. Donc, d'après b), α_r et α_s appartiennent à $\mathbb{C}$. D'où $f(X)$ admet une racine dans $\mathbb{C}$. □

Proposition XII.2.2. *Un corps algébriquement clos est infini.*

Démonstration. Si K est un corps fini, $K = \{a_1 = 0, a_2 = 1, a_3, \ldots, a_n\}$, le polynôme

$$f(X) = \prod_{i=1}^{n}(X - a_i) + 1$$

n'a pas de racine dans K, puisque pour tout i, $f(a_i) = 1$. □

Remarque XII.2.1. On en déduit donc qu'un corps fini n'est jamais algébriquement clos.

Définition XII.2.2. Une extension E/K est une **clôture algébrique** de K si c'est une extension algébrique et si le corps E est algébriquement clos.

Remarque XII.2.2. D'après la proposition (XII.2.1.(iv)), un corps algébriquement clos est sa propre clôture algébrique.

Théorème XII.2.2. *Tout corps admet une clôture algébrique.*

Démonstration. Soient K un corps et $\mathcal{F}$ l'ensemble des polynômes non constants de $K[X]$. On considère l'anneau $K[X_f]_{f\in\mathcal{F}}$ (*cf.* TR.VIII.D) et l'idéal $\mathfrak{a} = (f(X_f))_{f\in\mathcal{F}}$ engendré par les $f(X_f)$.

Montrons que $\mathfrak{a} \neq K[X_f]$: si $\mathfrak{a} = K[X_f]$, alors 1 s'écrit comme combinaison à coefficients dans $K[X_f]$ d'une famille finie $f_i(X_{f_i}), i = 1, \ldots, n$. Soit Ω un corps

de décomposition sur K du polynôme $\prod_{1\leqslant i\leqslant n} f_i(X)$. Dans Ω, en spécialisant X_{f_i} en une racine du polynôme $f_i(X)$ pour $i = 1, \ldots, n$ et X_f en 0 pour les autres f, on obtient $0 = 1$, ce qui est impossible.

Puisque $\mathfrak{a} \neq K[X_f]$, soit $\mathfrak{m}$ un idéal maximal de $K[X_f]$ contenant $\mathfrak{a}$. On pose $K_1 = K[X_f]/\mathfrak{m}$. On identifie K à un sous-corps de K_1, *i.e.* K_1/K est une extension. Soit α_f la classe de X_f dans K_1 : alors $f(\alpha_f) = 0$ et α_f est une racine dans K_1 du polynôme $f(X)$. Puisque ceci est vrai pour tous les α_f, où f parcourt $\mathcal{F}$, K_1 est algébrique sur K et tout polynôme non constant de $K[X]$ a une racine dans K_1.

On construit K_2 à partir de K_1 comme K_1 à partir de K et, plus généralement, K_n à partir de K_{n-1} par le même procédé, de sorte que tout polynôme irréductible de $K_{n-1}[X]$ admet une racine dans K_n.

On pose $\overline{K} = \bigcup_{n\in\mathbb{N}} K_n$. Cette réunion a un sens puisque les K_n, $n \in \mathbb{N}$, forment une suite croissante. D'autre part, pour tous $x, y \in \overline{K}$, il existe $p \in \mathbb{N}$ tel que $x \in K_p$ et $y \in K_p$: on considère l'addition et la multiplication de x et y effectuées dans K_p. Puisque, pour tous $p, q \in \mathbb{N}$, $p \leqslant q$, K_p est un sous-corps de K_q, *i.e.* les structures de corps de K_p et K_q sont compatibles, les opérations ci-dessus définissent bien une structure de corps sur $\overline{K}$.

Montrons que $\overline{K}/K$ est algébrique : Soit $\alpha \in \overline{K}$, alors il existe $n \in \mathbb{N}$, tel que α appartienne à K_n. Comme $K = K_0 \subset K_1 \subset \ldots \subset K_n$ et que chaque K_{i+1}/K_i algébrique, K_n/K est algébrique et α est algébrique sur K.

Montrons que $\overline{K}$ est algébriquement clos : soit $f(X) \in \overline{K}[X]$. Il existe $n \in \mathbb{N}$ tel que $f(X) \in K_n[X]$; il a donc une racine dans K_{n+1}, donc dans $\overline{K}$. □

Exercice XII.2. (¶) Soient p un nombre premier et $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$.

a) Montrer que si x est un élément non nul de $\overline{\mathbb{F}_p}$, x est une racine de l'unité.

b) Montrer que si $q|q'$, alors $\mathbb{F}_q \subset \mathbb{F}_{q'}$.

c) Soit $q = p^n$. Montrer qu'il existe un unique sous-corps de $\mathbb{F}_{p^{n!}}$ isomorphe à $\mathbb{F}_q$.

d) Montrer que $K = \bigcup_{n\in\mathbb{N}^*} \mathbb{F}_{p^{n!}}$ est un corps et que c'est une clôture algébrique de tout corps fini de caractéristique p (donc de $\mathbb{F}_p$).

Théorème XII.2.3. *Soient F/K et E/F des extensions algébriques et $\overline{K}$ une clôture algébrique de K. Tout K-morphisme de F dans $\overline{K}$ se prolonge en un K-morphisme de E dans $\overline{K}$.*

Démonstration. Il faut montrer qu'il existe un K-morphisme $E \longrightarrow \overline{K}$ tel que le diagramme

$$\begin{array}{ccc} F & \longrightarrow & E \\ \downarrow & & \downarrow \\ \overline{K} & = & \overline{K} \end{array}$$

commute. Soit $\mathcal{E}$ l'ensemble des couples (L, h) avec $K \subset L \subset E$ et $h : L \longrightarrow \overline{K}$ un K-morphisme.

L'ensemble $\mathcal{E}$ est non vide puisque (F, f) appartient à $\mathcal{E}$. On munit $\mathcal{E}$ d'une relation d'ordre

$$((L, h) \leqslant (L', h')) \Longleftrightarrow (L \subset L' \text{ et } h'_{|L} = h).$$

Alors $\mathcal{E}$ est un ensemble inductif, d'où il existe un élément maximal $(L_0, h_0) \in \mathcal{E}$ majorant (F, f) (*cf.* l'appendice à la fin de cet ouvrage). Montrons, par l'absurde, que $L_0 = E$. Si L_0 est strictement contenu dans E, il existe $\alpha \in E \setminus L_0$ et soit $M_\alpha(X)$ le polynôme minimal de α sur L_0, $M_\alpha(X) = \sum_i a_i X^i$. Le polynôme $\sum_i h_0(a_i)X^i$ appartient à $\overline{K}[X]$ et a donc au moins une racine $\Xi \in \overline{K}$ ($\overline{K}$ algébriquement clos). Considérons $g : L_0(\alpha) \longrightarrow \overline{K}$ définie par $\alpha \mapsto \Xi$ et $g|_{L_0} = h_0$. Alors $(L_0(\alpha), g)$ majore strictement l'élément maximal (L_0, h_0), d'où une contradiction. □

Corollaire XII.2.1. *Soient K un corps et $\overline{K}$ une clôture algébrique de K. Toute extension algébrique de K se plonge dans $\overline{K}$.*

Démonstration. Soit E/K une extension algébrique. D'après le théorème (XII.2.3), il existe $f : E \longrightarrow \overline{K}$ qui prolonge $K \hookrightarrow \overline{K}$. Comme f est forcément injectif, E peut être identifié à un sous-corps de $\overline{K}$. □

Remarque XII.2.3. On peut donc identifier toute extension algébrique d'un corps K à un sous-corps d'une clôture algébrique $\overline{K}$ de K (*cf.* remarque XII.2.4 ci-dessous).

Corollaire XII.2.2. *Soient K un corps, $\overline{K}$ une clôture algébrique de K, E et F des sous-corps de $\overline{K}$ contenant K. Tout K-morphisme de E dans F se prolonge en un K-automorphisme de $\overline{K}$.*

Démonstration. On a

$$E \xrightarrow{f} F \longrightarrow \overline{K}.$$

On applique le théorème (XII.2.3) : alors $E \longrightarrow F \longrightarrow \overline{K}$ se prolonge en

$$\overline{K} \xrightarrow{\tilde{f}} \overline{K}.$$

Puisque $\overline{K}/K$ est algébrique, $\tilde{f}$ est un automorphisme (d'après la proposition (XI.1.5)). □

Corollaire XII.2.3. *Deux clôtures algébriques d'un corps sont isomorphes.*

Démonstration. Soit Ω une clôture algébrique de K : l'extension Ω/K étant algébrique, d'après le théorème (XII.2.3), il existe un K-morphisme $s : \Omega \longrightarrow \overline{K}$ tel que $s(\Omega) \simeq \Omega$. Donc $s(\Omega)$ est algébriquement clos. On en déduit que $\overline{K}$ est une extension algébriquement close de $s(\Omega)$, donc $\overline{K} = s(\Omega)$. □

Proposition XII.2.3. *Soient K un corps, L/K une extension algébrique, $\overline{K}$ une clôture algébrique de K et $\overline{L}$ une clôture algébrique de L. Alors $\overline{K}$ et $\overline{L}$ sont K-isomorphes.*

Démonstration. On a $K \subset L \subset \overline{L}$ et $\overline{L}/L$ est algébrique. Donc $\overline{L}/K$ est algébrique et, puisque $\overline{L}$ est un corps algébriquement clos, $\overline{L}$ est une clôture algébrique de K. D'après le corollaire (XII.2.3), $\overline{K}$ et $\overline{L}$ sont K-isomorphes. □

Remarques XII.2.4.

a) Il n'y a pas, en général, unicité de l'isomorphisme du corollaire XII.2.3. On ne doit donc pas parler de LA clôture algébrique d'un corps, mais d'UNE clôture algébrique.

b) Soient K un corps et E_i/K, $i \in I$, une famille quelconque d'extensions. On démontrera au TR.XII ci-après qu'il existe une extension E/K telle que, pour tout $i \in I$, E_i s'identifie à une sous-extension de E, *i.e.* il existe un K-morphisme injectif $u_i : E_i \longrightarrow E$. En considérant une clôture algébrique $\overline{E}$ de E, on en déduit que, pour toute famille donnée d'extensions E_i/K, les E_i, $i \in I$, peuvent être considérés comme des sous-corps d'une extension algébriquement close de K.

THÈMES DE RÉFLEXION

♠ TR.XII. Plongements dans une clôture algébrique

L'objectif de ce TR est de démontrer le résultat annoncé à la remarque (XII.2.3) ci-dessus, *i.e.* pour toute famille donnée d'extensions E_i/K, il existe une extension E/K telle que, pour tout $i \in I$, E_i s'identifie à une sous-extension de E.

Pour cela, nous sommes amenés à introduire la notion de produit tensoriel de K-espaces vectoriels et de K-algèbres. Cette notion, capitale en mathématiques, est définie pour les modules sur un anneau, mais, pour simplifier notre propos, nous ne l'étudierons que dans le cadre des espaces vectoriels et des algèbres sur un corps commutatif.

Dans tout ce qui suit, K est un corps commutatif.

Produit tensoriel de deux K-espaces vectoriels et de deux K-algèbres

Soient E et F deux K-espaces vectoriels : le ***produit tensoriel*** de E et F est le K-espace vectoriel engendré par les éléments $x \otimes y$, $x \in E$, $y \in F$, soumis aux relations

$(x + x') \otimes y - x \otimes y - x' \otimes y$,
$x \otimes (y + y') - x \otimes y - x \otimes y'$,
$k(x \otimes y) - kx \otimes y$,
$k(x \otimes y) - x \otimes ky$,
avec $x, x' \in E$, $y, y' \in F$, $k \in K$.

On le note $E \otimes F$, ou $E \otimes_K F$ si l'on veut spécifier le corps de base.

On définit une application $\varphi : E \times F \longrightarrow E \otimes F$ par $\varphi(x, y) = x \otimes y$, $x \in E$, $y \in F$. Nous allons montrer que le couple $(E \otimes F, \varphi)$ est solution d'un problème universel.

1. *Montrer que pour tout K-espace vectoriel G et toute application K-bilinéaire $f : E \times F \longrightarrow G$, il existe une unique application K-linéaire $g : E \otimes F \longrightarrow G$ telle que $f = g \circ \varphi$.*

D'après l'unicité de la solution d'un problème universel, le problème universel précédent caractérise le produit tensoriel de deux K-modules.

2. *Montrer que si $B_E = \{e_i\}_{i\in I}$ et $B_F = \{f_j\}_{j\in J}$ sont des bases des K-espaces vectoriels E et F respectivement, alors $\{e_i \otimes f_j\}_{(i,j)\in I\times J}$ est une base de $E \otimes F$.*

On en déduit que si $x = \sum_i a_i e_i$ et $y = \sum_j b_j f_j$ sont des éléments de E et F respectivement (les coefficients a_i et b_j sont nuls, sauf un nombre fini d'entre eux), on a $x \otimes y = \sum_{i,j}(a_i b_j)(e_i \otimes f_j)$.

3. *Montrer que l'application définie par $x \otimes y \mapsto y \otimes x$ est un isomorphisme de K-espaces vectoriels de $E \otimes F$ sur $F \otimes E$.*

4. *Montrer que les K-espaces vectoriels $E \otimes (F \otimes G)$ et $(E \otimes F) \otimes G$ sont canoniquement isomorphes.*

5. *Montrer que les K-espaces vectoriels $E \otimes_K K$ et E sont canoniquement isomorphes.*

On suppose maintenant que E et F sont des K-algèbres associatives, commutatives, unitaires. On remarquera qu'en identifiant, au moyen des morphismes structuraux, K à une sous-algèbre de E et F respectivement, on peut supposer que l'élément unité de K est aussi l'élément unité commun de E et F.

6. *Montrer que le K-espace vectoriel $E \otimes F$, muni de la multiplication définie par $(x \otimes y)(x' \otimes y') = xx' \otimes yy'$, que l'on étend linéairement, est une K-algèbre associative, commutative, dont l'unité est $1 \otimes 1$.*

7. *Montrer que l'application $x \mapsto x \otimes 1$ (resp. $y \mapsto 1 \otimes y$) est un isomorphisme de E (resp. F) sur une sous-algèbre E_1 (resp F_1) de $E \otimes F$.*

Produits tensoriels infinis

On considère une famille quelconque $(E_i)_{i\in I}$ de K-espaces vectoriels. On définit le produit tensoriel $\bigotimes_{i\in I} E_i$ comme le quotient du K-espace vectoriel des combinaisons linéaires formelles d'éléments de $\prod_{i\in I} E_i$, à coefficients dans K, par le sous-espace vectoriel engendré par les éléments du type suivant :

a) $(x_i) + (y_i) - (z_i)$, avec $x_l + y_l = z_l$ pour un indice l arbitraire et $x_i = y_i = z_i$ pour tout $i \neq l$.

b) $(x_i) - k(y_i)$, avec $k \in K$ et $x_l = ky_l$ pour un indice arbitraire l et $x_i = y_i$ pour tout $i \neq l$.

On désigne par φ l'application multilinéaire $\prod_{i\in I} E_i \longrightarrow \bigotimes_{i\in I} E_i$ définie par $(x_i) \mapsto \otimes_{i\in I} x_i$.

8. *Montrer que* $(\bigotimes_{i\in I} E_i, \varphi)$ *est solution d'un problème universel analogue à celui exposé ci-dessus.*

9. *Si* $(I_l)_{l\in L}$ *est une partition de* I*, montrer que* $\bigotimes_{i\in I} E_i$ *est canoniquement isomorphe au* K*-espace vectoriel* $\bigotimes_{l\in L} F_l$*, avec* $F_l = \bigotimes_{i\in I_l} E_i$*.*

On suppose que $(E_i)_{i\in I}$ est une famille de K-algèbres associatives, commutatives, unitaires.

10. *Montrer que le* K*-espace vectoriel* $\bigotimes_{i\in I} E_i$*, muni de la multiplication définie par* $(\otimes_{i\in I} x_i)(\otimes_{i\in I} y_i) = \otimes_{i\in I}(x_i y_i)$*, est une* K*-algèbre associative, commutative, unitaire.*

Pour tout indice $l \in I$, on considère le morphisme d'algèbres

$$f_l : E_l \longrightarrow \bigotimes_{i\in I} E_i$$

défini par $f_l(x) = \otimes_{i\in I} y_i$, avec $y_l = x$ et $y_i = 1$ pour tout $i \neq l$.

11. *Montrer que pour tout* $l \neq m$*, tout élément de* $f_l(E_l)$ *commute avec tout élément de* $f_m(E_m)$*.*

On appelle ***produit tensoriel des algèbres*** E_i, que l'on note $\bigotimes_{(I)} E_i$, la sous-algèbre de $\bigotimes_{i\in I} E_i$ engendrée par les $f_i(E_i)$. Elle est donc formée des sommes finies d'éléments de la forme $\otimes_{i\in I} x_i$, où $x_i = 1$, sauf pour un nombre fini d'indices.

12. *Montrer que pour tout* $l \in I$*,* f_l *est un isomorphisme de* E_l *sur la sous-algèbre* $f_l(E_l)$ *de* $\bigotimes_{(I)} E_i$*.*

Comme dans le cas de deux algèbres, on peut identifier les éléments unités de K, $\bigotimes_{(I)} E_i$ et $f_i(E_i)$, i parcourant I.

Cas des extensions

On suppose maintenant que $(E_i)_{i\in I}$ est une famille d'extensions de K. On pose $F = \bigotimes_{(I)} E_i$ et on considère un idéal maximal $\mathfrak{m}$ de F.

13. *Montrer que pour tout* $i \in I$*,* $f_i(E_i) \cap \mathfrak{m}$ *est un idéal de* $f_i(E_i)$*.*

14. *En déduire que, pour tout* $i \in I$*, la restriction à* $f_i(E_i)$ *de la projection canonique* $\pi : F \longrightarrow F/\mathfrak{m}$ *est injective.*

15. *Déduire de ce qui précède que la réunion des corps* $\pi(f_i(E_i))$*,* $i \in I$*, engendre* $F/\mathfrak{m}$*.*

16. *Montrer que, en posant* $E = F/\mathfrak{m}$ *et* $u_i = \pi \circ f_i$*,* $i \in I$*, les conditions décrites à la remarque (XII.2.3) sont satisfaites.*

This page intentionally left blank

TRAVAUX PRATIQUES

TP.XII. Calculs dans les corps de nombres

Ce TP fait suite au TP.XI et poursuit l'étude des corps de nombres, c'est-à-dire des extensions finies de $\mathbb{Q}$. On commence par illustrer la notion de corps de rupture et de corps de décomposition, puis on s'intéresse à des extensions $\mathbb{Q}(a,b)$. Par exemple, comment trouver le polynôme minimal de $b+\lambda a$, $\lambda \in \mathbb{Q}$, à partir des polynômes minimaux de a et b ? On y répond en utilisant la norme, dont il a été question au sein du TP.XI. Cela permet de donner un algorithme de détermination d'un élément primitif de l'extension $\mathbb{Q}(a,b)/\mathbb{Q}$. Pour finir, on démontre certaines identités algébriques remarquables dues à Ramanujan, en calculant dans des corps de nombres.

Corps de rupture, corps de décomposition

Soient $P \in \mathbb{Q}[x]$ et $\mathbb{Q}(a)$ l'extension de $\mathbb{Q}$ définie par une racine a d'un polynôme irréductible $Q \in \mathbb{Q}[x]$. A une constante près, Q est le polynôme minimal μ_a de a sur $\mathbb{Q}$ et $\mathbb{Q}(a) \simeq \mathbb{Q}[x]/(Q)$. Après avoir défini algébriquement a par `alias(a=RootOf(Q,x))` sous MAPLE, la commande `factor(P,a)` donne la factorisation de P, dans $\mathbb{Q}(a)[x]$, en produit de polynômes irréductibles. On obtient la liste des facteurs (avec multiplicités) par `factors(P,a)` et la liste des racines (avec multiplicités) de P dans $\mathbb{Q}(a)$ par `roots(P,a)`. Les commandes `factor(P)`, `factors(P)` et `root(P)` ont trait à la décomposition et aux racines sur $\mathbb{Q}$.

Si P est irréductible et si l'on prend $Q = P$, le corps $\mathbb{Q}(a)$ est un corps de rupture de P. Il y a autant de tels corps que de racines complexes de P, mais la « définition » `alias(a=RootOf(P,x))` ne tient compte que de P. Comme on l'a vu, l'évaluation algébrique dans $\mathbb{Q}(a)$ est équivalente à calculer dans $\mathbb{Q}[x]/(P)$, la racine a correspondant à la classe de x modulo P. C'est la construction du corps

de rupture. Préciser de quelle racine il s'agit par `alias(a=RootOf(P,x,index=i))` n'influe pas sur ces algorithmes algébriques.

Les calculs sur les polynômes à coefficients dans $\mathbb{Q}(a)$ s'effectuent comme suit : `evala(Quo(A,B,x))` et `evala(Rem(A,B,x))` pour le quotient et le reste, `evala(Gcd(A,B))` pour le calcul du pgcd.

Un corps de décomposition n'est pas unique à isomorphisme *unique* près, aussi doit-on parler d'« un » corps de décomposition. Par contre, lorsque l'on fixe une clôture algébrique (par exemple $\mathbb{C}$) dans laquelle P est scindé, c'est le sous-corps engendré par le corps de base et les racines de P. Aussi peut-on parler « du » corps de décomposition de P, puisque Maple possède un algorithme numérique de calcul d'approximation des racines (commande `evalf(allvalues(a))`) et ordonne les racines à partir d'un ordre sur $\mathbb{C}$ qui est donc en arrière-plan. Par contre, on dira que $\mathbb{Q}[x]/(Q)$ est « un » corps de décomposition de P (si c'est le cas), puisqu'il n'est pas fait référence à $\mathbb{C}$.

1. a) Prenons $P = x^3 + 2x^2 - x - 1$. Tester l'irréductibilité de P sur $\mathbb{Q}$ et vérifier que tout corps de rupture de P est également corps de décomposition. Les racines de P s'expriment donc comme des polynômes en l'une quelconque d'entre elles. On dit que le polynôme irréductible P est *normal*.

b) Décomposer $P = x^3+7x^2+19x+21$ sur $\mathbb{Q}$. En déduire un corps de rupture et le corps de décomposition. Décomposer également P sur $\mathbb{Q}(i)$ et $\mathbb{Q}(i\sqrt{3})$ (où $\mathbb{C} = \mathbb{R}(i)$, $i^2 = -1$). Que dire de ces deux corps par rapport à P ? Décrire un isomorphisme $\mathbb{Q}[x]/(x^2+3) \xrightarrow{\sim} \mathbb{Q}[x]/(x^2+4x+7)$ entre les deux corps de décomposition (il y a deux tels isomorphismes).

2. Soient $P = x^3 - 2x + 2$ et a une racine de P. Vérifier que la liste des facteurs de la décomposition en irréductibles de P dans $\mathbb{Q}(a)[x]$ contient un élément R de degré 2 et définir sous Maple une racine b de ce facteur (la commande `op([2,i,1],factors(P,a))` permet d'obtenir le i-ième facteur, mais attention, l'ordre des facteurs diffère *a priori* à chaque appel de la commande `factors` ; se rappeler qu'un algorithme probabiliste se cache derrière cette commande).

Décomposer P dans $\mathbb{Q}(a,b)[x]$ à l'aide de la commande `factor(P,{a,b})`. En déduire le degré sur $\mathbb{Q}$ du corps de décomposition de P. Vérifier que ce degré divise $\deg(P)$! (*cf.* exercice XII.1). Enfin, tester la ligne suivante :

```
> PolynomialTools[Split](P,x,'r'); r;
```

Maple sait donc déterminer un corps de décomposition, du moins pour des polynômes de bas degré.

Il est possible de mener des calculs dans $\mathbb{Q}(a,b) \simeq \mathbb{Q}(a)[x]/(R)$: tester `evala(a^7*b^3)` et vérifier que le polynôme en b obtenu, à coefficients dans $\mathbb{Q}(a)$, correspond au reste de la division euclidienne de a^7x^3 par R dans $\mathbb{Q}(a)[x]$.

Autour du théorème de l'élément primitif

Le théorème suivant sera démontré au chapitre XIII :

Théorème 1. *Toute extension finie $L/\mathbb{Q}$ admet un élément primitif c (*i.e. *$L = \mathbb{Q}(c)$).*

Ainsi, pour a et b deux nombres algébriques (de degrés respectifs m et n sur $\mathbb{Q}$), l'extension $\mathbb{Q}(a,b)/\mathbb{Q}$ est monogène. Mieux encore, on démontre que l'on peut prendre $c = b + \lambda a$, avec λ un entier tel que $1 \leqslant \lambda \leqslant (m-1)(n-1)+1$. Le théorème en découle, par récurrence.

3. (a) Définir $a = \sqrt{2}$ et $b = \sqrt{3}$ à l'aide de la commande `RootOf`. Quel est le degré de $\mathbb{Q}(a,b)$ sur $\mathbb{Q}$?

(b) Soit a une racine de $P = x^3+x+1$ et b une racine de $Q = x^3-x^2+4x-3$. Factoriser Q dans $\mathbb{Q}(a)[x]$. De quel facteur a est-il racine ? On constatera qu'il y a, en fait, deux choix possibles, qui conduisent à des extensions $\mathbb{Q}(a,b) = (\mathbb{Q}(a))(b)$ de degrés sur $\mathbb{Q}$ différents. En d'autre termes, les polynômes minimaux de a et de b ne déterminent pas l'extension $\mathbb{Q}(a,b)/\mathbb{Q}$. Si l'on suppose de plus que a et b sont réels, de quel facteur s'agit-il ? Une façon de s'en sortir est de recourir à des méthodes numériques : évaluer chaque facteur en des approximations numériques de a (parmi `evalf(allvalues(a))`) et b. En déduire le degré de $\mathbb{Q}(a,b)/\mathbb{Q}$ dans ce cas précis.

Remarque. On peut aussi préciser le choix de la racine directement au niveau du `RootOf` grâce à l'option `index=`, ce qui permet l'évaluation numérique *via* `evalf` *a posteriori*. Cependant, on se gardera de procéder ainsi systématiquement, car le recours à des méthodes numériques n'est qu'occasionnel.

4. On va maintenant déterminer le polynôme minimal sur $\mathbb{Q}$ d'un élément $c = b + \lambda a$, $\lambda \in \mathbb{Q}$, en fonction des polynômes minimaux $P = \mu_a$ de a sur $\mathbb{Q}$ et $R = \mu_{b,\mathbb{Q}(a)}$ de b sur $\mathbb{Q}(a)$, ce qui définit bien l'extension $\mathbb{Q}(a,b)/\mathbb{Q}$. Démontrer que la norme (voir TP.XI) $N = N_{\mathbb{Q}(a)/\mathbb{Q}}(P(x-\lambda a))$ est un multiple du polynôme minimal μ_c de c sur $\mathbb{Q}$. (On utilisera la proposition 4 du TP.XI). En déduire une procédure `minimal2:=proc(lambda,R,a,P)` renvoyant μ_c. L'appliquer aux deux exemples de la question 3, afin de déterminer des éléments primitifs.

5. On va automatiser cela : avec les notations de la question précédente, démontrer que c est primitif si et seulement si N est sans facteur carré. En déduire une procédure `primitif:=proc(R,a,P)` renvoyant un couple (λ, μ) tel que $b + \lambda a$ soit un élément primitif de polynôme minimal μ sur $\mathbb{Q}$. Tester avec $P = x^3 - 2x + 2$ et R le facteur de degré 2 obtenu en décomposant P sur $\mathbb{Q}(a)$. En déduire un élément primitif du corps de décomposition de P.

On désire maintenant exprimer a et b en fonction d'un élément primitif $c = b + \lambda a$ de $\mathbb{Q}(a, b)$, connaissant les polynômes minimaux μ_a et μ_b, et λ ayant été déterminé par la méthode exposée précédemment.

***Proposition* 1.** *Avec les notations précédentes (et $\lambda \neq 0$), on a*

$$x - a = \operatorname{pgcd}(\mu_a, \mu_b(c - \lambda x)).$$

On obtient donc a en prenant l'opposé du coefficient constant de $\operatorname{pgcd}(\mu_a, \mu_b(c - \lambda x))$, ce pgcd (unitaire) étant calculé dans $\mathbb{Q}(c)[x]$.

Démonstration. Écrivons la décomposition en irréductibles $\mu_b = P_1 \dots P_r$ dans $\mathbb{Q}(a)[x]$ et supposons que b soit racine de P_1. Alors μ_c est de degré mn, où l'on a posé $m = \deg \mu_a$ et $n = \deg P_1$. Sur $\mathbb{C}$, les polynômes se scindent en $\mu_a = \prod_{i=1}^{m}(x - a_i)$ et $P_1 = \prod_{j=1}^{n}(x - b_{1,j})$ et l'on peut supposer que $a = a_1$ et $b = b_{1,1}$.

Soit $\sigma_i : \mathbb{Q}(a) \hookrightarrow \mathbb{C}$ les m plongements définis par $\sigma_i(a) = a_i$; le polynôme ${}^{\sigma_i}P_1$ obtenu en appliquant σ_i aux coefficients de P_1 se décompose sur $\mathbb{C}$ en ${}^{\sigma_i}P_1 = \prod_{j=1}^{n}(x - b_{i,j})$, tous les $b_{i,j}$ étant distincts deux à deux car μ_b est à racines simples. On a alors mn plongements $\mathbb{Q}(c) = \mathbb{Q}(a, b) \hookrightarrow \mathbb{C}$ qui peuvent être définis par $\sigma_{i,j}(a) = a_i$ et $\sigma_{i,j}(b) = b_{i,j}$. Ils sont deux à deux distincts, donc aussi les conjugués $\sigma_{i,j}(c) = b_{i,j} + \lambda a_i$.

Revenons à $\operatorname{pgcd}(\mu_a, \mu_b(c - \lambda x))$: ses racines sont parmi les a_i. Or a_i est racine de $\mu_b(c - \lambda x)$ si et seulement si $c - \lambda a_i$ est racine de μ_b. De plus, c n'est égal à $b_{i,j} + \lambda a_i$ que pour $a_i = a$ (et $b_{i,j} = b$). Le pgcd vaut donc $x - a$. □

6. Mener les calculs sur l'exemple de la question 3 (b), lorsque $\mathbb{Q}(a, b) = \mathbb{Q}(c)$ est de degré 6 sur $\mathbb{Q}$. On exprimera a et b comme des polynômes en c. Vérifier numériquement que les différentes approximations complexes de $a = a(c)$, obtenues lorsque c décrit les racines de son polynôme minimal μ_c, coïncident avec les valeurs des racines de μ_a.

Effectuer également une vérification de type algébrique : décomposer P sur $\mathbb{Q}(c)$, vérifier que $a(c)$ est racine et que le produit des deux autres facteurs de degré 1 (ce polynôme s'avère scindé) coïncide avec le facteur indécomposable de degré 2 sur $\mathbb{Q}(a)$.

Enfin, écrire une procédure `primitif2:=proc(R,a,P)` renvoyant, en fonction de l'extension $\mathbb{Q}(a,b)$ définie par $P = \mu_a$ et $R = \mu_{b,\mathbb{Q}(a)}$, un quadruplet $(\lambda, \mu_c, a(c), b(c))$, où $c = b + \lambda a$ est un élément primitif de polynôme minimal μ_c, et $a(c)$, $b(c)$ sont deux polynômes en c correspondant à l'écriture de a et b dans $\mathbb{Q}(c)$ respectivement. (Attention, les `alias(RootOf)` ne fonctionnent pas à l'intérieur d'une procédure : il faut se contenter d'un `RootOf`.) Tester en comparant avec le résultat de la commande

```
evala(Primfield({a,RootOf(R,x)}))
```

de Maple.

7. Le problème de la détermination d'un élément primitif se pose parfois, dans la pratique, en les termes suivants : on se donne deux éléments de $\mathbb{Q}(c)$, définis comme des polynômes $U(c)$ et $V(c)$, et il s'agit de déterminer un élément primitif $W(c)$ de $\mathbb{Q}(U(c),V(c))/\mathbb{Q}$. On cherche alors W sous la forme $W = U + \lambda V$ et l'on remarque que $W(c)$ convient si et seulement si $V(c)$ appartient à $\mathbb{Q}(W(c))$. C'est un problème d'algèbre linéaire : notant $[\mathbb{Q}(c) : \mathbb{Q}] = n$, on écrit $V(c)$ dans la base $(1, c, \ldots, c^{n-1})$ (on obtient un vecteur v) ainsi que la matrice M dont les vecteurs colonnes sont les $W(c)^i$, $0 \leqslant i \leqslant n-1$ (ces derniers engendrent $\mathbb{Q}(W(c))$ qui est de dimension au plus n sur $\mathbb{Q}$). La condition revient à vérifier que la matrice augmentée `<v|M>` (en notation Maple) a même rang que M, ce que l'on réalise avec la commande `LinearAlgebra[Rank]`.

Traiter l'exemple

$$\mu_c = x^6 - 12x^4 + 36x^2 + 76,$$

$$U(c) = 4/9 + c/2 - 5c^2/18 + c^4/36,\ V(c) = -8/9 + 5c^2/9 - 1/18c^4,$$

en essayant $\lambda = 1$, puis 2. Enfin, écrire une procédure

```
primitif3:=proc(H,c,U,V)
```

renvoyant (λ, μ_W) en fonction de c, de polynôme minimal $\mu_c = H$, U et V.

Identités remarquables de Ramanujan

On désire vérifier les deux identités suivantes, observées par le mathématicien Ramanujan :

$$\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{1/9} - \sqrt[3]{2/9} + \sqrt[3]{4/9}, \tag{XII.1}$$

$$\sqrt{\sqrt[3]{5} - \sqrt[3]{4}} = (\sqrt[3]{2} + \sqrt[3]{20} - \sqrt[3]{25})/3. \tag{XII.2}$$

8. Première identité.

(a) Vérifier que l'identité est vraie à 10^{-30} près (utiliser la commande `Digits`).

(b) Définir sous Maple $\sqrt[3]{2}$ comme racine a de son polynôme minimal sur $\mathbb{Q}$, puis déterminer le polynôme minimal de $b = \sqrt[3]{a-1}$ sur $\mathbb{Q}(a)$ et, enfin, sur $\mathbb{Q}$. Définir alors directement b sous Maple comme racine d'un polynôme irréductible de $\mathbb{Q}[x]$.

(c) Factoriser le polynôme $x^3 - 1/9$ dans $\mathbb{Q}(b)[x]$ et montrer qu'il possède une unique racine dans $\mathbb{Q}(b)$, notée c. Pourquoi s'agit-il de $\sqrt[3]{1/9}$? Exprimer c comme un polynôme en b. Faire de même avec $x^3 - 2/9$ et $x^3 - 4/9$, dont les racines (uniques) dans $\mathbb{Q}(b)$ seront notées d et e respectivement.

(d) Vérifier que $2c^2 = de$ à l'aide d'une évaluation algébrique. Est-ce étonnant ? Démontrer que $b = c - d + e$ et conclure.

9. Seconde identité.

(a) Vérifier que l'identité est vraie à 10^{-30} près.

(b) Définir sous Maple $\sqrt[3]{5}$ (resp. $\sqrt[3]{4}$) comme racine a (resp. b) de son polynôme minimal sur $\mathbb{Q}$. Vérifier que $c = a - b$ est un élément primitif de $\mathbb{Q}(a, b)$ et calculer son polynôme minimal sur $\mathbb{Q}$.

(c) Calculer le polynôme minimal de $d = \sqrt{c}$ sur $\mathbb{Q}$. (On commencera par déterminer le polynôme minimal sur $\mathbb{Q}(c)$.)

(d) Vérifier que $x^3 - 2$ possède une unique racine dans $\mathbb{Q}(d)$, notée e. Pourquoi s'agit-il de $\sqrt[3]{2}$? Exprimer e comme un polynôme en d. Faire de même avec $x^3 - 20$ et $x^3 - 25$, dont les racines (uniques) dans $\mathbb{Q}(d)$ seront notées f et g respectivement.

(e) Démontrer que $d = (e + f - g)/3$ et conclure.

XIII

EXTENSIONS NORMALES, SÉPARABLES

Ayant trouvé une extension L/K dans laquelle un polynôme $f(X) \in K[X]$ admet une racine, il n'est pas certain que L contienne toutes les racines de $f(X)$. Par exemple, $\mathbb{R}$ ne contient qu'une seule racine du polynôme $X^3-1 \in \mathbb{Q}[X]$. Pour pallier cet inconvénient, nous introduisons la notion d'extension **normale**. Si une telle extension contient une racine d'un polynôme, elle les contient toutes. De ce fait, elle a un très bon comportement par rapport à l'action du groupe de Galois. Cependant, si les racines ne sont pas toutes simples, les corps de décomposition du polynôme « manquent » de K-automorphismes. Ceci n'est pas le cas lorsque l'extension est **séparable**.

Il apparaîtra, au chapitre suivant, que les extensions qui peuvent être étudiées grâce à leur groupe de Galois sont les extensions normales et séparables.

Toutes les extensions considérées dans ce chapitre sont algébriques.

XIII.1. Extensions et éléments conjugués

Dans ce paragraphe, on fixe un corps k : on sait (*cf.* remarque XII.2.3), que toutes les extensions de k sont plongées dans une extension algébriquement close Ω de k. Dans toute la suite, on prendra $\Omega = \overline{k}$.

Définition XIII.1.1. Soient E/k et F/k deux extensions. On dit que E/k et F/k sont **conjuguées** dans Ω s'il existe un k-automorphisme σ de Ω tel que $\sigma(E) = F$. Deux éléments α et β de Ω sont **conjugués** sur k s'il existe un k-automorphisme σ de Ω tel que $\sigma(\alpha) = \beta$.

Proposition XIII.1.1. *Soient α un élément algébrique sur k et $\beta \in \Omega$. Les assertions suivantes sont équivalentes :*

(i) *β est conjugé de α sur k*

(ii) *β est racine de $M_\alpha(X)$*

(iii) *Il existe un k-morphisme $\sigma : k(\alpha) \longrightarrow \Omega$ tel que $\sigma(\alpha) = \beta$.*

Démonstration. C'est une conséquence évidente des corollaires (XII.1.1) et (XII.2.2). □

XIII.2. Extensions normales

On étudie maintenant une notion intermédiaire entre corps de décomposition d'un polynôme et corps algébriquement clos.

Proposition XIII.2.1. *Soient K/k une extension algébrique, $\overline{k}$ une clôture algébrique de k contenant K. Les assertions suivantes sont équivalentes :*

(i) *K est le corps de décomposition sur k d'une famille de polynômes de $k[X]$*

(ii) *Tout k-morphisme σ de K dans $\overline{k}$ est un k-automorphisme de K,* i.e. *$\sigma(K) = K$*

(iii) *Tout polynôme irréductible de $k[X]$ qui a une racine dans K est scindé dans K.*

Démonstration. Montrons que (i) implique (ii) : considérons $\{f_i(X)\}_{i\in I}$ une famille de polynômes de $k[X]$ dont K soit un corps de décomposition. Soit $\alpha \in K$ une racine d'un $f_i(X)$; pour tout k-morphisme $\sigma : K \longrightarrow \overline{k}$ on a : $0 = \sigma(f_i(\alpha)) = f_i(\sigma(\alpha))$. Puisque K est un corps de décomposition des $f_i(X)$, il est engendré par les racines des $f_i(X)$, donc $\sigma(K) \subset K$, *i.e.* σ est un k-endomorphisme de K. Mais K/k est algébrique, donc, d'après la proposition (XI.1.5), c'est un k-automorphisme.

Montrons que (ii) implique (i) : soient $\alpha \in K$ et $M_\alpha(X)$ son polynôme minimal. Soit β une racine de $M_\alpha(X)$ dans $\overline{k}$. Alors, d'après la proposition (XII.1.2), il existe un k-isomorphisme $\sigma : k(\alpha) \longrightarrow k(\beta)$ tel que $\sigma(\alpha) = \beta$. On a $k(\alpha) \longrightarrow k(\beta) \longrightarrow \overline{k}$. Comme $k(\alpha) \subset K$, d'après le théorème (XII.2.3), σ se prolonge en un k-morphisme $\widetilde{\sigma} : K \longrightarrow \overline{k}$, qui, par hypothèse (ii), est un k-automorphisme de K. Donc $\widetilde{\sigma} = \sigma(\alpha) = \beta \in K$. Ceci montre que toutes les racines de $M_\alpha(X)$ sont dans K. Ceci est valable pour tous les $M_\alpha(X)$, $\alpha \in K$, donc K est un corps de décomposition d'une famille de polynômes de $k[X]$.

La démonstration ci-dessus prouve que (ii) implique (iii). Montrons que (iii) implique (ii) : soit $\sigma : K \longrightarrow \overline{k}$ un k-morphisme. Soient $\alpha \in K$ et $M_\alpha(X)$ son polynôme minimal. Alors $\sigma(\alpha)$ est racine de $M_\alpha(X)$ donc, par hypothèse (iii), appartient à K. D'où σ est un k-endomorphisme de K et, d'après la proposition (XI.1.5), est un k-automorphisme de K. □

Définition XIII.2.1. Une extension algébrique K/k satisfaisant aux conditions équivalentes ci-dessus est dite **normale**.

Exemples XIII.2.1.

a) Un corps de décomposition d'un polynôme irréductible de $k[X]$ est une extension normale de k. Par exemple, une clôture algébrique $\overline{k}$ de k est une extension normale de k.

b) $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$ est une extension normale de $\mathbb{Q}$, car corps de décomposition sur $\mathbb{Q}$ du polynôme $X^3 - 2$.

c) $\mathbb{Q}(\sqrt[3]{2})$ n'est pas une extension normale de $\mathbb{Q}$, car le polynôme minimal de $\sqrt[3]{2}$ n'est pas scindé dans $\mathbb{Q}(\sqrt[3]{2})$.

Remarque XIII.2.1.

a) Une extension K/k est normale si et seulement si elle est identique à toutes ses conjuguées sur k, en vertu de la proposition (XIII.2.1.(ii)).

b) Si K/k est normale et $\alpha \in K$, tous les conjugués de α appartiennent à K.

Exercice XIII.1.

1. Montrer que toute extension de degré 2 est normale.

2. Soient k un corps, $\overline{k}$ une clôture algébrique de k et L/k une extension algébrique de k, $L \in \overline{k}$. Montrer que $k(\bigcup_\sigma \sigma(L))$, où σ parcourt l'ensemble des k-morphismes de L dans $\overline{k}$, est une extension normale de k (qui contient L).

Remarque XIII.2.2. On sait que si k est un corps et $\overline{k}$ est une clôture algébrique de k, toute extension algébrique L/k se plonge dans $\overline{k}$ (corollaire XII.2.1). L'exercice XIII.1.2 ci-dessus montre donc que, pour toute extension algébrique L/k, il existe une extension normale N/k (contenue dans $\overline{k}$), avec $k \subset L \subset N$ (*cf.* aussi définition (XIII.2.2) et suivants ci-dessous).

Exercice XIII.2. Soient $k \subset \mathbb{C}$ un corps et $f(X) \in k[X]$ un polynôme irréductible de degré 3 et de discriminant $D = d^2$, $d \in \mathbb{C}$ (pour la définition du discriminant *cf.* l'exercice XII.1). Soit $a \in \mathbb{C}$ une racine de $f(X)$. Montrer que l'extension $k(a)/k$ est normale si et seulement si d est dans k. (Indication : on utilisera les résultats de l'exercice XII.1.)

Proposition XIII.2.2. *Soient L/K et K/k des extensions. Si L/k est normale, alors L/K est normale.*

Démonstration. Tout K-morphisme de L dans $\overline{k}$ est aussi un k-morphisme, donc un automorphisme de L. □

Attention. *Avec les notations ci-dessus :*

a) L/k normale $\not\Longrightarrow$ K/k normale.

b) (K/k normale et L/K normale) $\not\Longrightarrow$ L/k normale.

En effet, considérons les exemples suivants :
a) $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$.

b) $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[4]{2})$. Alors $[K : k] = [L : K] = 2$, les extensions K/k et L/K sont donc normales, mais L/k n'est pas normale car L ne contient pas toutes les racines du polynôme $X^4 - 2$.

Remarque XIII.2.3. On donnera, à la proposition (XIII.2.6) ci-dessous, sous certaines hypothèses, une condition nécessaire et suffisante pour que L/k normale implique K/k normale.

Proposition XIII.2.3. *Soit K_i/k, $i \in I$, une famille d'extensions normales, $K_i \subset \overline{k}$. Alors $\bigcap_{i\in I} K_i$ et $k\big(\bigcup_{i\in I} K_i\big)$ sont des extensions normales de k.*

Démonstration. Soit σ un k-automorphisme de $\overline{k}$. Alors $\sigma(K_i) = K_i$, pour tout $i \in I$, d'où $\sigma(\bigcap_{i\in I} K_i) = \bigcap_{i\in I} K_i$ et $\bigcap_{i\in I} K_i$ est une extension normale de k. On vérifie que $\sigma(k(\bigcup_{i\in I} K_i)) = k(\bigcup_{i\in I} K_i)$, d'où $k(\bigcup_{i\in I} K_i)$ est normale. □

Définition XIII.2.2. Soit K/k une extension algébrique. On appelle extension ***normale*** de k ***engendrée*** par K, ou ***clôture normale*** de l'extension K/k, la plus petite extension normale de k (dans $\overline{k}$) contenant K.

Remarque XIII.2.4.

a) La remarque qui suit l'exercice XIII.1 et la proposition précédente montrent que la définition ci-dessus est consistante. Il est clair que la clôture normale de K/k est l'intersection de toutes les extensions normales de k (dans $\overline{k}$) contenant K.

b) Cette clôture normale est indépendante, à K-isomorphisme près, de la clôture algébrique choisie $\overline{k}$. Notons N la clôture normale de K/k contenue dans $\overline{k}$. Soient Σ une autre clôture algébrique de k et M la clôture normale de K/k

contenue dans Σ. Alors $\overline{k}$ et Σ sont deux clôtures algébriques de k, donc de K. D'après le corollaire (XII.2.3), il existe un K-isomorphisme $\theta : \overline{k} \longrightarrow \Sigma$ et, d'après le théorème (XII.2.3), l'inclusion $i : K \longrightarrow \overline{K}$ se prolonge en un K-morphisme $j : M \longrightarrow \overline{K}$. Le morphisme composé $\theta \circ j$ est un K-morphisme de M dans Σ et, puisque M/k est normale, $\theta \circ j(M) = M$. On en déduit que $j(M)/k$ est une extension normale contenant K, d'où $N \subset j(M)$. Mais, si N était strictement contenu dans $j(M)$, alors $\theta(N)$ serait une extension normale de k contenant K et strictement contenue dans $\theta \circ j(M) = M$, ce qui est impossible puisque M est la plus petite extension normale de k contenant K et contenue dans Σ. Donc $N = j(M)$ et $M = \theta \circ j(M) = \theta(N)$. Ainsi, le K-morphisme $\theta : \overline{k} \longrightarrow \Sigma$ induit un K-isomorphisme de N sur M.

Proposition XIII.2.4. *Soient k un corps, $\overline{k}$ une clôture algébrique de k et A une partie de $\overline{k}$. Si B est l'ensemble de tous les conjugués sur k des éléments de A, $k(B)$ est l'extension normale de k engendrée par $k(A)$.*

Démonstration. Toute extension normale de k contenant A doit contenir B (*cf.* remarque XIII.2.1.b), donc $k(B)$. De plus, $k(B)$ est une extension normale de k, car pour tout k-automorphisme σ de $\overline{k}$, on a $\sigma(B) \subset B$, donc $\sigma(k(B)) = k(\sigma(B)) \subset k(B)$. Évidemment $k(B) \supset k(A)$. C'est donc l'extension normale de k engendrée par $k(A)$. □

Corollaire XIII.2.1.

(i) *Si K/k est une extension algébrique finie, l'extension normale de k engendrée par K est finie sur k.*

(ii) *Toute extension normale N/k est réunion des sous-corps de N qui sont des extensions normales finies de k.*

Démonstration. (i). On a $K = k(A)$ avec $Card(A) < +\infty$, donc l'ensemble B des conjugués est fini, puisque les éléments de B ont mêmes polynômes minimaux que les éléments de A. D'où $[k(B) : k] < +\infty$.

(ii). L'extension N est réunion des $k(A)$, où A parcourt l'ensemble des parties finies de N. Donc N est réunion des extensions normales de k engendrées par les $k(A)$ qui, d'après (i), sont finies sur k. □

Proposition XIII.2.5. *Soient E/k une extension algébrique normale, L et L' deux corps intermédiaires. Les corps L et L' sont conjugués si et seulement s'il existe un k-automorphisme s de E tel que $s(L) = L'$.*

Démonstration. Si L et L' sont conjugués, il existe un k-automorphisme σ de $\overline{k}$ tel que $\sigma(L) = L'$. On a donc un k-morphisme

$$s : E \hookrightarrow \overline{k} \xrightarrow{\sigma} \overline{k}$$

tel que $s(L) = L'$. Puisque E/k est normale, s est un k-automorphisme de E. Réciproquement, si s est un k-automorphisme de E, il se prolonge en un k-automorphisme σ de $\overline{k}$ et si $s(L) = L'$, alors $\sigma(L) = L'$. □

Proposition XIII.2.6. *Soient E/k une extension normale, $Gal(E/k)$ son groupe de Galois, L un corps intermédiaire, $k \subset L \subset E$. Les assertions suivantes sont équivalentes :*

(i) *L'extension L/k est normale.*

(ii) *Pour tout s dans $Gal(E/k)$, $s(L) = L$.*

Démonstration. C'est une conséquence de la remarque (XIII.2.1.a) et de la proposition (XIII.2.5). □

XIII.3. Extensions séparables

Définition XIII.3.1. Soit k un corps.

a) Soient $f(X) \in k[X]$ un polynôme non constant et K un corps de décomposition de $f(X)$ sur k. On dit que le polynôme $f(X)$ est **séparable** sur k s'il n'a que des racines simples dans K.

b) Soient K/k une extension algébrique et α un élément de K. On dit que α est **séparable** sur k si son polynôme minimal sur k est séparable sur k.

c) Une extension algébrique K/k est dite ***séparable*** si tous les éléments de K sont séparables sur k.

Exemples XIII.3.1.

a) Si k est un corps de caractéristique nulle, tout polynôme irréductible non constant de $k[X]$ est séparable sur k (*cf.* corollaire XI.1.1).

b) Donnons ici un exemple d'un polynôme irréductible non séparable. Soient p un nombre premier, $k = \mathbb{Z}/p\mathbb{Z}$, a un élément transcendant sur k. On pose $K = k(a)$ et on considère $f(X) = X^p - a \in K[X]$. Soient E un corps de décomposition de $f(X)$ sur K et α une racine de $f(X)$ dans E. On a $\alpha^p = a$, d'où, dans $K[X]$, on a

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

L'unicité de la décomposition d'un polynôme en produit de polynômes irréductibles implique que α est l'unique racine de $f(X)$, de multiplicité p.

Montrons maintenant que le polynôme $f(X)$ est irréductible. En effet, si $f(X) = g(X)h(X) \in K[X]$, avec g et h polynômes unitaires, $d^\circ g(X) < d^\circ f(X)$ et $d^\circ h(X) < d^\circ f(X)$, alors, d'après ce qui précède, $g(X) = (X-\alpha)^s$ avec $0 < s < p$, d'où $\alpha^s \in K$. Mais puisque p est premier et $s < p$, il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tels que $1 = us + vp$, d'où $\alpha = \alpha^{us+vp} = (\alpha^s)^u(\alpha^p)^v = (\alpha^s)^u a^v \in K$, *i.e.* $\alpha \in K$. On peut donc exprimer α sous la forme $\alpha = \frac{m(a)}{n(a)}$, avec $m(a) \in k[a]$ et $n(a) \in k[a]$, $m(a)$ et $n(a)$ premiers entre eux. On en déduit que $a = \frac{m(a)^p}{n(a)^p}$, *i.e.* $an(a)^p - m(a)^p = 0$, d'où la contradiction puisque l'élément a est transcendant sur k.

c) Un élément α d'une extension algébrique K/k est séparable sur k si et seulement si le nombre de conjugués de α sur k est égal au degré du polynôme minimal de α sur k.

On a fait au b) ci-dessus une démonstration « à la main », mais on aurait pu appliquer le critère général suivant, qui est une conséquence immédiate de la proposition (XI.1.6) : si k est un corps de caractéristique $p > 0$, un polynôme irréductible $f(X) \in k[X]$ est séparable si et seulement si $f(X) \notin k[X^p]$.

La proposition (XIII.3) ci-dessous précisera l'ordre de multiplicité des racines dans le cas des corps de caractéristique $p > 0$.

Exercice XIII.3. Soient K un corps de caractéristique p et E/K une extension finie. Montrer que, pour tout élément α de E dont le polynôme minimal $M_\alpha(X)$ n'est pas séparable, le degré $[K(\alpha) : K]$ est divisible par p. En déduire que si $[E : K]$ est premier avec p, l'extension E/K est séparable.

Proposition XIII.3.1. *Soient K/k une extension algébrique, $\overline{k}$ une clôture algébrique de K et σ un morphisme de corps de k dans $\overline{k}$. Alors le cardinal de l'ensemble S_σ des prolongements de σ à K (*i.e. *des morphismes de corps de K dans $\overline{k}$ dont la restriction à k est σ) est indépendant de σ.*

Démonstration. L'isomorphisme $\sigma : k \longrightarrow \sigma(k)$ se prolonge en un k-automorphisme θ de $\overline{k}$ (corollaire XII.2.2). Alors l'application $\lambda \mapsto \theta \circ \lambda$ est une bijection de l'ensemble des $\overline{k}$-morphismes $K \longrightarrow \overline{k}$ dans S_σ. □

Remarque XIII.3.1.

a) Dans ce qui précède, nous avons considéré les k-morphismes $K \longrightarrow \overline{k}$, *i.e.* le cas où σ est l'inclusion $k \subset \overline{k}$. Nous avons besoin de faire varier σ pour démontrer la proposition (XIII.3.3) ci-dessous.

b) Le cardinal de S_σ est également indépendant du choix de $\overline{k}$. En effet, cela résulte du fait que le nombre de k-morphismes $K \longrightarrow \overline{k}$ est indépendant de $\overline{k}$: si Ω est une autre clôture algébrique de k et si $\varphi : \overline{k} \longrightarrow \Omega$ est un k-isomorphisme (corollaire XII.2.3), alors $\sigma \mapsto \varphi \circ \sigma$ induit une bijection de l'ensemble des k-morphismes $K \longrightarrow \overline{k}$ dans l'ensemble des k-morphismes $K \longrightarrow \Omega$.

Définition XIII.3.2. Avec les notations précédentes, on appelle ***degré séparable*** de K sur k, ou ***degré séparable de l'extension algébrique*** K/k, le cardinal de S_σ. Lorsque ce cardinal est fini, on le note $[K : k]_s$.

Proposition XIII.3.2. *Si α est algébrique sur k et si $K = k(\alpha)$, alors $[K : k]_s$ est égal au nombre de racines distinctes du polynôme minimal sur k de α, dans un corps de décomposition sur k de ce polynôme.*

Démonstration. Par définition, $[k(\alpha) : k]_s = card(S_\sigma)$, avec $\sigma : k \longrightarrow \overline{k}$. On considère l'application $\lambda \mapsto \lambda(\alpha)$, où λ appartient à S_σ. C'est, d'après (1.3), une application bijective de S_σ sur l'ensemble des racines distinctes du polynôme minimal de α. □

Proposition XIII.3.3. *Soient K/k et L/K des extensions telles que L/k soit algébrique.*

(i) *$[L : k]_s$ est fini si et seulement si $[L : K]_s$ et $[K : k]_s$ sont finis et alors $[L : k]_s = [L : K]_s[K : k]_s$.*

(ii) *Si K/k est finie, $[K : k]_s \leqslant [K : k]$.*

Démonstration. (i). Soit $\sigma : k \hookrightarrow \overline{k}$ et soit $\sigma_i : K \longrightarrow \overline{k}$, $i \in I$, la famille des prolongements à K de σ, distincts. On a $[K : k]_s = Card(I)$. Soit $i \in I$ et soit $\sigma_{i,j} : L \longrightarrow \overline{k}$, $j \in J(i)$, les prolongements distincts de σ_i à L. On a $[L : K]_s = Card(J(i))$. Tout $\sigma : L \longrightarrow \overline{k}$ est un prolongement d'un σ_i, d'où $\sigma_{i,j}, (i, j) \in I \times J(i)$, est la famille des prolongements distincts de σ à L. D'où

$$[L : k]_s = Card(I \times J(i)) = [K : k]_s[L : K]_s.$$

(ii). On a $K = k(\alpha_1, \ldots, \alpha_n)$ et $k \subset k(\alpha_1) \subset \ldots \subset k(\alpha_1, \ldots, \alpha_n) = K$. À chaque étape, on a, d'après la proposition (XIII.3.2), $[K_i(\alpha_{i+1}) : K_i]_s \leqslant [K_i(\alpha_{i+1}) : K_i]$, d'où $[K : k]_s \leqslant [K : k]$. □

Théorème XIII.3.1. *Si K/k une extension finie, les assertions suivantes sont équivalentes :*

(i) *L'extension K/k est séparable*

(ii) $[K : k]_s = [K : k]$.

Démonstration. Cas monogène : On suppose $K = k(\alpha)$, α algébrique sur k. On a alors les équivalences suivantes :

(1) (α séparable sur k) $\Longleftrightarrow [k(\alpha) : k]_s = [k(\alpha) : k]$

(2) ($[k(\alpha) : k]_s = [k(\alpha) : k]$) $\Longleftrightarrow k(\alpha)/k$ séparable.

En effet :

(1) découle de la proposition (XIII.3.2) (*i.e.* $[k(\alpha) : k]_s$ = nombre de racines distinctes de $M_\alpha(X)$) ; pour (2), remarquons que $k(\alpha)/k$ séparable implique α séparable sur k, d'où $[k(\alpha) : k]_s = [k(\alpha) : k]$ d'après (1). D'autre part, montrons que

$$([k(\alpha) : k]_s = [k(\alpha) : k]) \Longrightarrow k(\alpha)/k \text{ séparable.}$$

Soit $\beta \in k(\alpha)$, on a :

$$[k(\alpha) : k(\beta)]_s[k(\beta) : k]_s = [k(\alpha) : k]_s.$$

Mais α est séparable sur $k(\beta)$, car le polynôme minimal de α sur $k(\beta)$ divise le polynôme minimal de α sur k, d'où :

$$[k(\alpha) : k(\beta)]_s = [k(\alpha) : k(\beta)].$$

On en déduit que

$$[k(\beta) : k]_s = [k(\alpha) : k]_s/[k(\alpha) : k(\beta)]_s = [k(\alpha) : k]/[k(\alpha) : k(\beta)] = [k(\beta) : k].$$

D'où, d'après (1), β est séparable sur k et $k(\alpha)$ séparable sur k.

Cas général : Si $K = k(\alpha_1, \ldots, \alpha_n)$, on applique le cas monogène et la multiplicativité du degré et du degré séparable. □

Corollaire XIII.3.1. *Soit K/k une extension algébrique. Les assertions suivantes sont équivalentes :*

(i) *L'extension K/k est séparable*

(ii) *Pour tout corps intermédiaire E tel que l'extension E/k soit finie,* $[E : k]_s = [E : k]$.

Démonstration. En effet, si K/k est séparable et si $k \subset E \subset K$, alors E/k est séparable et on applique le théorème (XIII.3.1). Réciproquement, pour tout $\alpha \in K$, en prenant $E = k(\alpha)$, on déduit de l'hypothèse que α est séparable sur k.

□

Les extensions séparables satisfont la propriété de transitivité :

Théorème XIII.3.2. *Soient K/k et L/K des extensions algébriques. Alors L/k est une extension séparable si et seulement si K/k et L/K sont des extensions séparables.*

Démonstration. Remarquons d'abord que si $[L : k] < +\infty$, on a

$$[L : k] = [L : K][K : k] \text{ et } [L : k]_s = [L : K]_s[K : k]_s$$

et

$$[L : K]_s \leqslant [L : K] \text{ et } [K : k]_s \leqslant [K : k],$$

d'où

$$([L : k]_s = [L : k]) \Longleftrightarrow ([L : K]_s = [L : K] \quad \text{et} \quad [K : k]_s = [K : k]).$$

Considérons maintenant le cas général.

Si L/k est séparable, il est évident que K/k est séparable. Pour tout $\alpha \in L$, le polynôme minimal de α sur k, considéré à coefficients dans K, s'annule en α. Donc $M_\alpha(X)_{|K}$ divise $M_\alpha(X)_{|k}$ et α est séparable sur K, d'où le résultat.

Supposons que K/k et L/K sont séparables. Soit $\alpha \in L$: il existe K' tel que $k \subset K' \subset K$, $[K' : k] < +\infty$ avec $M_\alpha(X)_{|K} \in K'[X]$. On pose $L' = K'(\alpha)$; or, on sait que K/k séparable implique que K'/k est séparable et, puisque L'/K' est séparable (car α est séparable sur K et $M_\alpha(X)_{|K'} = M_\alpha(X)_{|K}$), d'après la démonstration dans le cas fini, on a L'/k séparable, d'où α est séparable sur k.

□

Nous avons vu précédemment (Remarque 3.2), que si k est de caractéristique nulle, tout polynôme irréductible non constant de $k[X]$ est séparable. C'est donc le cas du polynôme minimal d'un élément algébrique sur k. Nous allons donner ici un résultat qui précise l'ordre de multiplicité de ses racines dans le cas où le corps k est de caractéristique $p > 0$.

Proposition XIII.3.4. *Soient k un corps de caractéristique $p > 0$, $\overline{k}$ une clôture algébrique de k, $\alpha \in \overline{k}$ et $M_\alpha(X)$ le polynôme minimal de α sur k. Toutes les racines de $M_\alpha(X)$ sont d'ordre de multiplicité p^μ, pour un certain entier $\mu \geqslant 0$. De plus, α^{p^μ} est séparable sur k et*

$$[k(\alpha) : k] = p^\mu [k(\alpha) : k]_s.$$

Démonstration. Montrons d'abord que toutes les racines $\alpha = \alpha_1, ..., \alpha_n$ de $M_\alpha(X)$ ont même ordre de multiplicité. Pour tout i, $1 \leqslant i \leqslant n$, il existe un k-isomorphisme $\sigma : k(\alpha) \longrightarrow k(\alpha_i)$ tel que $\sigma(\alpha) = \alpha_i$, d'où un k-automorphisme $\overline{\sigma}$ de $\overline{k}$ qui prolonge σ. On a $\overline{\sigma}(M_\alpha)(X) = M_\alpha(X) = \prod_{i=1}^{n}(X - \sigma(\alpha_i))^{m_i}$ (car $\sigma(\alpha_i)$ parcourt les conjugués de α_i, *i.e.* les racines de $M_\alpha(x)$), où m_i est l'ordre de multiplicité de α_i. Comme $k[X]$ est principal, par unicité de la décomposition en facteurs irréductibles, on a $m_i = m_1$. Ceci est vrai pour tout i. Donc toutes les racines ont même ordre de multiplicité.

On considère l'entier $\mu \geqslant 0$ tel que $M_\alpha(X) = h(X^{p^\mu})$ et $h \notin k[X^p]$. Alors, d'après (XI.1.6), α^{p^μ} est racine d'un polynôme séparable et, en comparant les degrés de $M_\alpha(X)$ et $h(X)$, on a :

$$[k(\alpha) : k(\alpha^{p^\mu})] = p^\mu$$

car $h(X)$ est irréductible sur k, c'est donc $M_{\alpha^{p^\mu}}$. Mais comme h est séparable, on a :

$$[k(\alpha^{p^\mu}) : k]_s = [k(\alpha^{p^\mu}) : k].$$

De plus, le nombre de racines distinctes de $M_\alpha(X)$ est le même que celui de $h(X)$. Donc :

$$[k(\alpha) : k]_s = [k(\alpha^{p^\mu}) : k]_s$$

et

$$[k(\alpha) : k] = [k(\alpha) : k(\alpha^{p^\mu})][k(\alpha^{p^\mu}) : k] = p^\mu [k(\alpha) : k]_s. \qquad \square$$

XIII.4. Éléments primitifs

***Définition* XIII.4.1.** Soient K/k une extension et $\alpha \in K$. On dit que α est un élément **primitif** de l'extension K/k si $K = k(\alpha)$.

***Théorème* XIII.4.1.** *Soit K/k une extension finie. Il existe un élément primitif pour l'extension K/k si et seulement s'il n'y a qu'un nombre fini de corps intermédiaires E, $k \subset E \subset K$.*

Démonstration. Si $|k| < +\infty$, alors $[K : k] < +\infty$ implique $|K| < +\infty$. Donc $K^\star$ est cyclique, engendré par un élément α (TR.IX.A). Cet élément engendre K sur k.

Traitons maintenant le cas $|k| = +\infty$.

Supposons qu'il n'y ait qu'un nombre fini de corps intermédiaires $k \subset E \subset K$. Soient $x, y \in K$. Pour tout $c \in k$, on considère $k(x+cy)$. Puisque $|k| = +\infty$, le nombre de corps $k(x+cy)$ étant fini, il existe $c_1 \neq c_2 \in k$ tels que $k(x+c_1y) = k(x+c_2y) = E_0$. Les éléments $x+c_1y$ et $x+c_2y$ sont dans le même corps E_0, donc aussi $(c_1-c_2)y$. Il en est donc de même pour y et donc aussi x. D'où

$$k(x,y) = k(\alpha) \quad \text{avec} \quad \alpha = x + c_1 y.$$

Si $K = k(\alpha_1, \ldots, \alpha_n)$, alors, par hypothèse de récurrence $k(\alpha_2, \ldots, \alpha_n) = k(y)$, d'où $K = k(\alpha_1, y)$, puis $K = k(\alpha)$ en vertu du résultat au rang 2.

Réciproquement, supposons $K = k(\alpha)$: alors α est algébrique (car $[K:k] < +\infty$ implique K/k algébrique) et soit $M_\alpha(X)$ son polynôme minimal sur k. Soit E un corps intermédiaire, $k \subset E \subset K$, et notons $f_E(X)$ le polynôme minimal de α sur E. Comme $M_\alpha(\alpha) = 0$, considéré comme polynôme à coefficients dans E, $f_E(X)$ divise $M_\alpha(X)$. Puisque $E[X]$ est principal, un polynôme n'a qu'un nombre fini de diviseurs. Donc, l'application φ définie par $\varphi(E) = f_E(X)$ est à valeurs dans un ensemble fini. Montrons que cette application est injective. On considère E_0 le sous-corps de E engendré sur k par les coefficients de $f_E(X)$. On peut donc considérer $f_E(X)$ dans $E_0[X]$ et $f_E(X)$ est irréductible dans $E_0[X]$, puisqu'il est irréductible dans $E[X]$ ($E_0[X] \subset E[X]$). Par conséquent, le degré de α sur E_0 est le même que le degré de α sur E. D'où $E_0 = E$. Ceci montre que le corps intermédiaire E est déterminé, de manière unique, par $f_E(X)$, donc φ est injective. L'ensemble des corps intermédiaires E, $k \subset E \subset K$, est donc fini. □

Théorème XIII.4.2. *Toute extension finie séparable admet un élément primitif.*

Démonstration. Si $|k| < +\infty$, le résultat est vrai d'après le théorème précédent. Supposons que $|k| = +\infty$: on a $K = k(\alpha_1, \ldots, \alpha_q)$. On peut, modulo une récurrence, supposer $K = k(\alpha, \beta)$, où α et β sont séparables sur k. Soit $\overline{k}$ une clôture algébrique de k et $\sigma_1, \ldots, \sigma_n$ les k-plongements distincts de $k(\alpha,\beta)$ dans $\overline{k}$. On forme le polynôme

$$P(X) = \prod_{1 \leqslant i < j \leqslant n} (\sigma_i - \sigma_j)(\alpha + \beta X).$$

Ce polynôme est non nul : si $\sigma_i(\alpha) = \sigma_j(\alpha)$ et $\sigma_i(\beta) = \sigma_j(\beta)$, on a $\sigma_i = \sigma_j$, ce qui est impossible car, $\forall i \neq j$, $\sigma_i \neq \sigma_j$. Puisque $|k| = +\infty$, il existe $c \in k$ tel que $P(c) \neq 0$. D'où $i \neq j$ implique $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$. Par conséquent, le degré séparable, donc le degré, de l'extension $k(\alpha + c\beta)/k$ est au moins n. Mais

$$n = [k(\alpha,\beta) : k]_s = [k(\alpha,\beta) : k].$$

D'où $[k(\alpha,\beta):k] \leqslant [k(\alpha+c\beta):k]$ et, puisque $k(\alpha+c\beta) \subset k(\alpha,\beta)$, on en déduit que $k(\alpha,\beta) = k(\alpha+c\beta)$. □

Exercice XIII.4. Soient k un corps de caractéristique nulle et K/k une extension. Montrer que $[K:k] \leqslant n$ si et seulement si, pour tout $x \in K$, on a $[k(x):k] \leqslant n$. (Indication : pour la réciproque, on pourra prendre une famille finie $(x_i)_{i\in I}$ d'éléments de K tels que $[k(x_i)_{i\in I}:k]$ soit maximal – après en avoir justifié l'existence – et montrer que $K = k(x_i)_{i\in I}$.)

XIII.5. Norme et trace

Rappelons quelques définitions d'algèbre linéaire. Soient A un anneau commutatif, E un A-module libre de rang fini n (*i.e.* $E \simeq A^n$, isomorphisme linéaire), u un endomorphisme de E, $(e_i)_{i=1,\dots,n}$ une base de E et (a_{ij}) la matrice de u dans cette base. Les expressions

$$\sum_{i=1}^{n} a_{ii} \quad \text{et} \quad det(a_{ij})$$

sont indépendantes de la base choisie. On définit alors la trace et le déterminant de u par

$$Tr(u) = \sum_{i=1}^{n} a_{ii} \quad \text{et} \quad det(u) = det(a_{ij}).$$

On sait que la trace et le déterminant vérifient $Tr(u+u') = Tr(u) + Tr(u')$ et $det(uu') = det(u)det(u')$. De plus, on a

$$det(XId_E - u) = X^n - Tr(u)X^{n-1} + \dots + (-1)^n det(u).$$

On généralise ces définitions de la manière suivante. Soient B un anneau et A un sous-anneau de B tels que B soit un A-module libre de rang fini n (c'est le cas d'une extension de corps E/K avec $[E:K] = n$). Pour tout $x \in B$, on note m_x l'endomorphisme de B défini par $m_x(y) = xy$.

Définition XIII.5.1. Pour tout élément $x \in B$, on appelle **trace, norme, polynôme caractéristique** de x, relativement à l'extension B/A, les éléments respectifs

$$Tr_{B/A}(x) = Tr(m_x), \quad N_{B/A}(x) = det(m_x), \quad P_{x,B/A}(X) = det(XId_B - m_x).$$

Ce sont des éléments de A ou de $A[X]$.

***Remarque* XIII.5.1.** Si x, x' sont des éléments de B et si a est un élément de A, on a

$$m_x + m_{x'} = m_{x+x'},\ m_x.m_{x'} = m_{xx'},\ m_{ax} = am_x$$

et la matrice de m_a est diagonale dans n'importe quelle base. On en déduit que la trace et la norme vérifient les relations suivantes :

$$Tr_{B/A}(x+x') = Tr_{B/A}(x)+Tr_{B/A}(x'),\ Tr_{B/A}(ax) = aTr_{B/A}(x),\ Tr_{B/A}(a) = na$$

$$N_{B/A}(xx') = N_{B/A}(x)N_{B/A}(x'),\ N_{B/A}(ax) = a^n N_{B/A}(x),\ N_{B/A}(a) = a^n.$$

Si L/K est une extension de corps, finie, séparable, nous allons donner une explicitation précise de la norme et de la trace d'un élément de L.

***Théorème* XIII.5.1.** *Soient L/K une extension séparable, $[L : K] = n$, $x \in L$ et $r = [L : K(x)]$ (de sorte que $n = rs$ avec $s = [K(x) : K]$). On note $x_1, \ldots, x_n$ les racines du polynôme minimal sur K de x, $M_x(X)$, chacune répétée r fois. Alors :*

$$Tr_{L/K}(x) = x_1 + \ldots + x_n$$

$$N_{L/K}(x) = x_1 \ldots x_n$$

$$P_{x,L/K}(X) = (X - x_1)\ldots(X - x_n).$$

Démonstration. La démonstration comporte deux étapes.

– Supposons que x soit un élément primitif de L, *i.e.* $L = K(x)$. On sait que $L \simeq K[X]/(M_x(X))$ et que $(1, x, \ldots, x^{n-1})$ est une K-base du K-espace vectoriel L. Écrivons

$$M_x(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0.$$

Alors la matrice de m_x dans la base $(1, \ldots, x^{n-1})$ est :

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

donc $Tr_{L/K}(x) = -a_{n-1}$ et $N_{L/K}(x) = (-1)^n a_0$. Mais puisque x est un élément primitif, le polynôme minimal de x, $M_x(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, s'écrit $M_x(X) = (X-x_1)\ldots(X-x_n)$. Donc $-a_{n-1} = x_1+\ldots+x_n$ et $(-1)^n a_0 = x_1 \ldots x_n$. Par conséquent,

$$Tr_{L/K}(x) = x_1 + \ldots + x_n \quad \text{et} \quad N_{L/K}(x) = x_1 \ldots x_n.$$

– Cas général. Ce qu'on vient de faire s'applique à l'extension $K(x)/K$. Pour prouver le théorème, il suffit de montrer que $P_{x,L/K}(X) = (M_x(X))^r$. Soient $(y_1, \ldots, y_s)$ une base de $K(x)$ sur K et $(z_1, \ldots, z_r)$ une base de L sur $K(x)$. Alors, $(y_i z_j)$, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant r$, est une base de L sur K et $n = rs$. Soit $M = (a_{kh})$ la matrice de la multiplication par x dans $K(x)$, par rapport à la base (y_i). On a

$$xy_i = \sum_h a_{ih} y_h$$

d'où

$$x(y_i z_j) = \left(\sum_h a_{ih} y_h \right) z_j = \sum_h a_{ih} (y_h z_j).$$

Si on ordonne lexicographiquement la base $y_i z_j$, la matrice M' de la multiplication par x dans L, par rapport à cette base, se présente sous la forme d'une matrice carrée (r, r), diagonale par blocs :

$$M' = \begin{pmatrix} M & & \\ & \ddots & \\ & & M \end{pmatrix},$$

d'où $P_{x,L/K} = det(XId - M') = (det(XId - M))^r$. Mais $det(XId - M) = M_x(X)$ d'après l'étape 1. D'où le résultat. □

Exercice XIII.5. On suppose que E/K est une extension séparable de degré n, contenue dans une clôture algébrique $\overline{K}$ de K. On note $\sigma_1, \ldots, \sigma_n$ les n K-morphismes distincts de E dans $\overline{K}$.

a) Montrer que pour tout élément x de E, on a $Tr_{E/K}(x) = \sum_{i=1}^n \sigma_i(x)$ et $N_{E/K}(x) = \prod_{i=1}^n \sigma_i(x)$.

b) On suppose que $E = \mathbb{Q}(\sqrt{d})$, où d est sans facteur carré (*i.e.* E est une extension de degré 2 de $\mathbb{Q}$), en écrivant $x \in E$ sous la forme $x = a + b\sqrt{d}$, montrer que $Tr_{E/\mathbb{Q}}(x) = 2a$ et $N_{E\mathbb{Q}}(x) = a^2 - db^2$.

c) Montrer que, si E est normale, pour tout x de E, $Tr_{E/K}(x)$ et $N_{E/K}(x)$ sont des éléments de K.

d) Montrer qu'il existe x dans E tel que $Tr_{E/K}(x) \neq 0$. (Utiliser le théorème (X.3.1).)

Soit L un corps tel que $K \subset L \subset E$ et $[E : L] = m$.

e) Montrer que pour tout élément x de L, on a

$$Tr_{E/K}(x) = m Tr_{L/K}(x) \quad et \quad N_{E/K}(x) = (N_{L/K}(x))^m.$$

f) Montrer que

$$Tr_{E/K}(x) = Tr_{L/K}(Tr_{E/L}(x)) \quad et \quad N_{E/K}(x) = N_{L/K}(N_{E/L}(x)).$$

(Indication : remarquer que $Tr_{E/L}(x) \in L$.)

Remarque XIII.5.2. Les définitions de la norme et de la trace données dans la définition (XIII.5.1) s'appliquent bien entendu au cas des extensions finies non séparables de corps. Mais dans ce cas, l'explicitation de ces éléments est plus compliquée et doit prendre en compte le facteur d'inséparabilité du degré de l'extension (*cf.* TR.XIII.B).

THÈMES DE RÉFLEXION

♣ TR.XIII.A. Corps parfaits

1. *Soit K un corps. Montrer que les assertions suivantes sont équivalentes :*

(i) *Tout polynôme irréductible de $K[X]$ est séparable*

(ii) *Toute extension algébrique de K est séparable*

(iii) *Toute clôture algébrique de K est une extension séparable de K.*

Un corps K satisfaisant à l'une des conditions ci-dessus est dit ***parfait***.

2. *Montrer qu'un corps de caractéristique nulle est parfait.*

3. *Soit K un corps de caractéristique $p > 0$. Montrer que K est parfait si et seulement si $K = K^p$.* (Autrement dit, si le morphisme de Frobenius est un automorphisme.)

4. *Montrer qu'un corps fini ou algébriquement clos est parfait.*

5. *Montrer que toute extension algébrique d'un corps parfait est un corps parfait.*

♠ TR.XIII.B. Extensions inséparables et radicielles

Une extension algébrique E/K qui n'est pas séparable, *i.e.* dans laquelle il existe au moins un élément non séparable, est dite ***inséparable***. D'après l'exemple (XIII.3.1.a), cette notion n'a de sens qu'en caractéristique $p > 0$. En particulier, d'après la proposition (XIII.3.2), si α est un élément de E non séparable sur K, toutes les racines de son polynôme minimal sont d'ordre une puissance de la caractéristique de K.

1. *Soient E/K une extension algébrique et E_s l'ensemble des éléments de E qui sont séparables sur K. Montrer que E_s est une extension séparable de K.* (On montrera que E_s est la réunion des extensions séparables de K contenues dans E.)

Dans la situation précédente, on a $K \subset E_s \subset E$ et $E \setminus E_s$ est formé de tous les éléments de E qui ne sont pas séparables sur K. Lorsque $[E : K]$ est fini, on a $[E : K] = [E : E_s][E_s : K]$ et, comme $[E_s : K] = [E_s : K]_s$ puisque l'extension E_s/K est séparable, on a $[E : K] = [E : E_s][E_s : K]_s$. On appelle l'entier $[E : E_s]$ le ***facteur d'inséparabilité du degré*** de l'extension E/K.

Nous allons introduire et étudier un sous-corps de E, noté E_r, qui joue un grand rôle lorsque l'on est en caractéristique $p > 0$.

2. *Soient E/K une extension, α un élément de E algébrique sur K, $M_\alpha(X)$ le polynôme minimal de α sur K. Montrer que les assertions suivantes sont équivalentes :*

(i) *L'élément α n'est pas séparable sur K*

(ii) $M'_\alpha(X) = 0$

(iii) *La caractéristique de K est égale à $p > 0$ et $M_\alpha(X) \in K[X^p]$.*

Soient E/K une extension et α un élément de E. On dit que l'élément α est ***radiciel*** sur K si l'une des conditions suivantes est satisfaite :

(a) K est de caractéristique nulle et α appartient à K.

(b) K est de caractéristique $p > 0$ et il existe $n \in \mathbb{N}$ tel que α^{p^n} appartient à K. Si on note e le plus petit entier n tel que $\alpha^{p^n} \in K$, le polynôme minimal de α est $X^{p^e} - \alpha^{p^e}$.

L'extension E/K est ***radicielle*** si tout élément de E est radiciel sur K. On remarquera que si la caractéristique de K est nulle, l'extension E/K est radicielle si et seulement si $E = K$. La notion d'extension radicielle n'a donc d'intérêt que dans le cas de la caractéristique positive. Par conséquent, dans toute la suite, nous supposerons que K est un corps de caractéristique $p > 0$, tous les résultats étant triviaux si la caractéristique est nulle.

3. *Soit K un corps de caractéristique $p > 0$. Montrer que si E/K est une extension finie radicielle, $[E : K]$ est une puissance de p.*

4. *Montrer que si l'extension E/K est radicielle, alors $Gal(E/K) = \{1\}$.*

5. *Soient K un corps de caractéristique $p > 0$ et $\overline{K}$ une clôture algébrique de K. Montrer que :*

(i) *Pour tout entier $n > 0$, l'ensemble $\{a^{p^n} | a \in K\}$ est un sous-corps de $\overline{K}$, noté K^{p^n}*

(ii) *Pour tout entier $n > 0$, un élément $a \in K$ a une seule racine p^n-ième dans $\overline{K}$, qu'on notera $a^{p^{-n}}$*

(iii) *L'ensemble $\{a^{p^{-n}} | a \in K\}$ est un sous-corps de $\overline{K}$, noté $K^{p^{-n}}$.*

L'ensemble des éléments de $\overline{K}$ radiciels sur K est appelé la ***clôture radicielle*** de K.

6. *Montrer que si K est de caractéristique $p > 0$, la clôture radicielle de K est le corps $\bigcup_{n>0} K^{p^{-n}}$, qu'on note $K^{p^{-\infty}}$.*

7. *Montrer que $K^{p^{-\infty}}$ est le plus petit sous-corps parfait de $\overline{K}$ contenant K.*

On en déduit qu'***un corps est parfait si et seulement s'il est égal à sa clôture radicielle***.

8. *Montrer que si le corps K n'est pas parfait, l'extension $K^{p^{-\infty}}/K$ ne peut être de degré fini.*

9. *Montrer que la notion de clôture radicielle d'un corps K est indépendante, à isomorphisme près, de la clôture algébrique $\overline{K}$ choisie.*

Soit E/K une extension avec $E \subset \overline{K}$. On note E_r l'ensemble des éléments de E radiciels sur K.

10. *Montrer que l'extension E/E_s est radicielle et que l'extension E/E_r est séparable.*

♠ TR.XIII.C. Dérivations et extensions séparables

L'objectif de ce TR est de donner une caractérisation des extensions de type fini qui sont algébriques et séparables, au moyen des dérivations.

Soient K un anneau commutatif et E une K-algèbre associative. Une ***K-dérivation*** de E est un endomorphisme D du K-module E vérifiant $D(xy) = D(x)y + xD(y)$, pour tous éléments x et y de E.

Lorsque le contexte le permet, on omet la lettre K et on dit dérivation au lieu de K-dérivation. On remarquera que la notion de dérivation d'un anneau définie au chapitre VIII correspond à celle donnée ci-dessus en prenant $K = \mathbb{Z}$.

Les dérivations formelles des polynômes en une indéterminée ou les dérivations partielles de polynômes en plusieurs indéterminées sont des exemples de dérivations dans les algèbres de polynômes.

1. *Soit a un élément de E. Vérifier que l'application $x \mapsto ax - xa$ est une dérivation de E.* On appelle une telle dérivation ***dérivation intérieure***.

2. *Montrer que si E possède un élément unité 1_E, pour toute dérivation D de E on a $D(1_E) = 0$. En déduire que pour tout entier n et pour tout $k \in K$ on*

a $D(n1_E) = 0$ et $D(k1_E) = 0$. (Autrement dit, en identifiant k à $k1_E$, on a $D(k) = 0$, pour tout k de K.)

3. *Soit D une dérivation de E. Montrer que l'ensemble $\{x \in E | D(x) = 0\}$ est une sous-K-algèbre de E.*

4. *Montrer que l'ensemble $Der_K(E)$ de toutes les K-dérivations de E est un sous-K-module du K-module $End_K(E)$.*

5. *Déduire de ce qui précède que si D_1 et D_2 sont des dérivations qui coïncident sur une partie génératrice de la K-algèbre E, on a $D_1 = D_2$.*

6. *Soit $E = K[X_1, \ldots, X_n]$ l'algèbre des polynômes en n indéterminées. On note D_i, $1 \leqslant i \leqslant n$, la dérivation partielle par rapport à X_i. Montrer que les D_i, $1 \leqslant i \leqslant n$, forment une base du K-module $Der_K(E)$.*

7. *Soient A un anneau commutatif intègre et F son corps de fractions. Montrer que toute dérivation D de A se prolonge de manière unique en une dérivation $\overline{D}$ de F. Précisément, si a et $b \neq 0$ sont des éléments quelconques de A, on a $\overline{D}(\frac{a}{b}) = \frac{D(a)b - aD(b)}{b^2}$.*

8. *Soient K un corps commutatif et D_i, $1 \leqslant i \leqslant n$, les dérivations partielles de $K[X_1, \ldots, X_n]$ par rapport aux X_i. Montrer que les $\overline{D_i}$, $1 \leqslant i \leqslant n$, forment une base du K-espace vectoriel $Der_K(K(X_1, \ldots, X_n))$.*

On généralise la notion de dérivation étudiée ci-dessus de la façon suivante. On suppose que E est une sous-K-algèbre d'une K-algèbre F : on appelle ***dérivation de E dans F*** toute application K-linéaire D de E dans F vérifiant $D(xy) = D(x)y + xD(y)$, pour tous éléments x et y de E. Les propriétés établies ci-dessus sont encore vraies dans ce cadre.

Nous allons désormais nous placer dans la situation suivante : F/E est une extension de corps et nous étudions les $\mathbb{Z}$-dérivations de E dans F.

9. *Soit D une dérivation de E dans F. Montrer que l'ensemble $K = \{x \in E | D(x) = 0\}$ est un sous-corps de E. En déduire que les dérivations de E dans F sont des K-dérivations.*

10. *En déduire que toute dérivation d'un corps premier P dans tout sur-corps de P est nulle.*

Pour donner la caractérisation annoncée au début de ce TR, nous allons donner un critère de prolongement des dérivations aux extensions de type fini.

Soient $E \subset F$ des corps et D une dérivation de E dans F. On considère $L = E(x_1, \ldots, x_n)$ une extension de type fini de E contenue dans F et $\mathfrak{a}$ l'idéal des relations algébriques entre les x_i, $1 \leqslant i \leqslant n$, à coefficients dans E. On se donne une famille u_i, $1 \leqslant i \leqslant n$, d'éléments de F.

11. *Montrer que pour qu'il existe une dérivation $\overline{D}$ de L dans F prolongeant D et telle que $\overline{D}(x_i) = u_i$, $1 \leqslant i \leqslant n$, il faut et il suffit que pour tout polynôme $f \in \mathfrak{a}$, on ait*

$$f^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} u_i = 0,$$

où f^D est défini par : si $f = \sum_{(n_i)} \alpha_{n_1 n_2 \ldots n_p} X^{n_1} X^{n_2} \ldots X^{n_p}$, alors $f^D = \sum_{(n_i)} D(\alpha_{n_1 n_2 \ldots n_p}) X^{n_1} X^{n_2} \ldots X^{n_p}$. (On remarquera que $f \mapsto f^D$ est une dérivation qui prolonge la dérivation D. Pour démontrer que la condition est suffisante, on montrera que la relation ci-dessus permet de définir $\overline{D}$ sur l'anneau $E[x_1, \ldots, x_n]$ et on appliquera le résultat de la question 7.)

12. *En déduire que si, dans la situation ci-dessus, L est une extension transcendante pure de E, de base pure (x_i), $1 \leqslant i \leqslant n$, pour toute dérivation D de E dans F, $\overline{D}$ existe et est unique.*

13. *Soit L une extension algébrique séparable de E contenue dans F. Montrer que toute dérivation D de E dans F se prolonge de manière unique en une dérivation $\overline{D}$ de L dans F.* (Pour démontrer l'existence de $\overline{D}$, on montrera d'abord qu'on peut supposer que L est de type fini, $L = E(x_1, \ldots, x_n)$. On fera ensuite un raisonnement par récurrence sur n, en considérant le polynôme minimal de x_n sur $E(x_1, \ldots, x_{n-1})$.)

14. *En déduire que si la dérivation D de E est telle que $D(E) \subset E$, alors $\overline{D}(L) \subset L$.*

15. *Montrer que toute K-dérivation d'une extension E/K est nulle dans toute extension algébrique séparable de K contenue dans E.*

16. *Montrer que si $L \subset F$ est une extension radicielle finie de K, de degré strictement supérieur à 1, il existe une K-dérivation non nulle de E dans F.*

On en déduit la caractérisation des extensions algébriques séparables annoncée au début de ce TR :

17. *Montrer que pour qu'une extension E/K de type fini, $E \subset F$, soit algébrique et séparable, il faut et il suffit que la seule K-dérivation de E dans F soit la dérivation nulle.*

This page intentionally left blank

Troisième partie

THÉORIE DE GALOIS ET APPLICATIONS

This page intentionally left blank

XIV

EXTENSIONS GALOISIENNES THÉORIE DE GALOIS DES EXTENSIONS FINIES

La théorie de Galois permet de répondre, dans le cas des extensions **galoisiennes** finies, à la question posée en (X.4.1). Le résultat principal de cette théorie est que si E/K est une extension galoisienne finie, le groupe de Galois $Gal(E/K)$ et ses sous-groupes permettent de caractériser entièrement toutes les extensions intermédiaires $K \subset L \subset E$.

XIV.1. Extensions galoisiennes

Proposition XIV.1.1. *Soient E/K une extension séparable finie de degré n et N la clôture normale de cette extension. Alors, il y a exactement n K-morphismes distincts de E dans N.*

Démonstration. On fait une démonstration par récurrence sur le degré de l'extension E/K. Si $[E : K] = 1$ c'est évident. Supposons le résultat vrai pour les extensions de K de degré $p < n$. Soit $[E : K] = n$ et soient $\alpha \in E \setminus K$ et $M_\alpha(X)$ son polynôme minimal sur K, qu'on suppose de degré r $(r \leqslant n)$. Le polynôme $M_\alpha(X)$ est séparable, il a donc exactement r racines distinctes $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ dans N. Puisque N est une extension normale, il existe r K-automorphismes distincts u_i de N tels que $u_i(\alpha) = \alpha_i$. D'autre part, en considérant l'extension $E/K(\alpha)$, qui est de degré $s = n/r < n$, par hypothèse de récurrence, il existe s $K(\alpha)$-morphismes distincts v_i de E dans N. Les applications $w_{ij} = u_i v_j$ sont $rs = n$ K-morphismes distincts de E dans N. Montrons qu'il n'y en a pas d'autres.

Soit $s : E \longrightarrow N$ un K-morphisme. Alors $s(\alpha)$ est une racine de $M_\alpha(X)$, *i.e.* $s(\alpha) = \alpha_i$ pour un certain i. Par conséquent, $u_i^{-1} \circ s$ est un $K(\alpha)$-morphisme de E dans N, donc par hypothèse de récurrence, c'est l'un des v_j. D'où $s = u_i v_j$. □

***Remarque* XIV.1.1.** Soient E/K une extension algébrique et $\overline{K}$ une clôture algébrique de K contenant E. Tout élément $s \in Gal(E/K)$ induit un K-morphisme de E dans $\overline{K}$. Donc si l'extension est finie, $|Gal(E/K)| \leqslant [E : K]_s$. Inversement, si l'extension E/K est normale, tout K-morphisme $E \longrightarrow \overline{K}$ est un K-automorphisme de E, donc un élément de $Gal(E/K)$. Par conséquent, si l'extension E/K est finie et normale, $|Gal(E/K)| = [E : K]_s$.

***Corollaire* XIV.1.1.** *Soit E/K une extension algébrique finie, normale, séparable, alors $[E : K] = |Gal(E/K)|$.* □

***Définition* XIV.1.1.** Une extension E/K est dite **galoisienne** si elle est algébrique, normale et séparable.

***Remarque* XIV.1.2.** Une extension algébrique E/K est galoisienne si et seulement si pour tout $\alpha \in E$, le polynôme minimal $M_\alpha(X)$ de α sur K a toutes ses racines simples et contenues dans E.

On déduit du théorème (X.3.2) et de la proposition (X.4.1) que si E/K est une extension finie galoisienne, alors $Inv(Gal(E/K)) = K$. On a, plus généralement, le résultat suivant :

***Théorème* XIV.1.1.** *Soit E/K une extension algébrique. Les assertions suivantes sont équivalentes :*

(i) $Inv(Gal(E/K)) = K$

(ii) *L'extension E/K est galoisienne.*

Démonstration. Montrons que (i) implique (ii). Soient $\alpha \in E$ et $M_\alpha(X)$ son polynôme minimal sur K. On note $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ ses racines distinctes et contenues dans E. Tout élément $s \in Gal(E/K)$ permute les α_i, il laisse donc invariant le polynôme $f(X) = \prod_{i=1}^{n}(X - \alpha_i) \in E[X]$. D'après l'hypothèse, $f(X)$ appartient à $K[X]$. Or $f(\alpha) = 0$, donc $f(X)$ est un multiple de $M_\alpha(X)$. Mais, par construction, $f(X)$ divise $M_\alpha(X)$, d'où $f(X) = M_\alpha(X)$. Ainsi $M_\alpha(X)$ a toutes ses racines simples et contenues dans E. L'extension E/K est galoisienne.

Montrons que (ii) implique (i). Soient $\alpha \in E \setminus K$ et $M_\alpha(X)$ le polynôme minimal de α sur K. Puisque $d^\circ M_\alpha > 1$, d'après l'hypothèse, il existe $\beta \in E$, $\beta \neq \alpha$, tel que $M_\alpha(\beta) = 0$. Par conséquent, il existe un K-morphisme de E dans $\overline{K}$ appliquant α sur β. C'est, par normalité de E/K, un K-automorphisme s de E, *i.e.* $s \in Gal(E/K)$ tel que $s(\alpha) = \beta \neq \alpha$. Ceci montre que tout $\alpha \in E \setminus K$ n'appartient pas à $Inv(Gal(E/K))$. Comme $K \subset Inv(Gal(E/K))$, on en déduit que $Inv(Gal(E/K)) = K$. □

On peut maintenant donner une version plus précise du théorème (X.3.2).

Théorème XIV.1.2. *Soient K un corps, G un groupe fini d'automorphismes de K et K_0 le corps des invariants de G. L'extension K/K_0 est galoisienne, $[K : K_0] = |G|$ et $G = Gal(K/K_0)$.*

Démonstration. On a vu que $[K : K_0] = |G| < +\infty$, l'extension K/K_0 est donc algébrique. Puisque $K_0 = Inv(G)$, d'après le théorème (XIV.1.1), il suffit de prouver que $G = Gal(K/K_0)$. Or, G est contenu dans $Gal(K/K_0)$ et, de plus, on sait que $|Gal(K/K_0)| \leqslant [K : K_0]_s \leqslant [K : K_0]$. On a donc : $G \subset Gal(K/K_0)$ et $|Gal(K/K_0)| \leqslant |G|$, d'où $G = Gal(K/K_0)$. □

Théorème XIV.1.3. *Soient F/K et E/F des extensions. Si l'extension E/K est galoisienne, alors E/F est galoisienne et $Gal(E/F)$ est un sous-groupe de $Gal(E/K)$.*

Démonstration. La deuxième assertion est évidente et la première est une conséquence de la proposition (XIII.2.2) et du théorème (XIII.3.2). □

Attention. *Pour les mêmes raisons que dans la proposition (XIII.2.2),*

$$(E/K \text{ galoisienne}) \not\Longrightarrow (F/K \text{ galoisienne}).$$

Théorème XIV.1.4. *Soient E/K une extension galoisienne, L et L' deux corps intermédiaires. Les assertions suivantes sont équivalentes :*

(i) *Les corps L et L' sont conjugués*

(ii) *Les groupes $Gal(E/L)$ et $Gal(E/L')$ sont des sous-groupes conjugués de $Gal(E/K)$.*

Démonstration. Le fait que (i) implique (ii) est une conséquence de la proposition (XIII.2.5) et de la proposition (X.4.1). Montrons que (ii) implique (i). D'après la proposition (X.4.1), on sait que les corps $Inv(Gal(E/L)$ et $Inv(Gal(E/L'))$ sont conjugués. Mais d'après le théorème (XIV.1.3), les extensions E/L et E/L' sont galoisiennes et donc, d'après le théorème (XIV.1.1), on a : $Inv(Gal(E/L)) = L$ et $Inv(Gal(E/L')) = L'$. □

XIV.2. Clôture galoisienne d'une extension séparable

Proposition - Définition XIV.2.1. *Soit K/k une extension algébrique séparable. La clôture normale de K (dans $\overline{k}$) est une extension galoisienne, appelée clôture galoisienne de l'extension K/k.*

Démonstration. Il suffit de montrer que la clôture normale N de K est séparable sur k. D'après la proposition (XIII.2.4), tout élément de N est racine du polynôme minimal d'un élément de K. Il est donc séparable sur k. □

Proposition XIV.2.2. *Si l'extension K/k est séparable finie, sa clôture galoisienne est une extension finie de k.*

Démonstration. C'est une conséquence immédiate du corollaire (XIII.2.1). □

Remarque XIV.2.1. On pourra donc, pour étudier les sous-extensions d'une extension finie séparable, la plonger dans sa clôture galoisienne et appliquer alors la théorie de Galois des extensions galoisiennes finies développée ci-dessous.

XIV.3. Théorèmes fondamentaux de la théorie de Galois

Soient E/K une extension, $G = Gal(E/K)$ son groupe de Galois, $\mathcal{G}(G)$ l'ensemble des sous-groupes de G, $\mathcal{K}(E/K)$ l'ensemble des corps intermédiaires L, $K \subset L \subset E$. Les ensembles $\mathcal{G}(G)$ et $\mathcal{K}(E/K)$ sont ordonnés par inclusion. On a établi en (X.4) l'existence d'applications décroissantes

$$\Phi : \mathcal{K}(E/K) \longrightarrow \mathcal{G}(G), \quad L \longmapsto Gal(E/L)$$

$$\Psi : \mathcal{G}(G) \longrightarrow \mathcal{K}(E/K), \quad H \longmapsto Inv(H) = E^H.$$

Le résultat ci-dessous répond à la question (X.4.1).

Théorème XIV.3.1. *Soit E/K une extension finie galoisienne. L'application Φ est une application bijective, dont l'application bijective réciproque est Ψ.*

Démonstration. Montrons que $\Psi \circ \Phi$ est égale à l'identité. Soit L un corps intermédiaire : puisque E/K est galoisienne, E/L l'est aussi et, par conséquent, d'après le théorème (XIV.1.1), $E^{Gal(E/L)} = L$.

Montrons que $\Phi \circ \Psi$ est égale à l'identité. Soit H un sous-groupe de $Gal(E/K)$ et posons $L = Inv(H)$. Puisque $[E : K] < +\infty$, d'après le corollaire (XIV.1.1), H est fini, donc, d'après le théorème (XIV.2.2), $H = Gal(E/L)$. □

Attention. *L'hypothèse* $[E : K] < +\infty$ *est essentielle. L'énoncé du théorème XIV.3.1 n'est plus valable si* E/K *est une extension galoisienne infinie,* cf. *TR.XIV. Cependant, on remarquera que, dès que* E/K *est galoisienne, l'application* Φ *est injective (et l'application* Ψ *surjective).*

Exercice XIV.1. On reprend les notations de l'exercice XII.1. On note $G = Gal(K(a,b,c)/K)$.

a) On suppose que le polynôme $P(X)$ est réductible sur K. Quelles sont les structures possibles de groupes sur G ? Préciser ces structures en fonction de d.

b) On suppose que le polynôme $P(X)$ est irréductible sur K. Montrer que si $d \in K$, alors $G \simeq A_3$, et que si $d \notin K$, alors $G \simeq S_3$. Préciser les extensions intermédiaires entre K et $K(a,b,c)$.

Théorème XIV.3.2. *Soient* E/K *une extension finie galoisienne et* L *un corps intermédiaire. Les assertions suivantes sont équivalentes :*

(i) *L'extension* L/K *est galoisienne*

(ii) $Gal(E/L)$ *est un sous-groupe normal de* $Gal(E/K)$.

De plus, si ces conditions sont vérifiées, l'application, qui à un élément de $Gal(E/K)$ *fait correspondre sa restriction à* L*, induit un isomorphisme de groupes*

$$Gal(E/K)/Gal(E/L) \simeq Gal(L/K).$$

Démonstration. D'après la proposition (XIII.2.6), l'extension L/K est normale si et seulement si elle est égale à toutes ses conjuguées, donc, d'après le théorème (XIV.1.4), si et seulement si $Gal(E/L)$ est un sous-groupe normal de $Gal(E/K)$.

Supposons ces conditions vérifiées. Alors, si $s \in Gal(E/K)$, on a $s(L) = L$, d'où la restriction de s à L appartient à $Gal(L/K)$. Il est clair que

$$\varphi : Gal(E/K) \longrightarrow Gal(L/K),$$

où $\varphi(s)$ est la restriction de s à L, est un morphisme de groupes. Montrons que φ est surjectif ; soit $t \in Gal(L/K)$: le K-morphisme

$$L \xrightarrow{t} L \longrightarrow \overline{K}$$

se prolonge en $s : E \longrightarrow \overline{K}$. Puisque E/K est normale, s est un K-automorphisme de E, *i.e.* $s \in Gal(E/K)$. On a donc $t = \varphi(s)$. D'autre part, $\varphi(s) = id_L$ est équivalent à $s \in Gal(E/L)$, *i.e.* $Ker(\varphi)$ est égal à $Gal(E/L)$. □

Exercice XIV.2. Soit K un corps de caractéristique différente de 2.

a) Montrer que si E/K est une extension galoisienne de degré 4 dont le groupe de Galois est $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, alors $E = K(\alpha, \beta)$ avec $\alpha^2, \beta^2 \in K$.

b) On suppose que $\alpha^2 = a$ et $\beta^2 = b$ et que les éléments a, b, ab ne sont pas des carrés dans K. Montrer que $K(\alpha, \beta)/K$ est une extension galoisienne de degré 4 dont le groupe de Galois est $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

La théorie de Galois permet de préciser le lien entre les énoncés des théorèmes (XIII.4.1) et (XIII.4.2).

Proposition XIV.3.1. *Si E/K est une extension séparable finie, il n'existe qu'un nombre fini de corps intermédiaires entre K et E.*

Démonstration. Soit N la clôture normale de E sur K. Alors N/K est une extension galoisienne finie. Les corps intermédiaires entre K et E correspondent à une famille de sous-groupes de $Gal(N/K)$. Ce groupe étant fini, il n'a qu'un nombre fini de sous-groupes. □

Exercice XIV.3. Soient K un corps, N/K une extension galoisienne finie, L' et L'' des corps intermédiaires. On pose $G = Gal(N/K)$, $G' = Gal(N/L')$, $G'' = Gal(N/L'')$.

a) Montrer que si L'/K et L''/K sont des extensions normales telles que $L' \cap L'' = K$ et $L' \cup L''$ engendre N, alors le groupe G est isomorphe au produit direct $G' \times G''$. (Pour $G \simeq G' \times G''$, *cf.* proposition I.3.4 et remarquer que G' et G'' sont des sous-groupes normaux de G.)

b) Montrer que dans ce cas, on a $G \simeq Gal(L'/K) \times Gal(L''/K)$.

c) On suppose que le groupe G est isomorphe au produit direct de deux sous-groupes G_1 et G_2. On pose $L_1 = Inv(G_1)$ et $L_2 = Inv(G_2)$. Montrer que $L_1 \cap L_2 = K$ et que $L_1 \cup L_2$ engendre N.

XIV.4. Étude d'un exemple

Soit $K \subseteq \mathbb{C}$ le corps de décomposition sur $\mathbb{Q}$ du polynôme $f(X) = X^4 - 2$. Dans $\mathbb{C}$, on a

$$f(X) = (X - \alpha)(X + \alpha)(X - i\alpha)(X + i\alpha),$$

avec $\alpha = 2^{1/4} \in \mathbb{R}^+$.

D'où $K = \mathbb{Q}(i, \alpha)$. Par construction, l'extension $K/\mathbb{Q}$ est normale et, puisque $\mathbb{Q}$ est de caractéristique nulle, séparable. L'extension $K/\mathbb{Q}$ est donc galoisienne. Déterminons son degré. On a

$$[\mathbb{Q}(i, \alpha) : \mathbb{Q}] = [\mathbb{Q}(i, \alpha) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Par application du critère d'Eisenstein, le polynôme $X^4 - 2$ est irréductible sur $\mathbb{Q}$; on en déduit que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. D'autre part, le polynôme minimal de i sur $\mathbb{Q}(\alpha)$ est $X^2 + 1$, d'où $[\mathbb{Q}(i, \alpha) : \mathbb{Q}(\alpha)] = 2$. On a donc $[\mathbb{Q}(i, \alpha) : \mathbb{Q}] = 8$. L'extension $K/\mathbb{Q}$ est galoisienne de degré 8, son groupe de Galois G est donc un groupe d'ordre 8.

Détermination de G : il existe un élément σ de G définie par $\sigma(i) = i$ et $\sigma(\alpha) = i\alpha$ et un élément τ défini par $\tau(i) = -i$ et $\tau(\alpha) = \alpha$. On vérifie facilement que σ est d'ordre 4 et τ d'ordre 2 et que $\tau\sigma = \sigma^3\tau$. Le groupe diédral $D_4 = \langle \sigma, \tau | \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle$ (*cf.* TR.IV.A) est donc contenu dans G. Mais mbox$|D_4| = 8 = |G|$, d'où $G = D_4$.

Détermination des sous-groupes de G : Les sous-groupes de G sont d'ordre 8, 4, 2, 1. Explicitons-les :

Ordre 8 : G.

Ordre 4 :

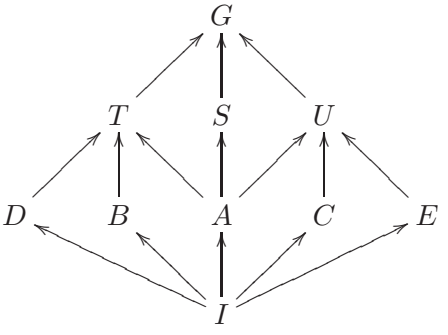
$$S = \langle \sigma \rangle \simeq \mathbb{Z}/4\mathbb{Z}$$
$$T = \{1, \sigma^2, \tau, \sigma^2\tau\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$U = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Ordre 2 :

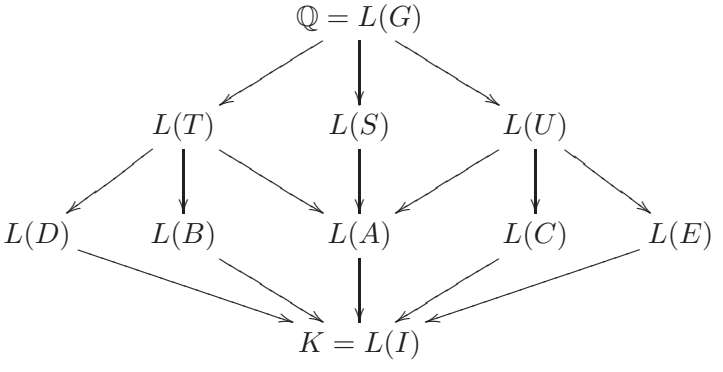
$$A = \{1, \sigma^2\}$$
$$B = \{1, \tau\}$$
$$C = \{1, \sigma\tau\}$$
$$D = \{1, \sigma^2\tau\}$$
$$E = \{1, \sigma^3\tau\}.$$

Ordre 1 : $I = \{1\}$.

On peut représenter les inclusions entre ces groupes par le diagramme ci-dessous, où chaque flèche (y compris composée) représente une inclusion.



Détermination des sous-extensions de $K/\mathbb{Q}$: d'après la théorie de Galois, on sait que chaque corps intermédiaire L, $\mathbb{Q} \subset L \subset K$, est le corps des invariants d'un des groupes ci-dessus. De plus, chaque inclusion entre sous-groupes induit une inclusion (dans l'autre sens) entre corps intermédiaires. Si, pour un sous-groupe H, on note $L(H)$ le corps de ses invariants, on peut, avec la même convention que ci-dessus, représenter les corps intermédiaires par le diagramme suivant :



Puisque $4 = |S| = |T| = |U|$, on a $4 = [K : L(S)] = [K : L(T)] = [K : L(U)]$, d'où $[L(S) : \mathbb{Q}] = [L(T) : \mathbb{Q}] = [L(U) : \mathbb{Q}] = 2$. Il est facile de vérifier que $L(S) = \mathbb{Q}(i)$, $L(T) = \mathbb{Q}(\sqrt{2})$, $L(U) = \mathbb{Q}(i\sqrt{2})$. Pour les mêmes raisons que ci-dessus, pour $\Lambda = A, B, C, D, E$, on a $[L(\Lambda) : \mathbb{Q}] = 4$. Pour calculer explicitement les corps $L(\Lambda)$, on écrit un élément générique de $\mathbb{Q}(i, \alpha)$,

$$x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3,$$

$a_i \in \mathbb{Q}$, $i = 0, ..., 7$, et on cherche à quelles conditions sur les a_i on a $\lambda(x) = x$ pour $\lambda \in \Lambda$.

À titre d'exemple, calculons $L(C)$. On a

$$\sigma\tau(x) = a_0 + a_5\alpha - a_2\alpha^2 - a_7\alpha^3 - a_4 i + a_1 i\alpha + a_6 i\alpha^2 - a_3 i\alpha^3.$$

D'où $\sigma\tau(x) = x$ si et seulement si $a_0 = a_0$, $a_1 = a_5$, $a_2 = -a_2$, $a_3 = -a_7$, $a_4 = -a_4$, $a_6 = a_6$. Donc $\sigma\tau(x) = x$ si et seulement si,

$$\begin{aligned} x &= a_0 + a_1(1+i)\alpha + a_6 i\alpha^2 + a_3(1-i)\alpha^3 \\ &= a_0 + a_1(1+i)\alpha + \frac{a_6}{2}[(1+i)\alpha]^2 - \frac{a_3}{2}[(1+i)\alpha]^3 \end{aligned}$$

autrement dit, $L(C) = \mathbb{Q}((1+i)\alpha)$.

De la même manière, on trouve $L(A) = \mathbb{Q}(i, \sqrt{2})$, $L(B) = \mathbb{Q}(\alpha)$, $L(D) = \mathbb{Q}(i\alpha)$, $L(E) = \mathbb{Q}((1-i)\alpha)$.

Détermination des extensions $L/\mathbb{Q}$ qui sont galoisiennes : les sous-groupes normaux de D_4 sont D_4, S, T, U, A, I. Par conséquent, les extensions $L(\Lambda)/\mathbb{Q}$, pour $\Lambda = D_4, S, T, U, A, I$ sont galoisiennes, de groupes de Galois isomorphes à D_4/Λ.

Puisque chacune des extensions intervenant ici est finie séparable, elle admet un élément primitif. On vérifiera que l'élément $i + \alpha$ est primitif pour $K/\mathbb{Q}$ (indication : $\forall \sigma \neq \sigma' \in G$, $\sigma(i+\alpha) \neq \sigma'(i+\alpha)$.)

This page intentionally left blank

THÈMES DE RÉFLEXION

♠ TR.XIV. Théorie de Galois des extensions infinies

Les théorèmes fondamentaux de la théorie de Galois exposés dans ce chapitre qui établissent une correspondance biunivoque entre les sous-groupes du groupe de Galois et les extensions intermédiaires, ainsi que la correspondance entre sous-groupes normaux et sous-extensions galoisiennes, utilisent très fortement le fait que les extensions galoisiennes considérées sont finies. Si on considère une extension galoisienne E/K infinie, ces résultats ne sont plus vrais. En particulier, il peut exister des sous-groupes du groupe $Gal(E/K)$, distincts de $Gal(E/K)$, ayant pour corps d'invariants K.

Cependant, dans le cas où l'extension galoisienne E/K est infinie, on peut énoncer des théorèmes analogues aux théorèmes (XIV.3.1) et (XIV.3.2), à condition de munir le groupe de Galois $Gal(E/K)$ d'une topologie.

Nous allons tout d'abord étudier la notion de groupe topologique. Un groupe G, dont on notera la loi multiplicativement, est un ***groupe topologique*** s'il est muni d'une topologie compatible avec la structure de groupe de G, *i.e.* rendant continues les applications définies par le produit et le passage à l'inverse, $(x, y) \mapsto xy$ et $x \mapsto x^{-1}$, pour tous éléments x et y de G.

Il en résulte, en particulier, que pour tout élément $a \in G$ les applications de G dans G définies par $x \mapsto ax$, $x \mapsto xa$, ainsi que l'application $x \mapsto x^{-1}$, sont des homéomorphismes. Ceci montre que la topologie du groupe est entièrement déterminée par la donnée d'une base de voisinages de son élément neutre. Précisément, si $\mathcal{V}$ est une base de voisinages de l'élément neutre de G, pour tout élément $a \in G$, $\{aV | V \in \mathcal{V}\} = \{Va | V \in \mathcal{V}\}$ est une base de voisinages de a.

Soit G un groupe topologique dont on notera e l'élément neutre et soit $\mathcal{V}$ une base de voisinages de e.

1. *Montrer que $\mathcal{V}$ vérifie les propriétés suivantes :*

(i) *Pour tout $U \in \mathcal{V}$, il existe $V \in \mathcal{V}$ tel que $V.V \subseteq U$*

(ii) *Pour tout $U \in \mathcal{V}$, il existe $V \in \mathcal{V}$ tel que $V^{-1} \subseteq U$*

(iii) *Pour tout $U \in \mathcal{V}$ et tout $a \in G$, il existe $V \in \mathcal{V}$ tel que $V \subseteq aUa^{-1}$.*

2. *Réciproquement, soit $\mathcal{V}$ une famille de parties de G satisfaisant aux propriétés ci-dessus. Montrer qu'il existe une topologie et une seule sur G, compatible avec la structure de groupe de G, pour laquelle $\mathcal{V}$ soit une base de voisinages de l'élément neutre de G.*

3. *Montrer que si $\mathcal{V}$ est formée de sous-groupes de G les conditions (i) et (ii) sont automatiquement vérifiées et que si ces sous-groupes sont normaux, la condition (iii) est vérifiée.*

4. *Montrer que le groupe topologique G est séparé si et seulement si $\{e\}$ est fermé.*

Dans toute la suite, E/K est une extension galoisienne et $G = Gal(E/K)$ est son groupe de Galois.

Pour toute sous-extension L de E, galoisienne et de degré fini sur K, on pose $g(L) = Gal(E/L)$. Les $g(L)$, pour L parcourant les sous-extensions E, galoisiennes et de degré fini sur K, sont des sous-groupes de G, normaux d'après le théorème (XIV.3.2). On obtient ainsi une base de voisinages de l'élément neutre de G. Dans toute la suite, on supposera G muni de la topologie ainsi définie, qu'on appellera « topologie de groupe de Galois ». C'est la topologie discrète lorsque l'extension E/K est galoisienne finie.

5. *Soit H un sous-groupe de G dont le corps des invariants est égal à K. Montrer que pour toute sous-extension L de E, galoisienne de degré fini sur K, tout K-automorphisme de L est la restriction d'un automorphisme appartenant à H.*

6. *Montrer que le résultat de la question précédente peut aussi s'énoncer de la façon suivante : H est partout dense dans G.*

On peut considérer G comme partie de l'ensemble $\mathbb{N}^{\mathbb{N}}$ des applications de $\mathbb{N}$ dans $\mathbb{N}$.

7. *Montrer que la topologie de G est induite par la topologie produit des topologies discrètes sur les facteurs de $\mathbb{N}^{\mathbb{N}}$.*

8. *En déduire que le groupe topologique G est compact, totalement discontinu.* (Puisque $\mathbb{N}^{\mathbb{N}}$ est séparé et totalement discontinu, il en est de même pour le sous-espace G. On montrera que G est relativement compact dans $\mathbb{N}^{\mathbb{N}}$, puis qu'il est fermé.)

9. *Soit F une sous-extension de E, de degré fini sur K. Montrer que $Gal(E/F)$ est un sous-groupe ouvert et fermé de G.*

10. *Soit N une sous-extension quelconque de E. Montrer que $Gal(E/N)$ est un sous-groupe fermé de G. Montrer que la topologie de $Gal(E/N)$ induite par celle de G coïncide avec la topologie de groupe de Galois de $Gal(E/N)$.* (On considérera G et $Gal(E/N)$ comme sous-espaces de $\mathbb{N}^{\mathbb{N}}$.)

11. *Soient H un sous-groupe de G et N le corps des invariants de H. Montrer que $Gal(E/N)$ est l'adhérence de H dans G.* (Utiliser la question 6.)

Les résultats précédents se résument dans l'énoncé suivant :

Théorème. *Soient E/K une extension galoisienne, $G = Gal(E/K)$ son groupe de Galois (topologique), $\mathcal{G}$ l'ensemble des sous-groupes fermés de G, $\mathcal{K}$ l'ensemble des corps intermédiaires entre K et E. Pour tout $H \in \mathcal{G}$, on note $Inv(H)$ le corps des invariants de H. Les applications*

$$\Phi : \mathcal{K}(E/K) \longrightarrow \mathcal{G}(G), \quad L \longmapsto Gal(E/L)$$

$$\Psi : \mathcal{G}(G) \longrightarrow \mathcal{K}(E/K), \quad H \longmapsto Inv(H)$$

sont des applications bijectives, réciproques l'une de l'autre.

12. *Soit L une sous-extension de E. Montrer que l'extension L/K est galoisienne si et seulement si le groupe $Gal(E/L)$ est un sous groupe normal de G. Dans ce cas, montrer que le groupe $Gal(L/K)$ est isomorphe au groupe topologique $Gal(E/K)/Gal(E/L)$* (i.e. *la projection canonique est un isomorphisme de groupes et un homéomorphisme).* (Utiliser le fait que les groupes $Gal(E/K)$ et $Gal(L/K)$ sont compacts et montrer que l'application, qui à $\sigma \in Gal(E/K)$ fait correspondre sa restriction à L, est continue.) (On rappelle qu'un espace quotient est muni de la topologie la plus fine rendant la projection canonique continue.)

This page intentionally left blank

TRAVAUX PRATIQUES

TP.XIV. Autour de la correspondance de Galois

Le but de ce TP est de calculer les sous-corps d'une extension $\mathbb{Q}(a)/\mathbb{Q}$ définie comme corps de rupture d'un polynôme irréductible P. Lorsque ce dernier est normal, c'est-à-dire lorsque $\mathbb{Q}(a)$ est corps de décomposition de P et l'extension $\mathbb{Q}(a)/\mathbb{Q}$ galoisienne, il est facile de calculer le groupe de Galois $G = Gal(P) = Gal(\mathbb{Q}(a)/\mathbb{Q})$ comme groupe de permutations des racines qui sont des polynômes en a. On utilise alors la correspondance de Galois pour déterminer les sous-corps maximaux de $\mathbb{Q}(a)$: il suffit de calculer les invariants sous un élément de G en résolvant un système linéaire.

Par contre, lorsque P n'est pas normal, il est beaucoup plus difficile de calculer le groupe de Galois (voir TP.XVI) et l'extension $\mathbb{Q}(a)/\mathbb{Q}$ n'est plus galoisienne. On va déterminer les sous-corps sans calculer $Gal(P)$, la correspondance de Galois étant cependant toujours en filigrane, quitte à passer à la clôture galoisienne. On a besoin pour cela de savoir décrire une intersection $\mathbb{Q}(a) \cap \mathbb{Q}(b)$ de deux corps de nombres. En résolvant algorithmiquement ce problème, on parvient à décrire les sous-corps maximaux, donc tous les corps intermédiaires, quitte à réitérer le processus.

☞ Il est souhaitable que le lecteur soit familier de la manipulation des groupes de permutations sous MAPLE (charger la librairies `group` et consulter au besoin le TP.I) et des calculs dans les corps de nombres (commande `RooOf`). Les algorithmes des TP.XI et TP.XII seront réinvestis.

Le groupe de Galois comme groupe de permutations : cas des polynômes normaux

Soit $P \in \mathbb{Q}[x]$ un polynôme irréductible de degré n. On suppose que P est *normal*, c'est-à-dire que tout corps de rupture de P est corps de décomposition.

Si a désigne une racine de P (dans une extension), $\mathbb{Q}(a)/\mathbb{Q}$ est donc une extension normale et séparable, *i.e.* galoisienne, et le groupe de Galois de P est $Gal(P) = Gal(\mathbb{Q}(a)/\mathbb{Q})$, de cardinal $n = [\mathbb{Q}(a) : \mathbb{Q}]$.

Les autres racines sont données par $a_i = F_i(a)$, où les polynômes $F_i \in \mathbb{Q}[x]$ sont de degré inférieur strictement à n. Le groupe de Galois, $Gal(P)$, permute les racines de P : $P(\sigma(a_i)) = \sigma(P(a_i)) = 0$ si $\sigma \in Gal(P)$. Comme les racines de P sont distinctes et qu'un élément σ de $Gal(P)$ est déterminé par l'image de $a = a_1$, on peut voir $Gal(P)$ comme un sous-groupe de S_n (après numérotation des racines). On pose $G = \{\sigma_1, \ldots, \sigma_n\}$, où $\sigma_j(a) = a_j$. La permutation $\tilde{\sigma}_j$ de S_n correspondant à σ_j est déterminée par :

$$\sigma_j(a_i) = F_i(\sigma_j(a)) = F_i(a_j) = a_{\tilde{\sigma}_j(i)}.$$

1. Exemple « à la main ».

- Vérifier que $P = x^6 + 243$ est normal ; donner la liste L des racines de P, exprimées comme des polynômes en a (avec les notations précédentes).
- Définir chaque élément $\tilde{\sigma}_j$ comme une « permutation list » en regardant quel élément de L correspond à chaque $\sigma_j(a_i)$, $a_i \in L$.
- Vérifier que l'ensemble des $\tilde{\sigma}_j$ forme bien un sous-groupe de S_6, du bon ordre.

2. Écrire une procédure `gal(P)` renvoyant le groupe $Gal(P)$ exprimé comme un `permgroup` selon la syntaxe de Maple. On prendra soin d'imprimer un message d'erreur si P n'est pas irréductible ou s'il n'est pas normal.

3. Tester sur les exemples suivants et identifier, à chaque fois que c'est possible, le groupe de Galois (dans l'esprit de la classification des groupes de petits ordres) :

- $P_1 = x^2 - 1$, $P_2 = x^4 + 3x^2 + 3$;
- $P_3 = x^6 + 12$;
- $P_4 = x^4 + x^3 + x^2 + x + 1$;
- $P_5 = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$;
- $P_6 = x^8 - 12x^6 + 23x^4 - 12x^2 + 1$.

La correspondance de Galois : détermination des sous-corps maximaux dans le cas normal

On rappelle le théorème de Galois (X.4.1 et théorème XIV.3.1) :

Théorème 1. *Soit L/K une extension galoisienne finie de groupe de Galois $G = Gal(L/K)$. On note $\mathcal{K}(L/K)$ l'ensemble des corps intermédiaires M et $\mathcal{G}(G)$ l'ensemble des sous-groupes H de G. Alors les applications*

$$\Phi : \begin{array}{c}\mathcal{K}(L/K) \to \mathcal{G}(G) \\ L \mapsto Gal(L/M)\end{array}, \qquad \Psi : \begin{array}{c}\mathcal{G}(G) \to \mathcal{K}(L/K) \\ H \mapsto L^H = \{x \in L,\ hx = x\ \forall h \in H\}\end{array}$$

sont des bijections réciproques l'une de l'autre. De plus, M/K est une extension normale (donc galoisienne) si et seulement si $H = Gal(L/M)$ est normal (ou distingué) dans G et alors $Gal(M/K) \simeq G/H$.

Pour obtenir les sous-corps *maximaux* d'une extension $\mathbb{Q}(a)/\mathbb{Q}$, il suffit donc de regarder les invariants sous les sous-groupes minimaux de $Gal(\mathbb{Q}(a)/\mathbb{Q})$, *i.e.* les invariants sous *un* élément, disons $\sigma : a \mapsto F(a)$, et faire varier $F(a)$ au sein des racines du polynôme minimal de a.

Pour calculer ces invariants sous σ, on cherche les polynômes $R = \sum_{i=0}^{n-1} c_i x^i$ (où n désigne le degré de l'extension) tels que $\sigma(R(a)) = R(\sigma(a)) = R(a)$ dans $\mathbb{Q}(a)$. Sachant que $(1, a, \ldots, a^{n-1})$ forme une base, cela constitue un système à résoudre en les c_i. On écrit la matrice A du système et on le résout sous Maple avec la commande `LinearAlgebra[NullSpace](A)`.

☞ *Quelques commandes* Maple *utiles* : `coeff`, `collect`, `subs`, `Matrix(n,f)` (où `f:=(i,j)->...` définit les coefficients) ; on ordonne par degré croissant une liste L de polynômes en invoquant `sort(L,ordpoly)`, où

```
> ordpoly:=proc(f,g)
if degree(f,x)<= degree(g,x) then return(true) else return(false) ;
 fi;
  end:
```

4. Soient $P \in \mathbb{Q}[x]$ un polynôme irréductible et $L = \mathbb{Q}(a)$ un corps de rupture. On suppose que L contient une deuxième racine $b = F(a)$. Écrire une procédure `invariant(a,P,F)` qui calcule les invariants, sous l'élément σ du groupe $Gal(L/\mathbb{Q})$ qui envoie a sur b (l'utilisateur a donc défini au préalable `alias(a=RootOf((P)))`). Ces éléments invariants seront présentés sous la forme d'une liste LP de polynômes (ordonnés selon le degré), qui, lorsqu'ils sont évalués en a, constituent une base sur $\mathbb{Q}$ du sous-corps $L^{\langle\sigma\rangle}$.

Tester avec $P = P_5$. On calculera les sous-corps maximaux en faisant varier $F(a)$ au sein des racines de P. Conclure qu'il n'existe pas de corps intermédiaire non trivial. Est-ce étonnant ?

5. Établir la correspondance de Galois pour le polynôme P_4. On donnera la liste des corps intermédiaires M et des sous-groupes H de Galois correspondants. Vérifier que l'on a bien $[M : \mathbb{Q}] = |G|/|H|$.

6. Modifier la procédure `invariant` en une procédure `invariant2:=proc(a,P,F)` renvoyant un élément primitif de $L^{\langle\sigma\rangle}$. On utilisera la procédure `primitif3` écrite au cours du TP.XII, que l'on itère autant de fois que nécessaire. Tester sur l'exemple de la question précédente.

7. On prend $P = P_3$. Déterminer $Gal(P)$, ses sous-groupes, et identifier ceux qui sont normaux.

Modifier la procédure `gal(P)` en une procédure `gal2(a,P)` qui renvoie une liste L d'éléments primitifs des sous-corps maximaux ainsi que la liste des éléments $\tilde{\sigma}_i$ du groupe de Galois, exprimés comme produits de cycles à supports disjoints, en prenant soin que le i-ième élément de L corresponde à $L^{\langle\sigma_i\rangle}$.

Tester sur l'exemple. Calculer également le polynôme minimal des éléments primitifs obtenus. Décrire la correspondance de Galois.

Correspondance de Galois : le cas général

On a besoin de développer, au préalable, une technique de calcul de l'intersection de deux corps de nombres.

Précisément, soient a et b deux nombres algébriques, de polynômes minimaux μ_a et μ_b. Il s'agit de calculer l'intersection $\mathbb{Q}(a)\cap\mathbb{Q}(b)$ dans $\mathbb{Q}(a,b)$. Comme on l'a vu au TP.XII, il faut préciser de quel facteur b est racine dans la décomposition de μ_b en irréductibles dans $\mathbb{Q}(a)[x]$. On le note P_1 et l'on choisit un élément primitif $c = b + \lambda a$, $\lambda \in \mathbb{Q}$, de $\mathbb{Q}(a,b)$.

Écrivons les décompositions en irréductibles de μ_c sur $\mathbb{Q}(a)$ et sur $\mathbb{Q}(b)$:

$$\mu_c = \prod_{i=1}^{r} A_i,\ A_i \in \mathbb{Q}(a)[x]\ ; \quad \mu_c = \prod_{j=1}^{s} B_j,\ B_j \in \mathbb{Q}(b)[x].$$

Le polynôme $P_1(x - \lambda a)$ est un polynôme irréductible de $\mathbb{Q}(a)[x]$ qui annule c : il s'agit donc de l'un des facteurs, disons A_1 quitte à renuméroter.

On définit un graphe dont les sommets sont les A_i et B_j et les arêtes les $[X_k, X_l]$ tels que X_k et X_l ont un facteur commun non trivial dans $\mathbb{Q}(c)[x]$, *i.e.* tels que $\text{pgcd}(X_k, X_l) \neq 1$.

***Proposition* 1.** *Avec les notations précédentes, soit $\mathcal{C}$ l'ensemble des A_i qui sont dans la composante connexe de A_1. Alors $P = \prod_{X\in\mathcal{C}} X$ est un polynôme à coefficients dans $\mathbb{Q}(a)\cap\mathbb{Q}(b)$, dont les coefficients engendrent $\mathbb{Q}(a)\cap\mathbb{Q}(b)$ sur $\mathbb{Q}$.*

Démonstration. Prenant N une clôture galoisienne de $\mathbb{Q}(c)$, il s'agit de prouver que P est invariant sous $Gal(N/\mathbb{Q}(b))$ (puisque P appartient à $\mathbb{Q}(a)[x]$ par définition). Considérons ${}^{\sigma}A_1$, pour $\sigma \in Gal(N/\mathbb{Q}(b))$ donné. Puisque A_1 divise μ_c, il possède un facteur commun non trivial avec l'un B_{j_0} des B_j. Il en est donc de même de ${}^{\sigma}A_1$, avec ${}^{\sigma}B_{j_0} = B_{j_0}$. On voit donc que A_1 et ${}^{\sigma}A_1$ sont reliés par une arête. Si maintenant A_i est dans la composante connexe de A_1, alors ${}^{\sigma}A_i$ est dans la composante connexe de ${}^{\sigma}A_1$, donc de A_1. Cela démontre que σ permute les éléments de $\mathcal{C}$, d'où ${}^{\sigma}P = P$.

Soit L le corps engendré sur $\mathbb{Q}$ par les coefficients de P. On va démontrer que si $\sigma \in Gal(N/\mathbb{Q})$ vérifie ${}^{\sigma}P = P$ (*i.e.* si σ appartient à $Gal(N/L)$), alors σ est l'identité sur $\mathbb{Q}(a) \cap \mathbb{Q}(b)$. Il en résultera l'inclusion $\mathbb{Q}(a) \cap \mathbb{Q}(b) \subset N^{Gal(N/L)} = L$ qui termine de démontrer la proposition. Comme c est racine de A_1, donc de P, on voit que $\sigma(c)$ est racine de ${}^{\sigma}P = P$, donc de l'un A_{i_0} des facteurs de P. On va démontrer qu'il existe $\tau \in Gal(N/\mathbb{Q}(a) \cap \mathbb{Q}(b))$ tel que $\tau(c) = \sigma(c)$. Ainsi τ et σ coïncident sur $\mathbb{Q}(c)$, ce qui démontre l'assertion.

Comme A_1 et A_{i_0} sont dans la même composante connexe, il existe un circuit dans le graphe permettant de passer de $A_1 = X_1$ à $A_{i_0} = X_t$. Il existe une racine $\alpha_2 \in N$ commune à A_1 et X_2, donc $\tau_1 \in Gal(N/\mathbb{Q}(a))$ tel que $\tau_1(c) = \alpha_2$. De même, on trouve $\alpha_3 \in N$ qui annule X_2 et X_3, donc τ_2 appartenant à $Gal(N/\mathbb{Q}(a))$ ou $Gal(N/\mathbb{Q}(b))$ tel que $\tau_2(\alpha_2) = \alpha_3$, selon que X_2 est un A_i ou un B_j. On continue ainsi jusqu'à τ_{t-1} tel que $\tau_{t-1}(\alpha_{t-1}) = \alpha_t$, avec α_t racine de $X_t = A_{i_0}$. Enfin, il existe $\tau_t \in Gal(N/\mathbb{Q}(a))$ tel que $\tau_t(\alpha_t) = \sigma(c)$. On prend pour τ la composée des τ_k. □

☞ *Quelques remarques concernant la manipulation des graphes sous* Maple :
Un graphe est défini par une commande

`graphe:=network[graph](sommet,aretes);`

où les n sommets sont, par exemple, les entiers de 1 à n et les arêtes sont de la forme $\{i_k, j_k\}$, c'est-à-dire

`sommets:={$1..n}` et `aretes:={{i1,j1},...,{ir,jr}}`.

La composante connexe de 1 s'obtient alors en invoquant

`networks[components](graphe,root=1)`.

Un algorithme de parcours du graphe est en effet implémenté dans Maple. La théorie des graphes n'étant pas le propos de cet ouvrage, il sera passé sous silence.

8. Commençons par traiter un exemple. On prend $\mu_a = x^4 - 10x^2 + 1$, $\mu_b = x^4 - 4x^2 - 2$ et $P_1 = \mu_{b,\mathbb{Q}(a)}$ l'un des facteurs irréductibles de la décomposition de μ_b sur $\mathbb{Q}(a)$ (au choix). Déterminer un élément primitif c et exprimer a et b comme des polynômes $a(c)$ et $b(c)$ (toutes les procédures ont été écrites au TP.XII !). En déduire les A_i et B_j en tant qu'éléments de $\mathbb{Q}(c)[x]$. Définir le graphe où les r premiers sommets correspondent aux A_i et les s suivants aux

B_j, puis calculer P. En déduire finalement $\mathbb{Q}(a)\cap\mathbb{Q}(b)$. On en donnera un élément primitif, dont on calculera également le polynôme minimal. En déduire que l'intersection $\mathbb{Q}(a)\cap\mathbb{Q}(b)$ est, en fait, $\mathbb{Q}(\sqrt{6})$.

9. On veut automatiser tout cela. Écrire une procédure `interP:=proc(P1,a,Q)` renvoyant, en fonction de P_1, a et $\mu_a = Q$, un élément primitif d de $\mathbb{Q}(a)\cap\mathbb{Q}(b)$ en tant que polynôme en c, le polynôme minimal de c et le polynôme minimal de d. Tester sur l'exemple de la question précédente.

Modifier la procédure `interP` en une procédure `interP2:=proc(P1,a,Q)` renvoyant d exprimé comme un polynôme en a, ainsi que son polynôme minimal. Tester sur l'exemple précédent. Prendre également $\mu_a = x^3+x+1$, $\mu_b = x^3-x^2+4x-3$ et pour P_1 les deux choix possibles. Tester enfin avec des extensions $\mathbb{Q}(a)$ et $\mathbb{Q}(b)$ de votre choix, dont les degrés sur $\mathbb{Q}$ sont premiers entre eux (bien entendu, on doit trouver $\mathbb{Q}$).

On dispose maintenant de tous les ingrédients. L'objectif est de trouver tous les sous-corps maximaux d'un corps de nombres $K = \mathbb{Q}(a)$ qui n'est plus forcément galoisien sur $\mathbb{Q}$. Le polynôme minimal μ_a de a se décompose sur K en facteurs irréductibles qui ne sont plus tous nécessairement de degré un. On associe à chaque facteur irréductible $P_i \neq x-a$ un sous-corps K_i comme suit :

- si $P_i = x - a_i$ alors $K_i = K^{\langle\sigma_i\rangle}$, où σ_i désigne le $\mathbb{Q}$-automorphisme de K qui envoie a sur a_i ;
- si, par contre, $\deg P_i \geqslant 2$, on pose $K_i = K\cap\mathbb{Q}(\alpha_i)$, pour α_i une racine quelconque de P_i dans une extension convenable (cela ne dépend pas du choix effectué, car les racines sont conjuguées par un $\mathbb{Q}(a)$-automorphisme qui laisse l'intersection inchangée).

Proposition 2. *Les sous-corps maximaux de K sont parmi les corps K_i ainsi construits.*

Démonstration. Soient N une clôture galoisienne de K (*i.e.* un corps de décomposition de μ_a) et L un sous-corps maximal de K. L'extension $N/\mathbb{Q}$ est galoisienne et, par la correspondance de Galois, il correspond à L un sous-groupe $G_L = Gal(N/L)$ de $G = Gal(N/\mathbb{Q})$. On considère également $G_K = Gal(N/K)$. On a donc $G_K \subset G_L \subset G$ et il n'existe pas de sous-groupe entre G_K et G_L, car L est maximal dans K. Par conséquent, le groupe G_L est engendré par G_K et un élément quelconque σ que l'on se donne dans $G_L \setminus G_K$.

Afin de traduire cela en théorie des corps, on peut dire aussi que G_L est engendré par G_K et $\sigma G_K\sigma^{-1}$, si $G_K \neq \sigma G_K\sigma^{-1}$, et par G_K et σ sinon.

Dans le premier cas, le corps laissé fixe par G_K et $\sigma G_K \sigma^{-1}$ est le corps $K \cap \mathbb{Q}(\sigma(a))$ et $\sigma(a)$ est une racine de μ_a. Dans le second cas, $\sigma(a)$ appartient à K, puisque $G_K = \sigma G_K \sigma^{-1}$, et le corps laissé fixe par G_K et σ est $\mathbb{Q}(\sigma(a))^{\langle\sigma\rangle}$. Cela démontre la proposition. □

On est donc ramené au calcul de l'intersection de deux corps de nombres, problème déjà résolu. On trouve tous les sous-corps en réitérant au besoin le processus (on calcule les sous-corps maximaux des sous-corps maximaux, etc.).

10. Écrire une procédure `SousCorps:=proc(P)` renvoyant, en fonction du polynôme irréductible P définissant le corps de rupture $K = \mathbb{Q}(a)$ (à isomorphisme près), une liste d'éléments primitifs des corps K_i de la proposition 2. Pour chaque exemple ci-dessous, déterminer tous les sous-corps propres et préciser ceux qui sont maximaux :

- $P_1 = x^3 + 3x^2 - x - 4$, $P_2 = x^6 + 2x^3 - 2$
- $P_3 = x^6 - 3x^5 + 6x^4 - 7x^3 + 2x^2 + x - 4$, $P_4 = x^6 + 3x^3 + 3$
- $P_5 = x^6 - 3x^2 + 1$, $P_6 = x^6 + 2x^4 + 2x^3 + x^2 + 2x + 2$.

Remarque. Cette approche est due à Laudau et Miller. Le lecteur intéressé trouvera décrite dans [22] une autre méthode qui mêle ces techniques à des techniques « modulaires ». En effet, on constate vite que les calculs algébriques sont assez gourmands en temps (pour P_6 par exemple), d'où la nécessité de développer de nouvelles stratégies.

This page intentionally left blank

XV

RACINES DE L'UNITÉ CORPS FINIS EXTENSIONS CYCLIQUES

Le but de ce chapitre est d'étudier quelques exemples d'extensions galoisiennes qui sont d'une importance capitale en arithmétique. Outre une description du groupe de Galois du corps des racines n-ième de l'unité, on démontrera que les corps finis sont nécessairement commutatifs et que leurs groupes de Galois sont engendrés par le morphisme de Frobenius. De plus, par l'étude des extensions cycliques, on abordera la théorie générale des extensions de Kummer.

XV.1. Racines de l'unité

***Définition* XV.1.1.** On dit qu'un élément x d'un corps K est une **racine n-ième de l'unité** s'il existe un entier $n > 0$ tel que $x^n = 1$. On dit que x est une **racine de l'unité** s'il existe un entier n tel que x soit une racine n-ième de l'unité.

Les racines de l'unité sont des éléments d'ordre fini du groupe multiplicatif K^*. Elles forment un sous-groupe $U(K)$ de K^* et les racines n-ième de l'unité forment un sous-groupe $U_n(K)$ de $U(K)$. Soit x un élément de K^* : on considère le morphisme de groupes $\varphi : \mathbb{Z} \longrightarrow K^*$ défini par $\varphi(a) = x^a$. Si x est un élément de $U(K)$, l'ensemble des $m \in \mathbb{Z}$ tels que $x^m = 1$ est le noyau de φ, c'est donc un sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$, où n est l'ordre de x dans K^*.

Lemme XV.1.1. *Si K est un corps de caractéristique $p > 0$ et si x est une racine de l'unité dans K, son ordre n'est pas divisible par p.*

Démonstration. Soit n l'ordre de x et supposons que $n = pm$. Alors, $x^{pm} = 1$ entraîne que $(x^m - 1)^p = x^{pm} - 1 = 0$ (*cf.* proposition IX.1.3), d'où $x^m = 1$ avec $m < n$. Contradiction. □

Corollaire XV.1.1. *Si K est un corps de caractéristique $p > 0$, alors, pour tout entier $m > 0$, il n'existe pas dans K de racine p^m-ième de l'unité autre que 1.* □

Remarques XV.1.1.

a) C'est également le cas, si $K = \mathbb{Q}$, pour les racines n-ième de l'unité, avec n impair.

b) Une racine n-ième de l'unité dans K étant racine du polynôme $X^n - 1 = 0$, est algébrique sur le sous-corps premier P de K. On peut donc, ce que nous ferons dans la suite, se placer dans une clôture algébrique $\overline{P}$ de P.

c) Si K est un corps de caractéristique $p > 0$ et si n est un entier non divisible par p, toute racine du polynôme $X^n - 1$ est simple, car le polynôme dérivé nX^{n-1} n'admet que zéro comme racine, qui n'est pas racine de $X^n - 1$. Il existe donc exactement n racines n-ième de l'unité dans $\overline{K}$. Autrement dit, le polynôme $X^n - 1$ est séparable sur K. On en déduit le théorème suivant :

Théorème XV.1.1. *Soient K un corps de caractéristique $p > 0$ et n un entier premier avec p. Le groupe $U_n(K)$ des racines n-ième de l'unité (dans $\overline{K}$) est un groupe cyclique d'ordre n.*

Démonstration. Ce qui précède montre que $U_n(K)$ est un groupe fini d'ordre n dans $\overline{K}^*$. On sait d'après (TR.IX.A) qu'un tel groupe est cyclique. □

Définition XV.1.2. Un générateur du groupe $U_n(K)$ est appelé racine n-ième **primitive** de l'unité.

Remarque XV.1.2. Si K est un corps de caractéristique $p > 0$ ne divisant pas n, le nombre des racines n-ième primitives de l'unité dans $\overline{K}$ est égal à $\varphi(n)$, où φ est l'indicateur d'Euler (*cf.* TR.I.B).

Exercice XV.1.

1. Soient $k \subset M$ une extension finie, K et L deux corps intermédiaires et KL le sous-corps de M engendré par K et L. Démontrer que $[KL : L] \leqslant [K : k]$.

2. Soient m et n des entiers premiers entre eux, ζ une racine primitive m-ième de l'unité, β une racine primitive n-ième de l'unité (ζ et β dans $\mathbb{C}$). Montrer que $\mathbb{Q}(\zeta) \cap \mathbb{Q}(\beta) = \mathbb{Q}$. (Indication : on pourra démontrer que le plus petit sous-corps de $\mathbb{C}$ contenant ζ et β est $\mathbb{Q}(\zeta, \beta) = \mathbb{Q}(\zeta\beta)$, engendré par une racine mn-ième primitive de l'unité. En déduire le degré de l'extension $\mathbb{Q}(\zeta, \beta)/\mathbb{Q}(\beta)$ et appliquer 1.)

XV.2. Corps des racines n-ième de l'unité

***Définition* XV.2.1.** Soit K un corps. On appelle **corps des racines n-ième de l'unité** sur K un corps de décomposition sur K du polynôme $X^n - 1$.

Soit ζ une racine n-ième primitive de l'unité. Alors $\mathbb{U}_n(K) = \zeta^k$, $0 \leqslant k \leqslant n-1$ et les racines primitives sont celles pour lesquelles l'exposant k est premier avec n. Le corps des racines n-ième de l'unité sur K est $K(\zeta)$.

D'après ce qui précède, si K est un corps dont la caractéristique est nulle ou est un nombre premier ne divisant pas n, l'extension $K(\zeta)/K$ est galoisienne.

***Définition* XV.2.2.** Une extension E/K est dite **abélienne** si elle est galoisienne de groupe de Galois abélien.

***Remarque* XV.2.1.** D'après les théorèmes fondamentaux de la théorie de Galois, si E/K est une extension abélienne finie, il en est de même pour les extensions E/L et L/K, pour tout corps intermédiaire L.

***Théorème* XV.2.1.** *Soient K un corps, n un entier positif, ζ une racine n-ième primitive de l'unité dans $\overline{K}$.*

(i) *Si K est un corps de caractéristique $p > 0$, p ne divisant pas n, l'extension $K(\zeta)/K$ est abélienne finie. Son groupe de Galois est isomorphe à un sous-groupe du groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

(ii) *Si $K = \mathbb{Q}$, on a $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ et le groupe de Galois de l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est isomorphe au groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. (i). Pour tout $s \in Gal(K(\zeta)/K)$, $s(\zeta)$ doit être une racine n-ième primitive de l'unité, car $\zeta^m = 1$ est équivalent à $s(\zeta)^m = 1$. Par conséquent, $s(\zeta) = \zeta^q$, où q est un nombre premier avec n et compris entre 1 et n, c'est-à-dire

que q représente un élément inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Considérons l'application $\chi : Gal(K(\zeta)/K) \longrightarrow \mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ ainsi définie, où $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ est le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Si $t \neq s$ est un élément de $Gal(K(\zeta)/K)$, avec $t(\zeta) = \zeta^r$, on a $\chi(st) = \chi(s)\chi(t)$, χ est un morphisme de groupes. Deux éléments s et t de $Gal(K(\zeta)/K)$ sont égaux si et seulement si $s(\zeta) = t(\zeta)$. On en déduit que le morphisme χ est injectif, d'où le résultat.

(ii). Pour montrer le résultat, il suffit de montrer que si $K = \mathbb{Q}$, le morphisme χ ci-dessus est surjectif. Pour cela, il suffit de montrer que pour tout nombre premier p, $1 \leqslant p \leqslant n$, ne divisant pas n, ζ^p est une racine du polynôme minimal de ζ sur $\mathbb{Q}$, $M_\zeta(X)$. Ce polynôme divise $X^n - 1$, *i.e.* $X^n - 1 = M_\zeta(X)f(X)$ dans $\mathbb{Q}[X]$. Si ζ^p n'est pas racine de $M_\zeta(X)$, alors ζ^p est racine de $f(X)$, donc ζ est racine du polynôme $f(X^p)$. Par conséquent, $M_\zeta(X)$ divise $f(X^p)$, $f(X^p) = M_\zeta(X)g(X)$. Puisque $M_\zeta(X)$ et $f(X)$ ont un coefficient dominant égal à 1 et divisent $X^n - 1$, d'après le lemme de Gauss (*cf.* chapitre VIII), $M_\zeta(X)$ et $f(X)$ sont à coefficients dans $\mathbb{Z}$. Il en est donc de même pour $g(X)$. Or, p étant un nombre premier, on sait que pour tout nombre entier u, on a : $u^p \equiv u \, mod(p)$. On en déduit que $f(X^p) \equiv f(X)^p \, mod(p)$, donc que $f(X)^p \equiv M_\zeta(X)g(X) \, mod(p)$. Si on note $\overline{f}(X)$ et $\overline{M_\zeta}(X)$ les polynômes de $(\mathbb{Z}/p\mathbb{Z})[X]$ obtenus à partir de $f(X)$ et $M_\zeta(X)$ en considérant la réduction modulo p sur les coefficients, on déduit de ce qui précède que $\overline{M_\zeta}(X)$ et $\overline{f}(X)$ ont un facteur commun, donc que $X^n - \overline{1}$ a une racine multiple, ce qui est en contradiction avec la remarque (XV.1.1.c). Donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = |Gal(\mathbb{Q}(\zeta)/\mathbb{Q})| = |\mathbb{U}(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$. □

***Remarque* XV.2.2.** Dans le cas de la caractéristique strictement positive, $\mathrm{Gal}(K(\zeta)/K)$ peut être isomorphe à un sous-groupe strict de $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ (*cf.* exemple XV.3.1 ci-dessous).

On peut généraliser l'étude précédente au cas du polynôme $X^n - a$, $a \in K$. Le cas général étant assez délicat (*cf.* TR.XV.C), nous allons nous placer sous des hypothèses restrictives, mais qui nous suffiront dans la suite.

***Proposition* XV.2.1.** *Soient K un corps de caractéristique nulle dans lequel le polynôme $X^n - 1$ est scindé, a un élément de K, L un corps de décomposition de $X^n - a$ sur K. Le groupe de Galois de L/K est abélien.*

Démonstration. Soit α une racine de $X^n - a$. Si ϵ est une racine n-ième de l'unité, il est clair que $\epsilon\alpha$ est une racine de $X^n - a$. On décrit ainsi toutes les racines de $X^n - a$ à partir de α en la multipliant par les racines n-ième de l'unité. Puisque les racines n-ième de l'unité sont dans K, on en déduit que $L = K(\alpha)$. Les éléments de $Gal(L/K)$ sont donc déterminés par les images de α. Soient s et t les

éléments de $Gal(L/K)$ définis par $s(\alpha) = \epsilon\alpha$, $t(\alpha) = \eta\alpha$, avec $\epsilon^n = \eta^n = 1$: alors, $s \circ t(\alpha) = \epsilon\eta\alpha = \eta\epsilon\alpha = t \circ s(\alpha)$, d'où $Gal(L/K)$ est abélien. □

***Remarque* XV.2.3.** On trouvera une version plus précise de ce théorème au théorème XV.5.2.

***Exercice* XV.2.** Soit $p \neq 2$ un nombre premier. Montrer que le corps $\mathbb{Q}(\mathbb{U}_p)$ a un unique sous-corps E tel que $E/\mathbb{Q}$ soit une extension quadratique. Montrer que si $p \equiv 1 \pmod 4$, alors $E \subset \mathbb{R}$, et que si $p \equiv 3 \pmod 4$, alors $E \not\subset \mathbb{R}$. (Indication : notant ζ une racine p-ième primitive, $f(x) = x^p - 1$ et $d = \prod_{1 \leqslant i < j \leqslant p}(\zeta^i - \zeta^j)$, on calculera le discriminant (*cf.* TR.XVI.A) $D(f) = d^2$ à l'aide de la formule $D(f) = (-1)^{\frac{p(p-1)}{2}} \prod f'(\zeta^i)$. En déduire que $E = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$.)

XV.3. Polynômes cyclotomiques

Soient K un corps, P son sous-corps premier, n un entier non divisible par la caractéristique p de K. On sait qu'il y a, dans $\overline{P}$, $\varphi(n)$ racines n-ième primitives de l'unité, $\zeta_1, \ldots, \zeta_{\varphi(n)}$. On considère le polynôme, appelé ***polynôme cyclotomique*** d'indice n,

$$\Phi_n(X) = \prod_{i=1}^{\varphi(n)} (X - \zeta_i).$$

Notons G_0 le groupe de Galois de l'extension $K(\zeta)/K$, où ζ est l'une des ζ_i. Le polynôme $\Phi_n(X)$ est invariant sous l'action de G_0, par conséquent $\Phi_n(X) \in K[X]$.

***Remarque* XV.3.1.**

a) Pour que $\Phi_n(X)$ soit irréductible, il faut et il suffit que l'ordre de G_0 soit égal à $\varphi(n)$. En effet, si $\Phi_n(X)$ est irréductible, alors $[K(\zeta) : K] = \varphi(n)$, d'où $|G_0| = \varphi(n)$. Réciproquement, si $|G_0| = \varphi(n)$, comme $K(\zeta)/K$ est galoisienne, alors $[K(\zeta) : K] = \varphi(n) = deg(\Phi_n)$; comme $\Phi_n(\zeta) = 0$, $M_\zeta(X)$ divise $\Phi_n(X)$ et, puisque $deg(M_\zeta(X)) = deg(\Phi_n(X))$ et que $\Phi_n(X)$ est unitaire, $\Phi_n(X)$ est irréductible.

b) On déduit de ce qui précède que $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$ et égal à $M_\zeta(X)$.

Soit x une racine n-ième de l'unité. Si x est d'ordre d, alors d divise n et x est une racine d-ième primitive de l'unité. Réciproquement toute racine d-ième

primitive de l'unité est racine n-ième de l'unité si d divise n. On a donc

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

ou encore

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d<n, d|n} \Phi_d(X)}.$$

Par conséquent, on peut construire $\Phi_n(X)$ dès qu'on connaît $\Phi_d(X)$ pour les diviseurs d de n. Ceci permet de dégager un procédé de construction par récurrence des polynômes cyclotomiques.

En particulier, comme $\Phi_1(X) = X - 1$, si n est un nombre premier, on a $X^n - 1 = (X - 1)\Phi_n(X)$, d'où $\Phi_n(X) = X^{n-1} + \ldots + X + 1$.

***Remarque* XV.3.2.** La méthode de calcul de $\Phi_n(X)$ par récurrence indiquée ci-dessus, pour $K = \mathbb{Q}$, prouve que $\Phi_n(X) \in \mathbb{Z}[X]$ et que les coefficients sont déterminés par la même formule de récurrence quel que soit le corps K. On démontre ainsi, par récurrence, que si K est un corps de caractéristique p, alors $\Phi_{n,K}(X)$ s'obtient à partir de $\Phi_{n,\mathbb{Q}}$ par réduction des coefficients modulo p.

***Exemple* XV.3.1.** Appliquons le procédé de récurrence pour calculer $\Phi_{12}(X)$. Les diviseurs de 12 sont 1, 2, 3, 4, 6, 12. Donc

$$X^{12} - 1 = \Phi_{12}(X)\Phi_6(X)\Phi_4(X)\Phi_3(X)\Phi_2(X)\Phi_1(X).$$

On a $X^{12} - 1 = (X^6 - 1)(X^6 + 1)$. Mais, puisque

$$X^6 - 1 = \Phi_6(X)\Phi_3(X)\Phi_2(X)\Phi_1(X),$$

alors

$$X^6 + 1 = \Phi_{12}(X)\Phi_4(X).$$

Mais

$$X^4 - 1 = \Phi_4(X)\Phi_2(X)\Phi_1(X),$$

et comme $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, on a $\Phi_4(X) = X^2 + 1$, d'où

$$\Phi_{12}(X) = X^4 - X^2 + 1.$$

Dans un corps de caractéristique 5 (par exemple $\mathbb{Z}/5\mathbb{Z}$), on a

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

Ceci prouve, d'après la remarque (XV.3.1.a), que dans le cas $n = 12$, $p = 5$, le corps des racines n-ième de l'unité sur K est une extension galoisienne dont le groupe de Galois est un sous-groupe strict de $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$.

XV.4. Corps finis

Contrairement à ce que nous avons considéré jusqu'à maintenant, nous allons supposer que le corps K est non nécessairement commutatif, c'est-à-dire que la multiplication n'est pas commutative (et donc le groupe K^* n'est pas abélien). Nous avons vu au TR.IX.B un exemple d'un tel corps : le corps des quaternions.

Nous allons démontrer le célèbre théorème de Wedderburn :

Théorème XV.4.1. *Un corps fini est commutatif.*

Démonstration. Soit F un corps fini, supposé non nécessairement commutatif. On considère son centre $Z(F) = \{x \in F \mid \forall y \in F, xy = yx\}$. Il est clair que $Z(F)$ est un sous-corps commutatif fini de F, donc de caractéristique $p > 0$. Par conséquent, en notant $\mathbb{F}_p$ le corps premier de caractéristique p, ($\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$) et $[Z(F) : \mathbb{F}_p] = f$, le cardinal de $Z(F)$ est $q = p^f$. La multiplication dans F munit F d'une structure de $Z(F)$-espace vectoriel et, puisque F est fini, $\dim_{Z(F)} F = n < +\infty$. De sorte que le cardinal de F est $q^n = (p^f)^n$. Soit x un élément non nul, donc inversible, de F. On considère $Z(x) = \{y \in F \mid xy = yx\}$: il est clair que $Z(x)$ est un sous-corps de F contenant $Z(F)$. Le cardinal de $Z(x)$ est égal à $q^{d(x)}$, où $d(x) = \dim_{Z(F)} Z(x)$. On considère l'action du groupe $F^* = F \setminus \{0\}$ sur lui-même par conjugaison ; on obtient une partition de F^* en orbites (disjointes) et ces orbites sont en nombre fini. Une application immédiate de l'équation aux classes (corollaire IV.2.1) donne l'égalité :

$$q^n - 1 = q - 1 + \sum_{x \in P} \frac{q^n - 1}{q^{d(x)} - 1}, \qquad (\star)$$

où P est un ensemble de représentants $x \in F^\star$ des orbites non ponctuelles, (*i.e.* $x \notin Z(F)$). Cet ensemble P est vide si et seulement si $F = Z(F)$, *i.e.* $n = 1$. Supposons que $n > 1$. On considère le polynôme cyclotomique $\Phi_n(X)$. Il résulte de l'égalité $X^n - 1 = \prod_{d|n} \Phi_d(X)$, que pour tout entier d divisant n, $d \neq n$, le polynôme $\Phi_n(X)$ divise le polynôme $\frac{X^n-1}{X^d-1}$. On en déduit que $\Phi_n(q)$ divise $q^n - 1$ et $\sum_{x \in P} \frac{q^n - 1}{q^{d(x)} - 1}$, donc, d'après $(\star)$, il divise aussi $q - 1$. Or, $\Phi_n(q) = \prod_i (q - \zeta_i)$, où les ζ_i sont les racines n-ième primitives de l'unité, donc différentes de 1 et, vues dans $\mathbb{C}$, de module 1. Comme $q \geqslant 2$, on a $\mid q - \zeta_i \mid > q - 1$. On en déduit que $\Phi_n(q)$ ne peut diviser $q - 1$ dans $\mathbb{Z}$, d'où une contradiction. Par conséquent, $n = 1$, *i.e.* $F = Z(F)$ et F est commutatif. □

L'étude des corps finis se ramène donc à celle des corps commutatifs finis. Nous allons maintenant compléter les résultats établis au chapitre IX. Nous allons énoncer un théorème général et renvoyer au chapitre IX pour les démonstrations des résultats établis alors.

Théorème XV.4.2. (i) *Un corps fini a une caractéristique $p > 0$ et son cardinal q est une puissance de p. Si $q = p^n$, son groupe additif est somme directe de n groupes cycliques d'ordre p, son groupe multiplicatif est cyclique d'ordre $q - 1$.*

(ii) *Pour tout nombre premier p et tout entier $n > 0$, il existe un corps $\mathbb{F}_q$ ayant $q = p^n$ éléments. Ce corps est un corps de décomposition du polynôme $X^q - X$ sur le corps premier $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et tout élément de $\mathbb{F}_q$ est racine de ce polynôme.*

(iii) *Tout corps fini à $q = p^n$ éléments est isomorphe à $\mathbb{F}_q$.*

Démonstration. Pour l'assertion (i), *cf.* chapitre IX.

Démontrons l'assertion (ii). Soit $q = p^n$; on considère dans $\overline{\mathbb{F}_p}$ un corps de décomposition, noté $\mathbb{F}_q$, du polynôme $X^q - X$ sur $\mathbb{F}_p$. Le polynôme dérivé étant égal à -1, toutes les racines de $X^q - X$ sont simples. Il y a donc, dans $\mathbb{F}_q$, q éléments distincts qui sont les racines de $X^q - X$. Montrons que ces racines forment un corps : soient α et β deux quelconques de ces racines. On a :

$$(\alpha + \beta)^q - (\alpha + \beta) = \alpha^q + \beta^q - \alpha - \beta = 0,$$

$$(-\alpha)^q - (-\alpha) = (-1)^q \alpha^q + \alpha\,;$$

si p est impair, $(-1)^q = -1$ et $-\alpha$ est racine ; si p est pair $-1 = 1$ dans $\mathbb{Z}/2\mathbb{Z}$ et $-\alpha$ est racine. De plus,

$$(\alpha\beta)^q - \alpha\beta = \alpha^q \beta^q - \alpha\beta = \alpha\beta - \alpha\beta = 0$$

et

$$\alpha \neq 0,\ (\alpha^{-1})^q - \alpha^{-1} = (\alpha^q)^{-1} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0.$$

Les racines de $X^q - X$ forment un corps et elles engendrent $\mathbb{F}_q$ sur $\mathbb{F}_p$. Ce corps est donc égal à $\mathbb{F}_q$, ce qui prouve (ii).

Démontrons l'assertion (iii). Si F est un corps ayant q éléments, tout élément $x \in F$ vérifie $x^q = x$ (cf. chapitre IX), donc est racine du polynôme $X^q - X$. Ceci entraîne que le polynôme $X^q - X$ a q racines distinctes dans F, qui sont donc toutes simples. Autrement dit F est un corps de décomposition (sur $\mathbb{F}_p$) du polynôme $X^q - X$, il est donc isomorphe à $\mathbb{F}_q$. □

Exercice XV.3. Soient p un nombre premier, n et r des entiers positifs.

a) Montrer que si $(r, p^n - 1) = 1$, tout élément de $\mathbb{F}_{p^n}$ est une puissance r-ième.

b) Montrer que si r divise $p^n - 1$, un élément x de $\mathbb{F}_{p^n}$ est une puissance r-ième si et seulement si $x^{(p^n-1)/r} = 1$.

Rappelons que nous avons montré au TR.IX.A le résultat suivant :

Proposition XV.4.1. *Si K un corps fini de caractéristique $p > 0$, le morphisme de Frobenius*

$$\varphi : K \longrightarrow K, \quad \varphi(x) = x^p$$

est un automorphisme. □

Théorème XV.4.3. *Soient p un nombre premier, $n > 0$ un entier, $\mathbb{F}_q$ un corps à $q = p^n$ éléments.*

(i) *Tout automorphisme de $\mathbb{F}_q$ est un $\mathbb{F}_p$-automorphisme.*

(ii) *L'extension $\mathbb{F}_q/\mathbb{F}_p$ est abélienne ; son groupe de Galois est cyclique, engendré par l'automorphisme de Frobenius.*

Démonstration. (i). Soit s un automorphisme de $\mathbb{F}_q$. Montrons que s laisse fixes les éléments de $\mathbb{F}_p$. Soit $x \in \mathbb{F}_p$; on a $x^p = x$, d'où $s(x^p) = s(x)^p = s(x)$ et $s(x) \in \mathbb{F}_p$. Donc $s_{|\mathbb{F}_p}$ est un automorphisme de $\mathbb{F}_p$, d'où $s_{|\mathbb{F}_p}$ est égal à l'identité.

(ii). Par construction, l'extension $\mathbb{F}_q/\mathbb{F}_p$ est galoisienne, de degré n. Soit φ l'automorphisme de Frobenius de $\mathbb{F}_q$ et G le groupe engendré par φ. On a $\varphi^n(x) = x^{p^n} = x$ pour tout $x \in \mathbb{F}_q$, donc $\varphi^n = id$. Soit $d \leqslant n$ l'ordre de φ. Pour tout x de $\mathbb{F}_q$, on a $\varphi^d(x) = x^{p^d} = x$; on en déduit que tout élément de $\mathbb{F}_q$ est racine du polynôme $X^{p^d} - X$, par conséquent, $d = n$. Puisque $[\mathbb{F}_q : \mathbb{F}_p] = n$, on sait que $Gal(\mathbb{F}_q/\mathbb{F}_p)$ est d'ordre n. On a donc $G \subset Gal(\mathbb{F}_q/\mathbb{F}_p)$ et $| G | = | Gal(\mathbb{F}_q/\mathbb{F}_p) |$. D'où l'égalité $Gal(\mathbb{F}_q/\mathbb{F}_p) = G = < \varphi >$. □

On obtient, de la même manière, la généralisation suivante.

Théorème XV.4.4. *Soient p un nombre premier, m et n deux entiers positifs.*

(i) *$\mathbb{F}_{p^n}$ et $\mathbb{F}_{p^m}$ étant considérés comme deux sous-corps de $\overline{\mathbb{F}_p}$, $\mathbb{F}_{p^n}$ est contenu dans $\mathbb{F}_{p^m}$ si et seulement si n divise m.*

Supposons que $m = nd$ et posons $q = p^n$.

(ii) *Pour tout générateur ζ du groupe cyclique $\mathbb{F}_{p^m}^*$, on a $\mathbb{F}_{p^m} = \mathbb{F}_q(\zeta)$.*

(iii) *Dans une extension algébriquement close de $\mathbb{F}_q$, il existe une seule extension de $\mathbb{F}_q$, de degré d, isomorphe à $\mathbb{F}_{p^m}$.*

(iv) *L'extension $\mathbb{F}_{p^m}/\mathbb{F}_q$ est abélienne ; son groupe de Galois est cyclique d'ordre d, engendré par φ^n, où φ est l'automorphisme de Frobenius de $\mathbb{F}_q/\mathbb{F}_p$* (i.e. $\varphi(x) = x^p$). □

Exercice XV.4.

1. Soient F un corps fini et $P(X) \in F[X]$ un polynôme irréductible de degré n. Montrer que le groupe $Gal(P)$ est engendré par le n-cycle $(1, \ldots, n)$, après numérotation convenable des racines lors de l'identification de $Gal(P)$ avec un sous-groupe de S_n. (On remarquera que, dans le cas des corps finis de cardinal q, un corps de rupture d'un polynôme irréductible est corps de décomposition, en faisant agir le Frobenius $x \mapsto x^q$.)

2. Soient $P(X) \in F[X]$ un polynôme de degré n et

$$P(X) = P_1(X) \ldots P_r(X)$$

sa décomposition en irréductibles, les racines de chaque facteur étant supposées de multiplicité 1 (P possède donc n racines distinctes dans une clôture algébrique $\overline{F}$ de F). On note $n_i = deg(P_i(X))$, $1 \leqslant i \leqslant r$. Montrer que le groupe $Gal(P)$ est engendré par le produit des r cycles

$$(1, \ldots, n_1),\ (n_1 + 1, \ldots n_1 + n_2),\ \ldots, (n_1 + \ldots + n_{r-1} + 1, \ldots, n)$$

quitte à numéroter correctement les racines. (On remarquera que si x_i désigne une racine quelconque de P_i dans $\overline{F}$, alors $K = F(x_1, \ldots, x_r)$ est un corps de décomposition de P et que $x_i^{q^m} = x_i$ pour tout i si et seulement si m est un multiple de $\mu = ppcm(n_i)$. En déduire que K/F est de degré μ et conclure.)

XV.5. Extensions cycliques

Définition XV.5.1. On appelle **extension cyclique** d'un corps K toute extension E/K galoisienne finie dont le groupe de Galois est cyclique.

Les corps finis sont des exemples de telles extensions.

Pour étudier cette classe d'extensions, nous allons d'abord établir un résultat très important, connu sous le nom de théorème de Hilbert 90. Rappelons la définition de la norme donnée au chapitre XIII (*cf.* définition XIII.5.1 et exercice XIII.5).

***Définition* XV.5.2.** Soient E/K une extension finie séparable et normale et $G = Gal(E/K)$. La **norme** $N(x)$ d'un élément $x \in E$ est définie par $N(x) = \prod_{s\in G} s(x)$.

***Remarque* XV.5.1.** Cette expression est bien définie puisque $|G| < +\infty$. Si l'extension E/K est galoisienne, alors $N(x) \in K$. En effet, pour tout $\tau \in G$, on a $\tau(N(x)) = \tau(\prod_{s\in G} s(x)) = \prod_{s\in G} \tau \circ s(x)$. Mais, puisque $|G| < +\infty$, quand s parcourt G, $\tau \circ s$ aussi, d'où $\tau(N(x)) = N(x)$ et $N(x) \in Inv(G) = K$.

***Théorème* XV.5.1 (Hilbert 90, version multiplicative).** *Soit E/K une extension normale finie dont le groupe de Galois G est cyclique, engendré par un élément τ. Un élément $x \in E$ est tel que $N(x) = 1$ si et seulement s'il existe $y \in E$, $y \neq 0$, tel que $x = \frac{y}{\tau(y)}$.*

Démonstration. Supposons que $\mid G \mid = n$ et qu'il existe $y \neq 0$ dans E tel que $x = \frac{y}{\tau(y)}$. Alors,

$$N(x) = x\tau(x)\tau^2(x)\dots\tau^{n-1}(x)$$
$$= \frac{y}{\tau(y)}\frac{\tau(y)}{\tau^2(y)}\frac{\tau^2(y)}{\tau^3(y)}\dots\frac{\tau^{n-1}(y)}{\tau^n(y)} = \frac{y}{\tau^n(y)} = \frac{y}{y} = 1.$$

Réciproquement, supposons que $N(x) = 1$; pour tout élément $z \in E$, on pose

$$u_0 = xz,\ u_1 = (x\tau(x))\tau(z), \dots, u_i = (x\tau(x)\dots\tau^i(x))\tau^i(z)$$

pour $0 \leqslant i \leqslant n-1$. Alors $u_{n-1} = N(x)\tau^{n-1}(z) = \tau^{n-1}(z)$. De plus $u_{i+1} = x\tau(u_i)$, $0 \leqslant i \leqslant n-2$. On définit alors $y = u_0 + u_1 + \dots + u_{n-1}$. Supposons que $y = 0$ pour tout $z \in E$. On pose $\lambda_i = x\tau(x)\dots\tau^i(x)$; on a alors :

$$\lambda_0\tau^0(z) + \lambda_1\tau(z) + \dots + \lambda_{n-1}\tau^{n-1}(z) = 0.$$

Par conséquent, les automorphismes distincts τ^i sont linéairement dépendants sur E, ce qui est en contradiction avec le théorème (X.3.1). D'où, il existe z tel que y soit non nul. On a :

$$\begin{aligned}\tau(y) &= \tau(u_0) + \dots + \tau(u_{n-1})\\ &= \frac{1}{x}(u_1 + \dots + u_{n-1}) + \tau^n(z)\\ &= \frac{1}{x}(u_0 + \dots + u_{n-1})\\ &= \frac{y}{x}\end{aligned}$$

d'où $x = \frac{y}{\tau(y)}$. □

Exercice XV.5. Théorème Hilbert 90, version additive.

Soit E/K une extension cyclique finie et soit τ un générateur de son groupe de Galois. Montrer qu'un élément $x \in E$ est tel que $Tr(x) = 0$ si et seulement s'il existe $y \in E$ tel que $x = y - \tau(y)$. (Pour la définition de la trace, *cf.* exercice (XIII.5).) On sait (*loc. cit.*) qu'il existe un élément $z \in E$ tel que $Tr(z) \neq 0$; considérer l'élément

$$y = \frac{1}{Tr(z)}(x\tau(z) + (x + \tau(x))\tau^2(z) + \ldots + (x + \tau(x) + \ldots + \tau^{n-2}(x))\tau^{n-1}(z)).$$

Remarque XV.5.2. Un résultat plus général, souvent appelé aussi théorème « Hilbert 90 », sera donné à la fin de ce chapitre (TR.XV.B).

Théorème XV.5.2. *Soient n un entier positif et K un corps de caractéristique première à n, contenant les racines n-ième de l'unité.*

(i) *Soit E/K une extension cyclique de degré n. Alors il existe $a \in K$ et $\alpha \in E$ racine du polynôme $X^n - a$, tels que $E = K(\alpha)$.*

(ii) *Réciproquement, soient $a \in K$ et α une racine du polynôme $X^n - a$. Alors l'extension $K(\alpha)/K$ est cyclique, de degré d divisant n et $\alpha^d \in K$.*

Démonstration. (i). Soit ζ une racine primitive n-ième de l'unité dans K et τ un générateur de $G = Gal(E/K)$. Puisque $\zeta \in K$, on a $N(\zeta) = \zeta^n = 1$. D'après le théorème Hilbert 90, il existe $\alpha \in E$ tel que $\zeta = \frac{\alpha}{\tau(\alpha)}$. On en déduit que $\tau(\alpha) = \zeta^{-1}\alpha, \ldots, \tau^i(\alpha) = \zeta^{-i}\alpha$, $i = 1, \ldots, n$. Donc les éléments $\zeta^{-i}\alpha$ sont n conjugués distincts de α sur K, d'où $[K(\alpha) : K] \geqslant n$. Mais, $K(\alpha) \subset E$ et $[E : K] = n$, d'où $E = K(\alpha)$. De plus, si on pose $a = \alpha^n$, on a

$$\tau^i(a) = \tau^i(\alpha^n) = \tau^i(\alpha)^n = (\zeta^{-i})^n\alpha^n = \alpha^n = a.$$

Autrement dit, a est laissé fixe par G, d'où $a \in K$, puisque l'extension E/K est galoisienne. Par conséquent, α est bien racine du polynôme $X^n - a$ de $K[X]$.

(ii). Soient $a \in K$ et α une racine du polynôme $X^n - a$. Alors, les $\zeta^i\alpha$, $i = 1, \ldots, n$, sont aussi racines de $X^n - a$ et $K(\alpha)$ est un corps de décomposition sur K de $X^n - a$, dans lequel toutes les racines sont distinctes. Donc l'extension $K(\alpha)/K$ est galoisienne. Soit G son groupe de Galois. Pour tout $\sigma \in G$, $\sigma(\alpha)$ est racine de $X^n - a$, donc $\sigma(\alpha) = \varepsilon_\sigma\alpha$, où ε_σ est une racine de l'unité. L'application $\sigma \mapsto \varepsilon_\sigma$ est un morphisme injectif de groupes de G dans le groupe des racines n-ième de l'unité. Donc G est isomorphe à un sous-groupe d'un groupe cyclique

d'ordre n. Par conséquent G est un groupe cyclique d'ordre d divisant n. Si τ est un générateur de G, alors ε_τ est une racine primitive d-ième de l'unité. D'où

$$\tau(\alpha^d) = \tau(\alpha)^d = (\varepsilon_\tau \alpha)^d = \alpha^d$$

et α^d est laissé fixe par G. Par conséquent $\alpha^d \in K$. □

Dans le théorème précédent, nous avons supposé que la caractéristique de K était première au degré de l'extension E/K. Nous allons maintenant étudier le cas où la caractéristique de K est égale au degré de l'extension.

Théorème XV.5.3. *Soit K un corps de caractéristique $p > 0$.*

(i) *Soit E/K une extension cyclique de degré p. Il existe $\alpha \in E$ tel que $E = K(\alpha)$ et α est racine du polynôme $X^p - X - a$ avec $a \in K$.*

(ii) *Réciproquement, soient $a \in K$ et $f(X) = X^p - X - a$. Alors, ou bien le polynôme $f(X)$ a une racine dans K et alors toutes ses racines sont dans K, ou bien le polynôme $f(X)$ est irréductible sur K et si α est une racine de $f(X)$, $K(\alpha)/K$ est une extension cyclique de degré p.*

Démonstration. (i). Soit E/K une extension cyclique de degré p et soit τ un générateur de son groupe de Galois G. On a $Tr_{E/K}(-1) = p(-1) = 0$, donc, d'après la version additive du théorème « Hilbert 90 », il existe $\alpha \in E$ tel que $\tau(\alpha) - \alpha = 1$, *i.e.* $\tau(\alpha) = \alpha + 1$. On en déduit que pour tout i, $1 \leqslant i \leqslant p$, $\tau^i(\alpha) = \alpha + i$. Donc α a p conjugués distincts, ce qui entraîne $[K(\alpha) : K] \geqslant p$. D'où $E = K(\alpha)$. On a

$$\tau(\alpha^p - \alpha) = \tau(\alpha)^p - \tau(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Autrement dit, $\alpha^p - \alpha$ est invariant par τ, donc par G, *i.e.* $(\alpha^p - \alpha) \in K$. En posant $a = \alpha^p - \alpha$, il est clair que α est racine du polynôme $f(X) = X^p - X - a$.

(ii). Soient $a \in K$ et $f(X) = X^p - X - a$. Si α est une racine de $f(X)$, alors $\alpha + i$, $1 \leqslant i \leqslant p$, sont des racines de $f(X)$, qui a donc p racines distinctes, et si l'une est dans K, elles sont toutes dans K.

Supposons que $f(X)$ n'a aucune racine dans K et supposons que $f(X) = g(X)h(X)$, avec $g(X) \in K[X]$ et $h(X) \in K[X]$, $1 \leqslant d = deg(g) < p$. Puisque $f(X) = \prod_{i=1}^{p}(X - \alpha - i)$, le coefficient de X^{d-1} est la somme de d termes $-(\alpha + i)$. Ce coefficient est égal à $-d\alpha + j$, pour un certain entier j. Comme $d \in K$ est non nul, on a $\alpha \in K$, d'où une contradiction et $f(X)$ est irréductible. Toutes les racines de $f(X)$ sont simples et dans $K(\alpha)$, donc $K(\alpha)/K$ est galoisienne. Puisque $\alpha + 1$ est aussi une racine, il existe un automorphisme τ de $K(\alpha)$ tel que $\tau(\alpha) = \alpha + 1$. On en déduit que, pour $1 \leqslant i \leqslant p$, $\tau^i(\alpha) = \alpha + i$, qui sont distincts, donc le groupe de Galois de $K(\alpha)/K$ est cyclique, engendré par τ. □

This page intentionally left blank

THÈMES DE RÉFLEXION

♣ TR.XV.A. Symboles de Legendre. Loi de réciprocité quadratique

Dans tout ce TR, p désigne un nombre premier impair.

Pour tout $x \in \mathbb{F}_p^*$, on définit le ***symbole de Legendre*** $\left(\frac{x}{p}\right)$ de la manière suivante :

$$\left(\frac{x}{p}\right) = 1 \Longleftrightarrow x \in \mathbb{F}_p^{*2}, \quad \left(\frac{x}{p}\right) = -1 \Longleftrightarrow x \notin \mathbb{F}_p^{*2}.$$

Soit d un entier premier à p. On dit que d est un ***résidu quadratique modulo*** p si $\left(\frac{\overline{d}}{p}\right) = 1$, où $\overline{d}$ est un représentant de la classe de d modulo p, et que d est ***non résidu quadratique modulo*** p si $\left(\frac{\overline{d}}{p}\right) = -1$.

1. *Montrer que pour tout* $x \in \mathbb{F}_p^*$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$.

2. *Montrer que l'application* $\mathbb{F}_p^* \longrightarrow \{1, -1\}$, *définie par* $x \mapsto \left(\frac{x}{p}\right)$, *est un morphisme de groupes.*

Soient K un corps de caractéristique différente de p et ζ une racine primitive p-ième de l'unité (dans une clôture algébrique de K). Pour tout $x \in \mathbb{F}_p^*$, ζ^x est bien défini par $\zeta^x = \zeta^k$, avec $x \equiv k \, mod(p)$. On pose

$$s = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \zeta^x$$

et on appelle cet élément ***somme de Gauss*** sur $\mathbb{F}_p$.

3. *Montrer que* $s^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$.

4. *Soit* q *un nombre premier,* $q \neq 2$, $q \neq p$. *Montrer que* $s^q = \left(\frac{q}{p}\right) s$ *et en déduire que* $s^{q-1} = \left(\frac{q}{p}\right)$.

5. *Soient p et q des nombres premiers impairs distincts. Montrer que*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Cette dernière égalité est la ***loi de réciprocité quadratique de Gauss***.

Elle permet, entre autres, de ramener le calcul du symbole de Legendre à des calculs simples, par réductions successives. Par exemple,

$$\left(\frac{1965}{2311}\right) = \left(\frac{3}{2311}\right)\left(\frac{5}{2311}\right)\left(\frac{131}{2311}\right).$$

Comme $2311 \equiv 1\, mod(3)$, on a $\left(\frac{3}{2311}\right) = \left(\frac{2311}{3}\right)(-1)^{1155\times 1} = -\left(\frac{1}{3}\right) = -1$. On procède de la même manière pour les deux autres termes et on trouve $\left(\frac{1965}{2311}\right) = 1$.

Comme application de ce qui précède, nous allons montrer le résultat suivant : toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique. Plus précisément :

Si $K/\mathbb{Q}$ est une extension de degré 2, il existe une racine de l'unité ζ telle que $K \subset \mathbb{Q}(\zeta)$.

On sait que si $K/\mathbb{Q}$ est une extension de degré 2, il existe un entier d, sans facteur carré, tel que $K = \mathbb{Q}(\sqrt{d})$. Alors d s'écrit $d = 2^e p_1 \dots p_r$, avec $e = 0, 1$ et les p_i sont premiers impairs, d'où

$$K \subset \mathbb{Q}\left(\sqrt{-1}, \sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}\right).$$

6. *Soit ζ_8 une racine primitive 8-ième de l'unité. Montrer que $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$ est contenu dans $\mathbb{Q}(\zeta_8)$.*

7. *Soit p un nombre premier impair et ζ_p une racine primitive p-ième de l'unité. Montrer que $\sqrt{p} \in \mathbb{Q}(\zeta_p)$.* (Utiliser la question 3.)

8. *En déduire que $K \subset \mathbb{Q}(\zeta_m)$, avec $m = 8p_1 \dots p_r$.*

Le résultat démontré ci-dessus est un cas particulier de l'important théorème suivant :

Théorème **(Kronecker-Weber).** *Si $K/\mathbb{Q}$ est une extension abélienne finie, il existe une racine de l'unité ζ telle que $K \subset \mathbb{Q}(\zeta)$.*

♠ TR.XV.B. Interprétation cohomologique du théorème « Hilbert 90 »

Introduisons d'abord quelques définitions très élémentaires de cohomologie des groupes. Soient G un groupe, A un groupe abélien, dont on notera la loi additivement, et $G \times A \longrightarrow A$, $(g, a) \mapsto g.a$ une action de G sur A par automorphismes (*cf.* définition IV.3.1).

On appelle ***1-cocycle*** ou ***morphisme croisé*** une application $f : G \longrightarrow A$ vérifiant $f(gg') = g.f(g') + f(g)$, pour tous g et g' dans G.

1. *Montrer que l'ensemble $Z^1(G, A)$ de tous les 1-cocycles de G dans A est un groupe abélien pour la loi définie par $(f, f') \mapsto f + f'$.*

Un 1-cocycle f est un ***1-cobord*** s'il existe $a \in A$ tel que $f(g) = g.a - a$, pour tout $g \in G$.

2. *Montrer que l'ensemble $B^1(G, A)$ de tous les 1-cobords est un sous-groupe de $Z^1(G, A)$.*

On note $H^1(G, A)$ le groupe quotient $Z^1(G, A)/B^1(G, A)$ et on l'appelle ***groupe de cohomologie*** de G à coefficients dans A. On pose $H^0(G, A) = A^G$ le sous-groupe formé des éléments de A invariants sous l'action de G.

3. *Vérifier que si l'action de G sur A est triviale* (i.e. $g.a = a$ *pour tout* $g \in G$ *et tout* $a \in A$)*, on a $H^0(G, A) = A$ et $H^1(G, A) = Hom(G, A)$.*

On suppose que le groupe G est cyclique d'ordre n, engendré par un générateur τ. On considère les deux endomorphismes de A suivants :

$$N = \sum_{g \in G} g = \sum_{i=0}^{n-1} \tau^i, \quad D = \tau - 1.$$

On a $Ker(N) = \{a \in A | N(a) = 0\}$ et $D(A) = \{\tau.a - a | a \in A\}$.

4. *Montrer que $H^1(G, A) \simeq Ker(N)/D(A)$.*

Nous allons maintenant appliquer ces résultats dans le cadre des extensions galoisiennes.

Soient E un corps et E^* le groupe de ses éléments non nuls ; le groupe E^* est un groupe abélien dont la loi est notée multiplicativement. Soit G un sous-groupe du groupe $Aut(E)$ des automorphismes de corps de E. Alors l'application $G \times E^*$ définie par $(f, x) \mapsto f(x)$, avec $f \in G$ et $x \in E^*$, définit une action du groupe G sur le groupe E^*. On peut donc appliquer les constructions précédentes à cette situation (on prendra soin de passer de la notation additive à la notation multiplicative), et on obtient le groupe $H^1(G, E^*)$.

5. *Soient E/K une extension galoisienne finie et $G = Gal(E/K)$ son groupe de Galois. Soient $f : G \longrightarrow E^*$ un 1-cocycle et c un élément de E : on considère $b = \sum_{g\in G} f(g)(g.c)$. Montrer que l'on peut choisir l'élément c tel que l'élément b soit non nul.* (Utiliser le théorème (X.3.1).)

6. *En déduire que, sous les hypothèses de la question 5, on a $H^1(G, E^*) = 0$.* (On vérifiera que $f(b) = bf(g)^{-1}$, ce qui prouve que f est un 1-cobord.)

Le résultat ci-dessus est aussi souvent appelé théorème « Hilbert 90 ».

7. *En utilisant les résultats des questions 4 et 6, démontrer le théorème (XV.5.1).*

8. *Montrer qu'on a une version additive du théorème (XV.5.1) en remplaçant les conditions $N(x) = 1$ par $Tr_{E/K}(x) = 0$ et $x = \frac{y}{\tau(y)}$ par $x = y - \tau(y)$.*

♠ TR.XV.C. Irréductibilité du polynôme $X^n - a$

Le théorème (XV.5.2) donne une description complète des racines de l'équation $X^n - a = 0$ lorsque le corps de base contient les racines n-ième de l'unité. Nous allons maintenant étudier l'irréductibilité du polynôme $X^n - a$, sans cette dernière hypothèse.

Nous allons établir le théorème suivant :

***Théorème* XV.C.1.** *Soient K un corps, $n \geqslant 2$ un entier, $a \in K$ un élément non nul. On suppose que $a \notin K^p$ pour tout nombre premier p divisant n et que si n est divisible par 4, alors $a \notin -4K^4$. Alors le polynôme $X^n - a$ est irréductible dans $K[X]$.*

Première étape. Nous allons montrer, par récurrence, que l'on peut se ramener au cas où n est une puissance d'un nombre premier.

On pose $n = p^r m$ avec p impair, premier à m. On écrit

$$X^m - a = \prod_{i=1}^{m}(X - a_i)$$

la factorisation de $X^m - a$ en facteurs du premier degré. Dans toute la suite, on pose $\alpha = a_1$. On remplace dans cette expression X par X^{p^r} et on obtient

$$X^n - a = \prod_{i=1}^{m}(X^{p^r} - a_i).$$

On peut, par hypothèse de récurrence, supposer que $X^m - a$ est irréductible dans $K[X]$.

1. *Montrer que α n'est pas une puissance de p dans $K(\alpha)$.* (On suppose que $\alpha = \beta^p$, $\beta \in K(\alpha)$ et, en utilisant la norme $N_{K(\alpha)/K}$, on montre qu'on aboutit à une contradiction.)

On suppose le théorème vrai si n est une puissance de p. Alors $X^{p^r} - a$ est irréductible sur $K(\alpha)$.

2. *Montrer que le polynôme $X^n - a$ est irréductible sur K.* (On note y une racine de $X^{p^r} - \alpha$ et on considère la suite d'extensions $K \subset K(\alpha) \subset K(y)$.)

Deuxième étape. On suppose maintenant que $n = p^r$ et que p est la caractéristique de K.

3. *Soit α une racine p-ième de a. Montrer que α n'est pas une puissance de p dans $K(\alpha)$. En déduire, par récurrence, que $X^{p^r} - a$ est irréductible sur K.*

On suppose que p n'est pas égal à la caractéristique de K et que $r \geqslant 2$. Soit α une racine de $X^p - a$; on a $X^p - a = \prod_{i=1}^{i=p}(X - a_i)$, avec $a_1 = \alpha$ et $(X^{p^r} - a) = \prod_{i=1}^{i=m}(X^{p^{r-1}} - a_i)$.

Supposons que α n'est pas une puissance de p dans $K(\alpha)$. Soit y une racine de $X^{p^{r-1}} - \alpha$.

4. *Montrer que si p est impair, y est de degré p^r sur K et conclure.*

5. *Montrer qu'il en est de même si $p = 2$.* (On suppose que $\alpha = -4\beta^4$, avec $\beta \in K(\alpha)$, d'où $-a = N_{K(\alpha)/K}(\alpha) = 16N_{K(\alpha)/K}(\beta)^4$, d'où une contradiction.)

Supposons que $\alpha = \beta^p$, avec $\beta \in K(\alpha)$. On a

$$-a = (-1)^p N_{K(\alpha)/K}(\alpha) = (-1)^p N_{K(\alpha)/K}(\beta^p) = (-1)^p N_{K(\alpha)/K}(\beta)^p.$$

6. *Montrer qu'alors p ne peut être impair.*

On a donc forcément $p = 2$, d'où $-a = N_{K(\alpha)/K}(\beta)^2$ est un carré dans K.

7. *En déduire que -1 n'est pas un carré dans K.*

On a donc une décomposition sur $K(i)$ $(i^2 = -1)$,

$$X^{2^r} - a = (X^{2^{r-1}} + ib)(X^{2^{r-1}} - ib).$$

8. *En déduire le résultat.* (Si les facteurs $(X^{2^{r-1}} ib)$ sont réductibles, on montre que ib est un carré dans $K(i)$, d'où une contradiction.)

Nous allons maintenant déduire du théorème (XV.C.1) ci-dessus le résultat suivant :

***Théorème* (XV.C.2).** *Soit K un corps tel qu'une clôture algébrique $\overline{K}$ de K soit une extension de K de degré fini strictement supérieur à 1. Alors $\overline{K} = K(i)$ $(i^2 = -1)$, et K est de caractéristique nulle.*

La démonstration proposée (¶) ici utilise les théorèmes fondamentaux de la théorie de Galois et des résultats du TR.XIII.B. Elle n'est qu'esquissée, ce qui rend certaines questions difficiles. Le lecteur intéressé pourra consulter [17] pour une démonstration détaillée.

Supposons que l'extension $\overline{K}/K$ ne soit pas séparable.

9. *Montrer qu'il existe un corps E, $K \subset E \subset \overline{K}$, et un élément $a \in E$, tels que $X^p - a$ soit irréductible sur E.* (D'après le TR.V.B, $\overline{K}$ est une extension radicielle de $\overline{K}_s$.)

10. *En déduire que $\overline{K}$ ne peut être de degré fini sur E, d'où une contradiction.* (Utiliser le théorème (XV.C.1).)

L'extension $\overline{K}/K$ est donc séparable et, puisqu'elle est normale, c'est une extension galoisienne, finie par hypothèse. L'extension $\overline{K}/K(i)$ est aussi galoisienne, on note $G = Gal(\overline{K}/K(i))$.

Nous allons montrer que $|G| = 1$, ce qui prouvera que $\overline{K} = K(i)$. On fait un raisonnement par l'absurde. Supposons qu'il existe un nombre premier p qui divise l'ordre de G. D'après le théorème de Sylow (V.1.1), il existe un sous-groupe H de G d'ordre p. Soit F le corps des invariants de H. On a $[\overline{K} : F] = p$.

11. *On suppose que p n'est pas égal à la caractéristique de K. Montrer que $\overline{K}$ est un corps de décomposition d'un polynôme $X^p - a$.* (Utiliser le théorème (XV.5.2).)

12. *On en déduit que le polynôme $X^{p^2} - a$ est réductible. Montrer que nécessairement $p = 2$ et $a = -4b^4$ avec $b \in F$. En déduire une contradiction.* (Utiliser le théorème (XV.C.1).)

13. (¶¶) *Montrer que si p est la caractéristique de K, on aboutit à une contradiction.*

On a donc prouvé que $\overline{K} = K(i)$, d'où $Gal(\overline{K}/K) \simeq \mathbb{Z}/2\mathbb{Z}$. On notera σ un générateur de ce groupe.

Il reste à prouver que K est de caractéristique nulle. On suppose que K est de caractéristique strictement positive. On note $\mathbb{F}$ le corps premier de K. Soit ζ une racine primitive 2^r-ième de l'unité.

14. *Montrer que $Gal(\overline{K}/K)$ correspond à un sous-groupe de $Gal(\mathbb{F}(\zeta)/\mathbb{F})$.*

15. *Montrer que le sous-corps de $\mathbb{F}$ invariant par σ est égal à $\mathbb{F}$.*

16. *En déduire que $[\mathbb{F}(\zeta) : \mathbb{F}] = 2$. En déduire une contradiction pour r assez grand.*

TRAVAUX PRATIQUES

TP.XV. Racines de l'unité dans un corps fini et codes *BCH*

On se propose, dans ce TP, de passer en revue la théorie des polynômes cyclotomiques sur un corps fini $\mathbb{F}_q$. Comme application, on génère des codes BCH construits, par définition, à partir des polynômes minimaux de puissances d'une racine primitive de l'unité sur $\mathbb{F}_q$. Puis l'on offre une initiation à la théorie des codes correcteurs d'erreurs : on expose comment coder et décoder un message dans le cas des codes BCH (ne pas confondre avec la cryptographie dont le propos est d'envoyer un message secret que seul le destinataire puisse décoder) et l'on teste expérimentalement la capacité de correction du code et la puissance de l'algorithme de décodage (une variante de l'algorithme d'Euclide étendu, due à Berlekamp et Massey). Ces méthodes sont fondamentales dans les technologies de transmission de l'information, d'où de multiples applications dans l'industrie.

Racines de l'unité et polynômes cyclotomiques sur un corps fini $\mathbb{F}_q$

Les polynômes cyclotomiques sont, par définition, les

$$\Phi_n(x) = \prod_{\zeta \in \mathcal{P}_n} (x - \zeta),$$

où $\mathcal{P}_n \subset \mathbb{C}$ désigne l'ensemble des racines primitive n-ièmes de l'unité, constitué des $\zeta_k = e^{\frac{2ik\pi}{n}}$, $\text{pgcd}(k, n) = 1$. Il y en a $\varphi(n)$, où l'on a noté φ la fonction indicatrice d'Euler. La relation

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{XV.1}$$

permet de calculer les Φ_d par récurrence et montre que ces derniers sont à coefficients entiers. On démontre que les Φ_d sont irréductibles dans $\mathbb{Z}[x]$ en réduisant

modulo un nombre premier p (voir le chapitre XV, paragraphe 3 ; le lecteur pourra, à titre d'exercice, démontrer l'irréductibilité sans recourir au groupe de Galois, en adaptant les idées du théorème XV.2.1(ii)).

Plus généralement, puisque Φ_n est à coefficients entiers, on peut évaluer Φ_n, tout comme $x^n - 1$, sur n'importe quel élément d'un anneau A. On peut aussi regarder Φ_n comme un polynôme de $A[x]$, en considérant que ses coefficients $a_i \in \mathbb{Z}$ sont maintenant $a_i.1_A \in A$, ce qui revient, pour $A = \mathbb{Z}/p\mathbb{Z}$, à réduire les coefficients modulo p. Les racines de $x^n - 1$ dans un corps K sont appelées les *racines de l'unité dans* K ; une telle racine est dite *primitive* si $x^n = 1_K$, mais $x^d \neq 1_K$ pour tout diviseur strict de n.

Proposition 1. *Supposons que la caractéristique de K soit première avec n. Alors les racines de l'unité dans K sont des racines simples du polynôme $x^n - 1 \in K[x]$. Plus généralement, les facteurs irréductibles dans la décomposition de $x^n - 1$ en irréductibles dans $K[x]$ sont tous de multiplicité un. Les racines primitives de l'unité dans K sont les racines de Φ_n dans K.*

Démonstration. Le polynôme dérivé de $P = x^n - 1$ est $P' = nx^{n-1}$, qui est non nul car la caractéristique de K ne divise pas n. On en déduit que $\operatorname{pgcd}(P, P') = 1$ (car 0 n'est pas racine de P), donc les racines de P (dans un corps de décomposition) sont simples et les facteurs irréductibles dans la décomposition sur $K[x]$ sont de multiplicité un.

L'égalité (XV.1) dans $\mathbb{Z}[x]$ se transforme en une égalité dans $K[x]$. Comme les racines de l'unité sont des racines simples, chacune est donc racine d'un unique Φ_d, pour d divisant n. Or les racines qui ne sont pas primitives sont les racines de $x^d - 1$, pour d un diviseur strict de n, donc ce sont les racines des Φ_d pour d un diviseur strict de n. Cela démontre que les racines primitives dans K sont les racines de Φ_n dans K. □

Bien que le polynôme Φ_n soit irréductible sur $\mathbb{Q}$, il n'en est pas nécessairement de même lorsqu'on le réduit modulo p. Par exemple, $\Phi_7(x) = x^6 + \ldots + x + 1$ se décompose en $\overline{\Phi}_7(x) = (x^3 + x + \bar{1})(x^3 + x^2 + \bar{1})$ dans $\mathbb{F}_2[x]$.

Nous allons dire ce qu'il advient si l'on regarde Φ_n comme un polynôme $\Phi_{n,q}$ de $\mathbb{F}_q[x]$, où $\mathbb{F}_q$ désigne un corps fini à $q = p^n$ éléments. Comme $K = \mathbb{F}_q$ est de caractéristique p, il contient canoniquement $\mathbb{F}_p = \{m.1_K\}$ et $\Phi_{n,q}$ se déduit de Φ_n en réduisant les coefficients modulo p (et non q !). Parler de la décomposition ou de l'irréductibilité de Φ_n sur $\mathbb{F}_q$ est une commodité de langage : il s'agit bien-entendu de $\Phi_{n,q}$.

Proposition 2. *Soit $\mathbb{F}_q$ un corps fini à q éléments et n un entier premier à q. Notons r l'ordre de la classe de q dans $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ (*i.e. *le plus petit entier tel que $q^r \equiv 1$*

mod n). *Alors les facteurs irréductibles dans la décompositon du polynôme cyclotomique Φ_n sur $\mathbb{F}_q$ sont tous de degré r et de multiplicité un.*

Démonstration. Les facteurs irréductibles étant tous de multiplicité un en vertu de la proposition précédente, il reste à démontrer qu'ils sont de degré r. Soit donc P un tel facteur et s son degré. On considère le corps $K = \mathbb{F}_q[x]/(P)$, de cardinal q^s. Tout élement non nul $\alpha \in K$ vérifie $\alpha^{q^s-1} = 1$. Soit ζ la classe de x dans $\mathbb{F}_q[x]/(P)$: cet élément annule l'image de P, donc l'image de Φ_n dans K. C'est donc une racine primitive n-ième dans K. Puisque $\zeta^{q^s-1} = 1$ et puisque ζ est primitive, n divise $q^s - 1$, *i.e.* $q^s \equiv 1 \mod n$. Cela démontre que s est un multiple de l'ordre r de q dans $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ et, en particulier, $s \geqslant r$.

Démontrons maintenant que $s \leqslant r$. Puisque $\zeta^n = 1$ et puisque n divise $q^r - 1$, on a $\zeta^{q^r-1} = 1$, donc $\zeta^{q^r} = \zeta$. On considère l'ensemble des racines dans K de l'équation $x^{q^r} = x$. C'est un sous-corps de K contenant $\mathbb{F}_q$ et ζ, qui est un élément primitif de l'extension $K/\mathbb{F}_q$. Il s'agit donc de K tout entier. Comme $x^{q^r} - x$ possède au plus q^r racines distinctes, le cardinal q^s de K est plus petit que q^r, d'où $s \leqslant r$. □

Corollaire 1. *Φ_n est irréductible sur $\mathbb{F}_q$ si et seulement si la classe de q est un générateur de $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$.*

Par exemple, les polynômes Φ_3 et Φ_5 sont irréductibles sur $\mathbb{F}_2$.

Corollaire 2. *Le polynôme Φ_{p^r-1} se décompose sur $\mathbb{F}_p$ en un produit de polynômes irréductibles unitaires de degré r, deux à deux distincts. En particulier, il existe des polynômes irréductibles sur $\mathbb{F}_p$ de n'importe quel degré r.*

Les polynômes cyclotomiques peuvent être calculés de façon efficace grâce aux formules ci-dessous :

(i) Si p est un nombre premier ne divisant pas n alors $\Phi_{pn}(x)\Phi_n(x) = \Phi_p(x^p)$ (démontrer que $\mathcal{P}_n^{1/p} = \{x \in \mathbb{C},\ x^p \in \mathcal{P}_n\}$ est l'union disjointe $\mathcal{P}_{pn} \bigsqcup \mathcal{P}_n$).

(ii) Si chaque diviseur premier de k divise n, alors $\Phi_{kn}(x) = \Phi_n(x^k)$.

On en déduit l'algorithme suivant de construction de Φ_n :

– on détermine les diviseurs premiers $p_1, \ldots, p_m$ (distincts) de n ;

– on définit par récurrence $f_i(x) = f_{i-1}(x^{p_i})/f_{i-1}(x)$ à partir de $f_0(x) = x-1$;

– alors $\Phi_n(x) = f_m(x^{\frac{n}{p_1 \cdots p_m}})$.

Puisque l'on dispose d'un algorithme efficace de factorisation sur $\mathbb{F}_p$ (TP.IX.A), le corollaire précédent fournit une méthode de construction des corps finis $\mathbb{F}_{p^r}$, alternative à celle exposée au TP.IX.A où le polynôme irréductible de degré r était obtenu par tirage aléatoire. Cependant, Φ_{p^r-1} est de degré $\varphi(p^r-1)$, qui est exponentiel en r : c'est impratiquable pour r très grand.

1. Écrire une procédure `cyclo:=proc(n)` calculant Φ_n en suivant l'algorithme exposé ci-dessus. Tester avec $n = 3^4 - 1$ et comparer avec le résultat de la commande Maple `numtheory[cyclotomic](3^4-1,x)`.

2. Vérifier que $P = x^4 - x^3 + x^2 - x + 1$ est irréductible sur $\mathbb{F}_3$ à l'aide de la commande `Irreduc(P) mod 3`. Si a désigne une racine de P dans une clôture algébrique $\overline{\mathbb{F}}_3$, le corps $\mathbb{F}_3(a) \simeq \mathbb{F}_3[x]/(P)$ est donc un corps fini à 3^4 éléments. Tester sous Maple :

```
> alias(a=RootOf(P) mod 3):
> Normal(a^9) mod 3;
> Normal(a^(-1))) mod 3;
```

et comparer avec les résultats des calculs menés dans $\mathbb{F}_3[x]/(P)$, où a correspond à la classe de x (commandes `Rem` pour le reste d'une division euclidienne et `Gcdex` pour obtenir l'inverse modulaire, c'est-à-dire les coefficients de Bezout calculés selon l'algorithme d'Euclide étendu).

3. Nous allons maintenant apprendre à décomposer en irréductibles dans $\mathbb{F}_q[x]$. L'algorithme de Berlekamp exposé au sein du TP.IX.A réalise cette tâche (bien que nous ayons supposé $q = p$ pour simplifier ; le lecteur motivé saura adapter les énoncés).

- Vérifier que $P_1 = x^3 + 2x^2 + 2x + 1$ est décomposé sur $\mathbb{F}_3$, à l'aide de la commande `Factor(P) mod 3`.
- Démontrer qu'un corps de rupture de $P_2 = x^3 + 2x^2 - x - 1$ sur $\mathbb{F}_3$ est corps de décomposition. On factorisera P_2 sur $\mathbb{F}_3(a)$, où a est défini par une commande `RootOf`, en invoquant `Factor(P2,a) mod 3`.
- Factoriser $P_3 = x^4 + 2x^3 + 2x^2 + x + 2$ sur $\mathbb{F}_9$. Déterminer un corps de rupture et un corps de décomposition. On utilisera les polynômes cyclotomiques (*cf.* corollaire 2) pour construire les corps finis $\mathbb{F}_{3^r}$.

4. Vérifier que les facteurs irréductibles de Φ_{3^4-1} sur $\mathbb{F}_{3^k}$, $1 \leqslant k \leqslant 4$, sont bien du degré prescrit par la proposition 2, sachant que l'ordre de q dans $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$ s'obtient avec la commande Maple `numtheory[order](q,n)`. Il est clair, au vu

du corollaire 2, que $\mathbb{F}_{3^4}$ est corps de rupture, donc de décomposition (puisque tous les facteurs sont de même degré).

Polynôme générateur d'un code $BCH(q, n, \delta)$

On suppose que n est premier avec q. Sans expliquer la terminologie (pour le moment), un polynôme générateur $g \in \mathbb{F}_q[x]$ d'un code $BCH(q, n, \delta)$ est le ppcm des polynômes minimaux sur $\mathbb{F}_q$ des $\delta - 1$ puissances consécutives $\beta, \ldots, \beta^{\delta-1}$ d'une racine primitive n-ième β dans $\overline{\mathbb{F}}_q$.

C'est un diviseur de $x^n - 1$. En effet, puisque les β^i annulent $x^n - 1$, leurs polynômes minimaux μ_{β^i} divisent tous $x^n - 1$. On peut donc écrire $g = \prod_{j\in\Sigma}(x - \beta^j)$, où Σ est une partie convenable de $\mathbb{Z}/n\mathbb{Z}$. Or g appartient à $\mathbb{F}_q[x]$ si et seulement si $g(x^q) = g(x)^q$, donc si et seulement si Σ est stable par multiplication par q.

Définition 1. Les classes cyclotomiques sont les orbites Σ_i de la multiplication par q dans $\mathbb{Z}/n\mathbb{Z}$, *i.e.* les classes pour la relation d'équivalence

$$i \sim j \Leftrightarrow \exists k \in \mathbb{Z},\ q^k i = j.$$

La classe Σ_i de i est la plus petite partie, stable par q, contenant i, ou encore $\Sigma_i = \{i, qi, \ldots, q^{s-1}i\}$, où s est le plus petit entier positif non nul tel que $q^k i \equiv i \mod n$. Les entiers $k \in \mathbb{Z}$ vérifiant cette congruence forment un sous-groupe de $\mathbb{Z}$ contenant l'ordre r de q dans $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$. On voit donc que s divise r. Enfin, le lecteur justifiera facilement que les différents facteurs irréductibles de $x^n - 1$ sur $\mathbb{F}_q$ corespondent aux $g_{i_k} = \prod_{j\in\Sigma_{i_k}}(x - \beta^j)$, pour les différentes classes cyclotomiques Σ_{i_k}.

Voici comment construire g :

- on calcule Φ_n ;
- puis on factorise Φ_n sur $\mathbb{F}_q$ et l'on choisit une racine β d'un facteur irréductible.
- Soient $\Sigma_{i_1}, \ldots, \Sigma_{i_l}$ les classes cyclotomiques distinctes associées à $1, \ldots, \delta-1$ (on peut même choisir i_k tel que $i_k = \min \Sigma_{i_k}$). On détermine le polynôme minimal g_{i_k} de β^{i_k} à l'aide de la décomposition en facteurs iréductibles sur $\mathbb{F}_q$ de $\Phi_{n/\operatorname{pgcd}(n,i_k)}$ (puisque β^{i_k} est racine primitive sur $\mathbb{F}_q$ d'ordre l'ordre de i_k dans $\mathbb{Z}/n\mathbb{Z}$) : on prend le facteur qui annule β^{i_k}.
- Alors $g = \prod_{k=1}^{l} g_{i_k}$.

5. On reprend l'exemple $n = 3^4 - 1$ de la question précédente et l'on se donne une racine β d'un facteur irréductible de Φ_n. Définir β par une commande `RootOf`, puis calculer `Expand(product(x-beta^(3^j),j=0..3)) mod 3`. Vérifier que l'on obtient bien le polynôme minimal de β.

Écrire une procédure $s := proc(i)$ calculant le cardinal de la classe cyclotomique de i. Calculer $s(1)$ et $s(2)$. En déduire $g_2 = \prod_{j\in\Sigma_2}(x - \beta^j)$, calculé comme un produit. Vérifier que β^2 est racine de Φ_m, pour m l'ordre de 2 dans $\mathbb{Z}/n\mathbb{Z}$. En déduire son polynôme minimal, en testant quel facteur irréductible il annule, et comparer.

6. On se restreint pour simplifier aux codes BCH binaires primitifs : on prend $q = 2$ et $n = 2^m - 1$. La théorie des classes cyclotomiques est alors extrêmement simple : elles sont représentées par les nombres impairs (justifier).

Écrire une procédure `Generateur:=proc(m,delta)` renvoyant g, calculé selon l'algorithme explicité plus haut, et le polynôme minimal de la racine β choisie au cours de la procédure. On prendra soin de ne calculer que les factorisations des Φ_k requises et de ne les calculer qu'une seule fois, afin d'optimiser le temps de calcul. Tester sur des exemples de votre choix.

Codes correcteurs d'erreurs, codage et décodage des codes *BCH*

Le propos de la théorie des codes correcteurs d'erreurs est la détection et la correction d'erreurs lors de la transmission d'un message dans un canal, qui est en général bruité, donc source d'erreurs. En rajoutant une information supplémentaire au message M (opération de codage) avant de le transmettre (on transmet donc le message codé m), on espère pouvoir reconstituer le message d'origine (opération de décodage) à partir du message reçu m'. Si les erreurs ne sont pas trop nombreuses, le message décodé M' est égal à M.

Par exemple, on peut répéter plusieurs fois le message M et décoder en prenant les symboles qui apparaissent majoritairement. Une erreur de transmission se produit avec une probabilité moindre qu'en transmettant simplement le message, cependant le coût de la transmission se trouve accru, puisque la longueur du message augmente. Le but est de construire des codes qui réduisent la probabilité d'erreur, avec un coût raisonnable, et tels que l'on dispose d'algorithmes de codage et surtout de décodage efficaces. Les bases de la théorie des codes ont été établies par Shannon vers 1950. Les applications technologiques sont nombreuses dans les télécommunications (minitel, TV par satellite, etc.). C'est également grâce à ces technologies qu'il est possible de lire un CD avec une bonne qualité d'écoute, même s'il est rayé.

L'algèbre fournit des codes très utiles. Un *code linéaire sur* $\mathbb{F}_q$*, de dimension* k *et longueur* n, est un sous-espace C de dimension k de $\mathbb{F}_q^n$. Le choix d'une base définit une application d'encodage $E : \mathbb{F}_q^k \to \mathbb{F}_q^n$ dont l'image est C.

Afin de transmettre un message, on commence par l'identifier à un élément de $\mathbb{F}_q^k$. Si l'on prend, par exemple, $q = 2$ et $k = 64$, et si l'on désire transmettre un message rédigé en ASCII[(1)], alors chaque lettre ASCII peut être identifiée à un octet et un bloc de 8 lettres à un « mot » de $\mathbb{F}_2^{64}$.

Pour chaque mot $a = (a_1, \ldots, a_{64}) \in \mathbb{F}_q^n$, on note

$$w(a) = \mathrm{Card}(\{i,\ a_i \neq 0\})$$

son *poids de Hamming*. La *distance minimale* du code est, par définition, $d(C) = \min(w(a),\ a \in C \backslash \{0\})$. Comme C est un espace vectoriel, $w(a-b) \geqslant d(C)$ pour deux mots distincts a et b du code. Le lecteur vérifiera facilement que $d(a,b) = w(a-b)$ définit une véritable distance sur les mots de $\mathbb{F}_q^n$, au sens des espaces métriques. Par exemple, le code de répétition pure $C = \{(a,a,a) \in \mathbb{F}_2^{192},\ a \in \mathbb{F}_2^{64}\}$ possède une distance minimale $d(C) = 3$.

Un mot reçu m' est décodé en $c \in C$ tel que $w(c-m')$ soit minimal. Comme les probabilités vont dans ce sens, on parle de décodage selon le principe du maximum de vraisemblance. On voit facilement que le message est décodé correctement si le nombre t d'erreurs commises vérifie $d(c) \geqslant 2t+1$. On dit que le code est t-correcteur, où t désigne la partie entière de $(d(C)-1)/2$: le code peut corriger t erreurs.

Expliquons maintenant le fonctionnement des codes $BCH(q,n,\delta)$, qui constituent une classe populaire de codes introduite par Bose, Ray-Chaudhuri et Hocquenghem.

Définition 2. Soit β une racine primitive n-ième de l'unité dans $\overline{\mathbb{F}}_q$, pour n un entier premier avec q et g le ppcm (unitaire) des polynômes minimaux de $\beta, \ldots, \beta^{\delta-1}$. L'espace vectoriel

$$C = \sum_{0 \leqslant i < n - \deg g} x^i \bar{g} \cdot \mathbb{F}_q \subset \mathbb{F}_q[x]/(x^n-1) = A \simeq \mathbb{F}_q^n,$$

où $\bar{g} \in A$ désigne la classe de g modulo $x^n - 1$, est appelé *code BCH* et noté $BCH(q,n,\delta)$. Il est de longueur n et dimension $k = n - \deg g$. On dit que g est son *polynôme générateur*, car C est l'idéal de A engendré par g.

(1) La norme American Standard Code for Information Interchange est la norme de codage de caractères la plus connue en informatique.

Précisons l'isomorphisme $\mathbb{F}_q^n \simeq A$: on identifiera un mot $a = (a_1, \ldots, a_n)$ du code avec le polynôme $a(x) = \sum_{i=1}^{n} a_i x^{i-1}$ (plus exactement sa classe). Faisant de même avec $\mathbb{F}_q^k$, l'application d'encodage n'est donc rien d'autre que la multiplication par g.

Remarque. Les mots du code $BCH(q, n, \delta)$ sont invariants par permutation circulaire : si $(a_1, \ldots, a_n) \in C$, alors $(a_n, a_1, \ldots, a_{n-1}) \in C$. En effet, cette opération correspond à la multiplication par x dans A. On parle de *code linéaire cyclique*. Ces codes correspondent aux idéaux de A (qui sont tous principaux, mais A n'est pas principal puisqu'il n'est pas intègre).

La définition précédente ne reflète pas le fait qu'un code $BCH(q, n, \delta)$ dépend du choix de β. Cependant, les propriétés du code sont essentiellement indépendantes de β, et en particulier la distance minimale.

Théorème 1. *La distance minimale de $C = BCH(q, n, \delta)$ vérifie $d(C) \geqslant \delta$. On pourra donc corriger au moins $E((\delta - 1)/2)$ erreurs.*

Démonstration. Un élément $a(x)$ appartient au code si et seulement si $a(\beta^i) = 0$ pour $1 \leqslant i < \delta$, ou encore si et seulement si

$$\begin{pmatrix} 1 & \beta & \ldots & \beta^{n-1} \\ 1 & \beta^2 & \ldots & \beta^{2(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{\delta-1} & \ldots & \beta^{(\delta-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = 0.$$

Parce que tous les déterminants de taille $\delta - 1$ extraits de la matrice ci-dessus sont, à une constante non nulle près, des déterminants de Vandermonde dont les coefficients parmi les β^i sont deux à deux distincts, on voit que ce système d'équations n'admet pas de solution $a \neq 0$ tel que $w(a) \leqslant \delta - 1$. Tout élément non nul de C vérifie donc $w(a) \geqslant \delta$. □

On a vu que les racines primitives n-ièmes de l'unité sont les racines dans $\overline{\mathbb{F}}_q$ de Φ_n. L'extension cyclotomique engendrée est de degré $r = m$ lorsque $n = q^m - 1$ et alors, $\mathbb{F}_q(\beta)^* = \{1, \beta, \ldots, \beta^{n-1}\}$. On parle de code *BCH primitif*. Dans le cas général, si l'on pose $m = [\mathbb{F}_q(\beta) : \mathbb{F}_q]$, on sait juste que l'ordre n de β divise le cardinal $q^m - 1$ de $\mathbb{F}_q(\beta)^*$.

7. Écrire deux procédures `Pol:=proc(M,n)` et `Mot:=proc(P,n)` permettant de passer d'un mot $M = (M_1, \ldots, M_n)$ de $\mathbb{F}_q^n$, au polynôme $P = M(x) = \sum_{i=1}^{n} M_i x^{i-1}$ et réciproquement.

Générer un code $BCH(2, 2^5 - 1, 7)$ à l'aide de la procédure `Generateur` déjà écrite. On obtient un polynôme de degré 15 sur $\mathbb{F}_2$.

Enfin, écrire une procédure `Encode:=proc(M,n,g)` renvoyant le message codé $m'(x) = g(x)M(x)$. Tester avec un M généré aléatoirement comme suit :

```
>RandMot:=proc(k) local mot,i;
   mot:=rand(0..1);
   return([seq(mot(),i=1..k)]);
 end:
```

Nous allons maintenant expliquer comment décoder. On suppose que $m = c \in C$ est transmis et que m' est reçu. Le polynôme d'erreur est $e(x) = \sum_{i=1}^{n} e_i x^{i-1}$, correspondant au vecteur d'erreur $e = m' - c$. On suppose qu'au plus $t = E((\delta-1)/2)$ erreurs se sont produites, *i.e.* $w(e) \leqslant t$ et l'on définit :

– l'ensemble $I = \{i,\ e_i \neq 0\}$ des positions des erreurs ;

– le polynôme $u(x) = \prod_{i\in I}(1 - \beta^i x) \in \mathbb{F}_g(\beta)[x]$ appelé *localisateur d'erreur* ;

– le polynôme $v = \sum_{i\in I} e_i\beta^i x \prod_{j\in I\setminus\{i\}}(1-\beta^j x)$ *évaluateur d'erreur.*

Les polynômes u et v vérifient $\deg u \leqslant t$ et $\deg v < t$. Ils déterminent à eux deux l'emplacement et la valeur des erreurs : il suffit d'évaluer en β^{-i} pour obtenir I ; on calcule e_i à l'aide de $u' = \sum_{i\in I} -\beta^i \prod_{j\in I\setminus\{i\}}(1-\beta^j x)$, d'où

$$v(\beta^{-i}) = e_i \prod_{j\in I\setminus\{i\}} (1-\beta^{j-i}) = -e_i\beta^{-i}u'(\beta^{-i})$$

puis $e_i = -v(\beta^{-i})\beta^i/u'(\beta^{-i})$.

Il existe différentes façons de calculer u et v. On peut, par exemple, formuler le problème en termes d'équations linéaires à résoudre. On va donner une autre méthode, plus performante en pratique.

On définit

$$w = \frac{v}{u} = \sum_{i\in I} \frac{e_i\beta^i x}{1-\beta^i x} = \sum_{i\in I}\sum_{j\geqslant 1} e_i(\beta^i x)^j = \sum_{j\geqslant 1} x^k \sum_{i\in I} e_i\beta^{ji} = \sum_{j\geqslant 1} e(\beta^j)x^j.$$

Comme $c(\beta^j) = 0$ pour $1 \leqslant j \leqslant \delta-1$, on a $e(\beta^j) = m'(\beta^j)$ pour $1 \leqslant j \leqslant \delta-1$. On connaît donc w modulo $x^{\delta-1}$: c'est $S(x) = \sum_{j=1}^{\delta-1} = m'(\beta^j)x^j$, appelé parfois *polynôme syndrôme.*

La congruence

$$v(x) \equiv u(x)S(x) \mod x^{2t} \tag{XV.2}$$

(noter que $2t \leqslant \delta - 1$) peut se résoudre en utilisant une variante de l'algorithme d'Euclide étendu, appelé *algorithme de Berlekamp-Massey* : on calcule

trois suites r_j, u_j et v_j telles que $r_j(x)x^{2t} + u_j(x)S(x) = v_j(x)$ pour tout j, à partir de $(r_0, u_0, v_0) = (1, 0, x^{2t})$ et $(r_1, u_1, v_1) = (0, 1, S(x))$, en effectuant les divisions euclidiennes $v_{i-1} = v_i q_i + v_{i+1}$ puis les soustractions $r_{i+1} = r_{i-1} - r_i q_i$ et $u_{i+1} = u_{i-1} - u_i q_i$ jusqu'à obtenir $\deg v_i < t$ et $\deg v_{i-1} \geqslant t$.

Proposition 3. *L'algorithme de Berlekamp-Massey donne (à facteur constant près) le couple $(u(x), v(x))$ recherché, avec $\deg u \leqslant t$ et $\deg v < t$, vérifiant la congruence (XV.2).*

Démonstration. Comme $\deg v_{i+1} < \deg v_i$, la suite $(\deg v_i)$ est strictement décroissante pour $i \geqslant 1$. Il existe donc j tel que $\deg v_j < t$ et $\deg v_{j-1} \geqslant t$. On a également $\deg q_i = \deg v_{i-1} - \deg v_i$ pour $i \geqslant 1$. Regardons la suite $(\deg u_i)$: on a $u_2 = -u_1 q_1$, d'où $\deg u_2 \geqslant \deg u_1$, puis $u_3 = u_1 - u_2 q_2$, d'où $\deg u_3 = \deg u_2 + \deg q_2 > \deg u_2$. On démontre par récurrence que la suite est strictement croissante à partir de $i = 2$: si $\deg u_i > \deg u_{i-1}$, alors $\deg u_{i+1} = \deg u_i + \deg q_i$, donc $\deg u_{i+1} > \deg u_i$. On obtient également, en sommant les égalités $\deg u_{i+1} - \deg u_i = \deg q_i = \deg v_{i-1} - \deg v_i$, pour $i \geqslant 1$:

$$\deg u_j = \deg u_j - \deg u_1 = \deg v_0 - \deg v_{j-1} = 2t - \deg v_{j-1} \leqslant t.$$

Donc (u_j, v_j) répond au problème. De plus, on a pour tout $i \geqslant 1$:

$$\begin{pmatrix} r_i & u_i \\ r_{i+1} & u_{i+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} = \begin{pmatrix} r_{i-1} & u_{i-1} \\ r_i & u_i \end{pmatrix},$$

d'où $r_i u_{i+1} - r_{i+1} u_i = -(r_{i-1} u_i - r_i u_{i-1})$ puis $r_i u_{i+1} - r_{i+1} u_i = (-1)^i$ par récurrence ($i \geqslant 0$). Cela montre que $\operatorname{pgcd}(r_j, u_j) = 1$.

Soit maintenant (u, v) la solution recherchée correspondant à l'erreur de décodage : on écrit $rx^{2t} + uS = v$. Noter que les polynômes localisateur et évaluateur d'erreur sont premiers entre eux par définition, donc $\operatorname{pgcd}(r, u) = 1$. On va prouver que $r_j u = r u_j$, ce qui implique la proportionalité (dans $K[x]$ puis dans K par primalité) des deux couples (r, u) et (r_j, u_j), donc également de (u, v) et (u_j, v_j). Dans le cas contraire où $r_j u - r u_j \neq 0$, les formules de Cramer pour le système

$$\begin{pmatrix} r_j & u_j \\ r & u \end{pmatrix} \begin{pmatrix} x^{2t} \\ S \end{pmatrix} = \begin{pmatrix} v_j \\ v \end{pmatrix}$$

nous donneraient $x^{2t} = \frac{v_j u - v u_j}{r_j u - r u_j}$. Comme

$$\deg(v_j u - v u_j) \leqslant \max(\deg v_j + \deg u, \deg v + \deg u_j) < 2t,$$

cela est impossible. □

On obtient donc u et v en divisant au besoin les polynômes obtenus pr $u(0)$ pour les rendre unitaires.

8. Écrire une procédure `Syndrome:=proc(R,beta,delta)` calculant le polynôme syndrôme $S(x)$ en fonction du message reçu $m' = R$, de β et δ.

Écrire ensuite une procédure `Localisateur:=proc(S,delta)` calculant $u(x)$ à partir de S et δ. On implémentera l'algorithme de Berlekamp-Massey exposé plus haut. Pour soigner l'affichage, utiliser la commande

`collect(Normal(P) mod 2,x)`.

Tester ces procédures sur l'exemple de la question 7, en rajoutant un polynôme d'erreur de votre choix au mot du code généré.

9. Écrire une procédure `Erreur:=proc(u,n,beta)` renvoyant le polynôme d'erreur $e(x)$, dans le cadre des codes BCH binaires, en fonction du polynôme localisateur d'erreur $u(x)$, de n et β (remarquer que la valeur des erreurs est connue !).

Écrire enfin une procédure `Decode:=proc(R,n,g,beta,deta)`, utilisant les trois procédures précédentes et renvoyant le message décodé, c'est-à-dire un élément de $\mathbb{F}_q^k$. Si tout se passe bien, on retrouve M. Tester sur l'exemple en cours de traitement. On pourra utiliser la commande `evalb(M1=M2)` pour vérifier l'égalité de deux mots.

10. On désire maintenant tester le codage/décodage en « vraie grandeur ».

Écrire une procédure `Bruit:=proc(NE,n)` générant un bruit, c'est-à-dire le polynôme d'erreur $e(x)$, sous l'hypothèse $w(e) = NE$ (nombre d'erreurs). On choisira les positions d'erreurs aléatoirement.

Prendre $C = BCH(2, 2^7 - 1, 19)$. Quelle est la dimension k du code ? Calculer le rapport k/n. Combien d'erreurs peut-on corriger ? (Essayer de dépasser le seuil $t = E((\delta - 1)/2)$.)

This page intentionally left blank

XVI

RÉSOLUBILITÉ PAR RADICAUX DES ÉQUATIONS POLYNOMIALES

Dans tout ce chapitre, K sera un corps de caractéristique nulle.

On connaît une formule explicite donnant les racines d'un polynôme du second degré à coefficients réels (par exemple), au moyen d'une racine carrée. On sait qu'il existe des formules analogues pour les polynômes du troisième et du quatrième degré (*cf.* TR.XVI.A). On dit que ces équations polynomiales sont **résolubles par radicaux**.

Le but de ce chapitre est de montrer que ces cas sont les seuls pour lesquels c'est possible. Plus précisément, on montrera que, si $n \geqslant 5$, il ne peut exister une formule générale (*i.e.* valable pour tous les polynômes) exprimant, à l'aide de radicaux (*i.e.* $\sqrt[k]{\ }$), toutes les racines d'un polynôme de degré n en une variable.

De plus, on montrera qu'une équation polynomiale $f(X) = 0$ est résoluble par radicaux si et seulement si le groupe de Galois de f est résoluble.

Pour ce faire, nous allons d'abord formaliser le problème, puis le résoudre à l'aide de la théorie de Galois.

XVI.1. Extensions radicales

Définition XVI.1.1. Une extension E/K est **radicale** si $E = K(\alpha_1, \ldots, \alpha_n)$ et, pour tout i, $i = 1, \ldots, n$, il existe un entier $p(i)$ tel que $\alpha_i^{p(i)} \in K(\alpha_1, \ldots, \alpha_{i-1})$. On dit alors que les α_i forment une **suite de radicaux** de l'extension E/K.

***Remarque* XVI.1.1.**

a) La définition d'une extension radicale donnée ci-dessus n'est valable que dans le cas de la caractéristique nulle. C'est la raison de l'avertissement placé en tête de ce chapitre, certains résultats établis ci-dessous n'étant plus valables en caractéristique strictement positive.

b) Considérons $K \subset L \subset E$: alors, si L/K et E/L sont radicales, il en est de même pour E/K. Mais il se peut que E/K soit radicale et L/K non radicale, comme le montre l'exemple suivant.

Soient $E = \mathbb{Q}(e^{2i\pi/7})$ et $L = \mathbb{Q}(\alpha)$ avec $\alpha = cos(2\pi/7)$. Le polynôme minimal de α sur $K = \mathbb{Q}$ est $M_\alpha(X) = X^3 + X^2/2 - X/2 - 1/8$. Si $L/\mathbb{Q}$ était radicale, alors $L = \mathbb{Q}(\beta)$, où $\beta^3 = b \in \mathbb{Q}$. Or $X^3 - b = (X - \beta)(X - j\beta)(X - j^2\beta)$, donc L contiendrait j, ce qui est en contradiction avec le fait que L est une extension réelle de $\mathbb{Q}$.

On peut remarquer que L est le corps de décomposition du polynôme $P(X) = (X - \alpha)(X - (2\alpha^2 - 1))(X - (-2\alpha^2 - \alpha + 1/2))$. L'extension $L/\mathbb{Q}$ est donc galoisienne, mais non radicale, bien que l'équation $P(X) = 0$ soit résoluble par radicaux.

***Proposition* XVI.1.1.** *Si E/K est une extension radicale et si N/K est une clôture normale de E/K, alors N/K est radicale.*

Démonstration. Soient $E = K(\alpha_1, \ldots, \alpha_n)$ et $M_{\alpha_i}(X)$ les polynômes minimaux des α_i sur K. Alors N est le corps de décomposition du polynôme $f(X) = \prod_i M_{\alpha_i}(X)$ dans une clôture algébrique de E (proposition XIII.2.4). Pour chaque zéro β_{ij} de $f(X)$ dans N, il existe un $K(\alpha_1, \ldots, \alpha_{i-1})$-isomorphisme

$$\sigma_{ij} : K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) \longrightarrow K(\alpha_1, \ldots, \alpha_{i-1}, \beta_{ij}), \quad \sigma_{ij}(\alpha_i) = \beta_{ij}.$$

Puisqu'il existe $p(i)$ tel que $\alpha_i^{p(i)} \in K(\alpha_1, \ldots, \alpha_{i-1})$, il en est de même pour β_{ij} et l'extension N/K est radicale. □

***Remarque* XVI.1.2.** Puisque K est un corps de caractéristique nulle, cette proposition montre qu'une extension radicale de K peut être plongée dans une extension radicale galoisienne.

***Théorème* XVI.1.1.** *Si K est un corps de caractéristique nulle et si E/K est une extension normale et radicale, le groupe de Galois $Gal(E/K)$ est résoluble.*

Démonstration. On remarquera que, puisque K est de caractéristique nulle et que E/K est normale, l'extension E/K est galoisienne finie. Quitte à adjoindre

des éléments supplémentaires α_j, on peut supposer que les entiers $p(i)$ tels que $\alpha_i^{p(i)} \in K(\alpha_1, \ldots, \alpha_{i-1})$ sont premiers.

On fait un raisonnement par récurrence sur n tel que $E = K(\alpha_1, \ldots, \alpha_n)$. Si $n = 1$, c'est évident. On suppose le résultat vrai pour $n-1$. Si $\alpha_1 \in K$, alors $E = K(\alpha_2, \ldots, \alpha_n)$ et le résultat est vérifié par hypothèse de récurrence. On peut donc supposer que $\alpha_1 \notin K$: par hypothèse, il existe un nombre premier p tel que $\alpha_1^p \in K$. Soit $M_{\alpha_1}(X)$ le polynôme minimal de α_1 sur K : d'après les hypothèses, $M_{\alpha_1}(X)$ est scindé dans E et toutes ses racines sont simples. Puisque $\alpha_1 \notin K$, le degré de $M_{\alpha_1}(X)$ est supérieur ou égal à 2. Soit $\beta \neq \alpha_1$ une racine de $M_{\alpha_1}(X)$ dans E : il existe $s \in Gal(E/K)$ tel que $s(\alpha_1) = \beta$, d'où $s(\alpha_1^p) = \beta^p$. Mais $\alpha_1^p \in K$, donc $s(\alpha_1^p) = \alpha_1^p$ et on a $\beta^p = \alpha_1^p$. Par conséquent, en posant $\varepsilon = \alpha_1\beta^{-1}$, on a $\varepsilon \neq 1$ et $\varepsilon^p = 1$. De plus, puisque p est premier, on en déduit que $1, \varepsilon, \ldots, \varepsilon^{p-1}$ sont des racines distinctes p-ième de l'unité dans E. On pose $L = K(\varepsilon)$: on a ainsi la suite d'extensions $K \subset L \subset L(\alpha_1) \subset E$. Puisque E/K est galoisienne finie, il en est de même de E/L. Puisque L contient les racines p-ième de l'unité et que $\alpha_1^p \in L$, $L(\alpha_1)$ est un corps de décomposition du polynôme $X^p - \alpha_1^p$ sur L. Donc l'extension $L(\alpha_1)/L$ est normale et le groupe $Gal(E/L(\alpha_1))$ est un sous-groupe normal du groupe $Gal(E/L)$; on a $Gal(L(\alpha_1)/L) \simeq Gal(E/L)/Gal(E/L(\alpha_1))$. Mais $E = L(\alpha_1)(\alpha_2, \ldots, \alpha_n)$, donc $E/L(\alpha_1)$ est une extension radicale et normale, et $[E : L(\alpha_1)] < n$. Donc, par hypothèse de récurrence, $Gal(E/L(\alpha_1))$ est résoluble. Mais on sait, (proposition XV.2.1), que $Gal(L(\alpha_1)/L)$ est abélien, donc résoluble. On en déduit, (théorème VII.3.1), que $Gal(E/L)$ est résoluble. De la même façon, L étant un corps de décomposition de $X^p - 1$ sur K, l'extension L/K est normale et $Gal(L/K) \simeq Gal(E/K)/Gal(E/L)$. Comme ci-dessus, $Gal(L/K)$ est abélien, (proposition VII.2.2), donc résoluble et, puisque $Gal(E/L)$ est résoluble, on en déduit que $Gal(E/K)$ est résoluble (théorème VII.3.1). □

Théorème XVI.1.2. *Soient K un corps de caractéristique nulle et $K \subset L \subset E$ des extensions. Si l'extension E/K est radicale, le groupe $Gal(L/K)$ est résoluble.*

Démonstration. Soient K_0 le corps des points fixes de L sous $Gal(L/K)$ et N/K_0 une clôture normale de E/K_0. On a alors la suite d'extensions $K \subset K_0 \subset L \subset E \subset N$. Puisque l'extension E/K est radicale, il en est de même pour E/K_0 et donc aussi, d'après la proposition (XVI.1.1), pour N/K_0. On déduit alors du théorème (XVI.1.1) que $Gal(N/K_0)$ est résoluble. D'après le théorème (XIV.1.1), l'extension L/K_0 est normale, d'où $Gal(L/K_0) \simeq Gal(N/K_0)/Gal(N/L)$. On en déduit que le groupe $Gal(L/K_0)$ est résoluble. Mais $Gal(L/K) = Gal(L/K_0)$, donc $Gal(L/K)$ est résoluble. □

XVI.2. Résolubilité des polynômes

Tous les polynômes sont supposés irréductibles.

Définition XVI.2.1.

a) Soient K un corps de caractéristique nulle, $f(X) \in K[X]$ et L un corps de décomposition de $f(X)$ sur K. On dit que l'équation polynomiale $f(X) = 0$ (ou que le polynôme $f(X)$) est **résoluble par radicaux** s'il existe un corps E contenant L tel que l'extension E/K soit radicale.

b) Si $f(X)$ est un polynôme de $K[X]$, on appelle **groupe de Galois de** f, le groupe $Gal(L/K)$, où L est un corps de décomposition de f sur K.

Remarque XVI.2.1.

a) Dans la définition a) ci-dessus, on suppose que le corps K est de caractéristique nulle à cause de la remarque (XVI.1.1.a) et on introduit le corps E car il se peut que l'extension L/K ne soit pas radicale.

b) La partie a) de cette définition exprime que **toutes** les racines de $f(X)$ s'écrivent à l'aide de radicaux. Mais il est vain d'espérer que tout ce qui est exprimable par des radicaux donnés soit dans le corps de décomposition L de f sur K.

c) On sait (théorème XII.1.1.(ii)) que si L et L' sont deux corps de décomposition de f sur K, ils sont K-isomorphes. Par conséquent, les groupes $Gal(L/K)$ et $Gal(L'/K)$ sont isomorphes (mais pas égaux). Le groupe de Galois de f est donc défini à isomorphisme près.

Exercice XVI.1. Soient K un corps et $f(X) \in K[X]$ un polynôme irréductible. Montrer que si une racine de $f(X)$ s'exprime par radicaux, il en est de même pour toutes ses racines. L'équation $f(X) = 0$ est alors résoluble par radicaux.

On obtient immédiatement, à partir du théorème XVI.1.2, le théorème suivant.

Théorème XVI.2.1. *Soit $f(X)$ un polynôme à coefficients dans un corps K de caractéristique nulle. Si $f(X)$ est résoluble par radicaux, son groupe de Galois $Gal(f)$ est résoluble.* □

Par conséquent, pour prouver que les polynômes de degré supérieur ou égal à 5 ne sont pas résolubles par radicaux, il suffit, pour chaque $n \geqslant 5$, d'exhiber ***un*** polynôme de degré n dont le groupe de Galois ne soit pas résoluble.

Nous allons d'abord traiter le cas où n est un nombre premier et fournir un exemple explicite pour $n = 5$, puis nous traiterons le cas général.

Proposition XVI.2.1. *Soient p un nombre premier et $f(X) \in \mathbb{Q}[X]$ un polynôme irréductible de degré p. Si le polynôme $f(X)$ a exactement deux racines complexes non réelles, le groupe de Galois de $f(X)$ est isomorphe au groupe des permutations S_p.*

Démonstration. Dans le corps $\mathbb{C}$, le polynôme $f(X)$ est scindé et toutes ses racines sont simples. Le groupe de Galois $Gal(f)$ est donc un sous-groupe de S_p. Si on note $E \subset \mathbb{C}$ un corps de décomposition de $f(X)$ sur $\mathbb{Q}$, $[E : \mathbb{Q}]$ est divisible par p. Par conséquent, p divise l'ordre de $Gal(f)$ et, puisque p est premier, d'après le premier théorème de Sylow, le groupe $Gal(f)$ possède un élément d'ordre p. Les seuls éléments d'ordre p de S_p sont les p-cycles. Donc $Gal(f)$ contient un p-cycle. D'autre part, la conjugaison complexe dans $\mathbb{C}$ induit un $\mathbb{Q}$-automorphisme de E qui laisse fixes les $p-2$ racines réelles et échange les deux racines complexes. Donc $Gal(f)$ contient un 2-cycle. On peut supposer, sans restreindre la généralité, que $Gal(f)$ contient le 2-cycle $(1, 2)$ et le p-cycle $(1, 2, \ldots, p)$ (quitte à renuméroter les racines et remplacer le p-cycle par l'une de ses puissances). On sait que ces deux éléments engendrent S_p (TR.I.A). D'où $Gal(f) = S_p$. □

On sait (corollaire VII.4.1), que pour $n \geqslant 5$ le groupe S_n n'est pas résoluble. Il suffit donc de donner un exemple d'un polynôme $f(X) \in \mathbb{Q}[X]$ vérifiant les hypothèses de la proposition (XVI.2.1), avec $p = 5$.

Corollaire XVI.2.1. *Le polynôme $X^5 - 6X + 3 \in \mathbb{Q}[X]$ n'est pas résoluble par radicaux.*

Démonstration. D'après le critère d'Eisenstein, $f(X)$ est irréductible sur $\mathbb{Q}$. Il suffit donc de montrer que $f(X)$ a exactement trois racines réelles. Une étude élémentaire du graphe de la fonction de $\mathbb{R}$ dans $\mathbb{R}$, $x \mapsto f(x)$ donne le résultat (on utilise le théorème des valeurs intermédiaires pour séparer les racines de $f(X)$ par $\sqrt[4]{6/5}$ qui sont les racines de $f'(X)$). □

Nous allons maintenant compléter ces résultats en montrant que, pour tout entier $n > 0$, il existe un polynôme dont le groupe de Galois est isomorphe à S_n, ce qui prouvera le résultat annoncé dans l'introduction de ce chapitre pour les polynômes de degré supérieur ou égal à 5.

Théorème XVI.2.2. *Soient k un corps (sans hypothèse de caractéristique), $t_1, \ldots, t_n$ des éléments transcendants et algébriquement indépendants sur k. Le groupe de Galois sur k du polynôme*

$$f(X) = X^n - t_1 X^{n-1} + \ldots + (-1)^i t_i X^{n-i} + \ldots + (-1)^n t_n$$

est isomorphe au groupe S_n.

Démonstration. Soient $r_1, \dots, r_n$ les racines de f dans un corps de décompositon $L = k(t_1, \dots, t_n)(r_1, \dots, r_n)$. On a $f(X) = \prod_{i=1}^n (X - r_i)$ et les t_k s'expriment en fonction des r_i à l'aide des fonctions symétriques élémentaires : $t_k = \sigma_k(r_1, \dots, r_n)$, où $\sigma_k(x_1, \dots, x_n) = \sum_{i_1 < \dots < i_k} \prod_{j=1}^n (x_{i_j})$. On a donc $L = k(r_1, \dots, r_n)$. Montrons que les r_i sont transcendants et algébriquement indépendants sur k (donc, en particulier, distincts) : quitte à renuméroter les racines, on peut supposer que $r_1, \dots, r_s$ ($s \leqslant n$) sont transcendants et algébriquement indépendants sur k et que l'extension $L/k(r_1, \dots, r_s)$ est finie. Il s'agit de montrer que $s = n$. Comme t_1 est algébrique sur $k(r_1, \dots, r_s)$ (car $L/k(r_1, \dots, r_s)$ est finie), il existe une équation polynomiale $Q(t_1, r_1, \dots, r_s) = 0$. Comme t_1 est transcendant sur k, cette équation doit faire intervenir l'un des r_i et, quitte à permuter $r_1, \dots, r_s$, on peut supposer qu'elle fait intervenir r_1. Donc r_1 est algébrique sur $k(t_1, r_2, \dots, r_s)$, de sorte que l'extension $L/k(t_1, r_2, \dots, r_s)$ est finie. On fait de même avec $r_2, \dots, r_s$, montrant ainsi que l'extension $L/k(t_1, \dots, t_s)$ est finie. Nécessairement $s = n$, sinon t_{s+1} serait algébrique sur $k(t_1, \dots, t_s)$, ce qui n'est pas puisqu'il est transcendant sur $k(t_1, \dots, t_s)$.

Considérons maintenant la restriction des $k(t_1, \dots, t_n)$-automorphismes de L à l'ensemble $\{r_1, \dots, r_n\}$ des racines : on a déjà vu qu'une telle application définit une injection du groupe $Gal(f)$ dans S_n. C'est un isomorphisme. En effet, un élément $\tilde{\sigma}$ de S_n provient du $k(t_1, \dots, t_n)$-automorphisme σ défini par $\sigma(r_i) = r_{\tilde{\sigma}(i)}$: ce dernier associe à une fraction rationnelle $\frac{P(r_1,\dots,r_n)}{Q(r_1,\dots,r_n)}$ la fraction $\frac{P(\sigma(r_1),\dots,\sigma(r_n))}{Q(\sigma(r_1),\dots,\sigma(r_n))}$. C'est bien un $k(t_1, \dots, t_n)$-automorphisme : comme les t_k sont symétriques en les r_i, ils sont invariants sous l'action de σ, donc une fraction rationnelle en les t_k est laissée fixe par σ. □

Corollaire XVI.2.2. *L'équation générale polynomiale sur $\mathbb{Q}$ de degré n est résoluble par radicaux si et seulement si $n \leqslant 4$.* □

Exercice XVI.2. Déduire du théorème (XVI.2.2) et de l'application démontrée au TR.II.B, que pour tout $n \geqslant 2$, il existe une extension $F/\mathbb{Q}$ de degré n qui ne contient pas de corps intermédiaire distinct de $\mathbb{Q}$ ou de F. (Indication : d'après le théorème (XVI.2.2), il existe un polynôme $f \in \mathbb{Q}[X]$ dont le corps de décomposition L vérifie $Gal(L/\mathbb{Q}) \simeq S_n$. Considérer $F = L^{S_{n-1}}$.)

Ceci est un exemple de la situation évoquée dans la mise en garde qui suit la remarque (IX.2.1).

Signalons que Hilbert a démontré le résultat suivant.

Proposition XVI.2.2. *Pour tout entier $n \geqslant 2$, il existe un corps de nombres* (i.e. *une extension finie de $\mathbb{Q}$*) ***dont le groupe de Galois est isomorphe à S_n.***

On notera que cet énoncé est équivalent à : *il existe un polynôme irréductible de $\mathbb{Q}[X]$, de degré n, dont le groupe de Galois est S_n.*

La preuve est basée sur le théorème suivant.

Théorème XVI.2.3. *Soient $P \in \mathbb{Z}[X]$ un polynôme unitaire à racines simples (dans $\mathbb{C}$) et p un nombre premier tels que la réduction $\overline{P}$ de P modulo p soit également à racines simples (dans $\overline{\mathbb{F}}_p$), alors $Gal(\overline{P})$ est isomorphe à un sous-groupe de $Gal(P)$.*

Démonstration. Soit $K = \mathbb{Q}(x_i)$ le corps de décomposition du polynôme P (dans $\mathbb{C}$), où x_i sont les racines, et soit $A = \mathbb{Z}[x_i]$. Alors A est un anneau dont le corps des fractions est K et A est, comme groupe abélien, libre de type fini de rang $n = [K : \mathbb{Q}]$. En effet, l'ensemble $\{\prod x_i^{n_i}\}_{n_i \leqslant n}$ engendre A (on utilise le fait que P est unitaire) et A est sans torsion. Une base de A, comme groupe abélien libre, est une base de K comme $\mathbb{Q}$-espace vectoriel, d'où le résultat sur le rang.

On vérifie facilement que l'application de restriction à A définit un isomorphisme entre $Gal(K/\mathbb{Q})$ et le groupe $Aut(A)$ des automorphismes de l'anneau A.

D'autre part, soit K_p le corps de décomposition de $\overline{P}$ (dans $\overline{\mathbb{F}}_p$). Soit $\mathfrak{m}$ un idéal maximal de A contenant p et soit $\phi : A \to A/\mathfrak{m}$ le morphisme de passage au quotient. Alors $\phi(\mathbb{Z})$ s'identifie à $\mathbb{Z}/p\mathbb{Z}$ (car $\phi(p) = 0$) et les $\phi(x_i)$ engendrent $A/\mathfrak{m}$ sur $\mathbb{F}_p$. Or $\phi(P) = \overline{P} = \prod(x - \phi(x_i))$, donc $A/\mathfrak{m}$ s'identifie à K_p. Ainsi ϕ définit un morphisme d'anneaux $A \to K_p$.

Notons $Hom(A, K_p)$ l'ensemble des morphismes d'anneaux de A dans K_p et démontrons que $Hom(A, K_p) = \{\phi \circ \sigma, \sigma \in Aut(A)\}$. Ces éléments sont deux à deux distincts car les $\phi(x_i)$ le sont (les racines de $\overline{P}$ sont supposées simples). D'autre part, un élément de $Hom(A, K_p)$ se prolonge de façon unique en un élément de $Hom(K, K_p)$ (propriété universelle du corps des fractions) et ces éléments sont linéairement indépendants sur K_p. Donc la dimension du K_p-espace vectoriel $Hom_{groupe}(A, K_p)$ ($Hom(A, K_p)$ n'est pas un espace vectoriel car les morphismes d'anneaux ne sont pas stables par multiplication par un scalaire) est supérieure ou égale au cardinal de $Hom(A, K_p)$. Or A est un groupe abélien libre de rang $[K : \mathbb{Q}]$; un morphisme de groupes $A \to K_p$ est déterminé par l'image d'une base de A, donc le rang sur K_p est au plus $[K : \mathbb{Q}]$. Cela montre que $Hom(A, K_p)$ est au plus de cardinal $[K : \mathbb{Q}]$, autrement dit que tous les éléments sont là.

Démontrons enfin le théorème : soit $\overline{\sigma} \in Gal(\overline{P})$. On a vu qu'il existe un unique $\sigma \in Aut(A)$ tel que $\overline{\sigma} \circ \phi = \phi \circ \sigma$. Alors $\Psi : \overline{\sigma} \mapsto \sigma$ est un morphisme injectif de groupes :

$$\overline{\sigma_1} \circ \overline{\sigma_2} \circ \phi = \overline{\sigma_1} \circ \phi \circ \Psi(\overline{\sigma_2}) = \phi \circ \Psi(\overline{\sigma_1}) \circ \Psi(\overline{\sigma_2}),$$

d'où $\Psi(\overline{\sigma_1} \circ \overline{\sigma_2}) = \Psi(\overline{\sigma_1}) \circ \Psi(\overline{\sigma_2})$ par unicité. L'injectivité provient du fait que si $\overline{\sigma} \circ \phi = \phi$, alors $\overline{\sigma}$ laisse fixes tous les $\phi(x_i)$, donc $\overline{\sigma}$ est l'identité. □

Démonstration de la proposition (XVI.2.2). On prend $p \geqslant n$ premier et on choisit trois polynômes irréductibles unitaires P_2, P_3 et P_5 dans $\mathbb{Z}[x]$, de degré n, tels que leurs réductions modulo 2, 3 et 5 se décomposent en irréductibles sur les corps finis respectifs comme suit : $\overline{P}_2$ est irréductible sur $\overline{\mathbb{F}}_2$, $\overline{P}_3 = xQ$ et $\overline{P}_5 = RS$ avec R de degré 2.

Soit alors $P = -15P_2 + 10P_3 + 6P_5$. On a $P \equiv P_i \bmod i$, pour $i = 2, 3, 5$. Comme P est irréductible sur $\mathbb{Q}$, car sa réduction modulo 2 l'est sur $\overline{F}_2$, il est à racines simples dans $\mathbb{C}$. D'après le théorème (XVI.2.3), on sait que $Gal(P)$ contient un $n-1$-cycle (à cause du facteur Q) et le produit d'une transposition et d'un $n-2$-cycle (facteurs R et S), donc une transposition (prendre une puissance convenable de ce produit). On en déduit que $Gal(P)$ est isomorphe à S_n, car un sous-groupe transitif de S_n qui contient une transposition et un $n-1$-cycle est S_n tout entier. □

En utilisant le théorème de Cayley, on obtient comme corollaire de ce qui précède que tout groupe fini G est groupe de Galois d'une extension de corps de nombres. Par contre, on ne sait pas si ce résultat est vrai pour une extension $K/\mathbb{Q}$ seulement, en dehors des cas où G est de l'un des types suivants : les groupes abéliens, S_n, A_n, les groupes résolubles (démonstration très difficile) et certains groupes $PSL_2(\mathbb{F}_p)$. Le « problème de Galois inverse », comme on l'appelle (*i.e.* étant donné un groupe fini G, est-il le groupe de Galois d'une extension finie ?) est un problème difficile.

Ce qui précède montre que, pour tout $n \geqslant 5$, il existe au moins un polynôme de degré n non résoluble par radicaux, d'où l'impossibilité d'une résolution générale par radicaux des équations polynomiales de degré supérieur ou égal à 5. Cependant, cela ne signifie pas que tous les polynômes de degré n ne soient pas résolubles par radicaux. On est donc amené à se poser la question suivante : peut-on caractériser les polynômes résolubles par radicaux ?

XVI.3. Caractérisation des polynômes résolubles

Théorème XVI.3.1. *Soient K un corps de caractéristique nulle et L/K une extension finie normale dont le groupe de Galois est résoluble. Alors, il existe une extension E/L telle que E/K soit radicale.*

Démonstration. Soit $G = Gal(L/K)$: on fait un raisonnement par récurrence sur l'ordre de G. Si $|G| = 1$, c'est évident. Supposons que $|G| \neq 1$ et le théorème vrai pour tout groupe d'ordre strictement inférieur à celui de G. Puisque G est fini, il possède un sous-groupe normal maximal H. Le groupe quotient G/H est simple et résoluble, il est donc cyclique d'ordre premier p (proposition VII.4.1).

Soit N un corps de décomposition de $X^p - 1$ sur L. Puisque l'extension L/K est finie, on a $L = K(\alpha_1, \ldots, \alpha_n)$; puisqu'elle est normale, L est un corps de décomposition sur K du polynôme $f(X) = \prod_i M_{\alpha_i}(X)$. Par conséquent, N est un corps de décomposition sur K du polynôme $(X^p - 1)f(X)$ et l'extension N/K est normale. On a donc la situation $K \subset L \subset N$ avec L/K et N/K galoisiennes finies. On sait alors que $Gal(L/K) \simeq Gal(N/K)/Gal(N/L)$ (théorème XIV.3.2). Or, d'après la proposition (XV.2.1), $Gal(N/L)$ est abélien, donc résoluble. On déduit du théorème (VII.3.1) que $Gal(N/K)$ est résoluble.

Soit M le sous-corps de N engendré par K et les racines de $X^p - 1$. Alors l'extension M/K est radicale. Pour prouver le théorème, il suffit donc de montrer qu'il existe une extension E de N telle que E/M soit radicale ; on aura ainsi une extension E de L telle que E/K soit radicale.

Montrons que le groupe $Gal(N/M)$ est isomorphe à un sous-groupe de G. À $\sigma \in Gal(N/M)$ on associe $\sigma_{|L}$ sa restriction à L. C'est un K-homomorphisme et, puisque L/K est normale, $\sigma_{|L} \in G$. On a donc un morphisme de groupes $\varphi : Gal(N/M) \longrightarrow G$ défini par $\varphi(\sigma) = \sigma_{|L}$. Si $\varphi(\sigma) = id_{|L}$, σ est un automorphisme de N qui laisse invariants les éléments de L et M. Or, ces éléments engendrent N, d'où $\varphi(\sigma) = id_{|L}$ implique $\sigma = id_{|N}$ et φ est injective. Ce qui prouve que $Gal(N/M)$ est isomorphe à un sous-groupe J de G.

Si J est un sous-groupe propre de G, par hypothèse de récurrence, il existe une extension E de N telle que E/M soit radicale, d'où le résultat.

Supposons que $J = G$; en posant $I = \varphi^{-1}(H)$, I est un sous-groupe normal de $Gal(N/M)$ qui est d'indice p. Soit R le corps des invariants de N sous l'action de I. L'extension N/R est normale et son groupe de Galois est d'ordre inférieur à celui de G, donc, par hypothèse de récurrence, il existe une extension E de N telle que E/R soit radicale. Mais d'après les théorèmes fondamentaux de la théorie de Galois, on a $[R : M] = p$ premier et l'extension R/M est galoisienne. Puisque M contient les racines p-ième de l'unité, on sait (théorème XV.5.2), que $R = M(\alpha)$, avec $\alpha^p \in M$. On en déduit que l'extension E/M est radicale. D'où le théorème. □

Les théorèmes XVI.2.1 et XVI.3.1 montrent que si K est un corps de caractéristique nulle, un polynôme $f(X)$ de $K[X]$ est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.

Exercice XVI.3.

a) Montrer que le groupe de Galois de tout polynôme à coefficients dans un corps fini est résoluble.

b) Montrer le polynôme $X^2 + X + 1$ sur $\mathbb{F}_2$ n'est pas résoluble par radicaux.

Cet exercice est un contre-exemple au résultat du théorème (XVI.2.1) dans le cas de la caractéristique non nulle.

This page intentionally left blank

THÈMES DE RÉFLEXION

♣ TR.XVI. Résolution des équations polynomiales de degrés 3 et 4

Comme nous allons le rappeler ci-dessous, toute équation polynomiale de degré 3 ou 4, à coefficients dans un corps de caractéristique nulle, est résoluble par radicaux. L'objectif de ce TR est de donner, dans ce cas, des formules explicites pour la résolution de ces équations.

La résolution par radicaux des équations polynomiales de degré 1 est évidente.

1. *Montrer que les formules de résolution des équations polynomiales de degré 2, à coefficients dans $\mathbb{R}$, sont encore valables pour des équations polynomiales, de degré 2, à coefficients dans un corps quelconque de caractéristique nulle.*

Les groupes S_3 et S_4 étant résolubles, le polynôme donné au théorème (XVI.2.2), pour $n = 3$ ou $n = 4$ est résoluble par radicaux.

2. *En déduire que toute équation polynomiale de degré 3 ou 4, à coefficients dans un corps quelconque de caractéristique nulle, est résoluble par radicaux.* (Procéder par substitution.)

A - Résolution des équations polynomiales de degré 3 – Méthode de Cardan

D'après la question 2, il suffit d'avoir un procédé de résolution pour l'équation $f(X) = X^3 - t_1X^2 + t_2X - t_3 = 0$, où t_1, t_2, t_3 sont des éléments d'une extension de K, algébriquement libres sur K.

L'étude ci-dessous utilise les notions de résultant et de discriminant développées dans le TR.VIII.C.

3. *Montrer que le polynôme $f(X)$ peut s'écrire $Y^3 + pY + q$, dont les racines y_1, y_2, y_3 vérifient $y_1 + y_2 + y_3 = 0$, $y_1y_2 + y_2y_3 + y_3y_1 = p$, $y_1y_2y_3 = -q$.* (Faire la transformation $Y = X - \frac{1}{3}t_1$.)

4. *Montrer que le groupe de Galois de Y^3+pY+q sur $K(p,q)$ est isomorphe à S_3.*

On sait que le groupe S_3 possède la suite de composition $\{id\} \lhd A_3 \lhd S_3$.

5. *Montrer que le corps $Inv(A_3)$ des invariants de A_3 est $K(p,q)(\sqrt{D})$, où D est le discriminant de Y^3+pY+q.*

On pose $j = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, et

$$\begin{cases} u = y_1 + jy_2 + j^2y_3 \\ v = y_1 + j^2y_2 + jy_3. \end{cases}$$

On en déduit

$$\begin{cases} y_1 = \frac{1}{3}(u+v) \\ y_2 = \frac{1}{3}(j^2u+jv) \\ y_3 = \frac{1}{3}(ju+j^2v). \end{cases}$$

6. *Montrer que u^3+v^3 et u^3v^3 appartiennent à $K(p,q)$.*

7. *Montrer que u^3 et v^3 sont racines du polynôme $T^2+27qT-27p^3$.*

Ce polynôme est appelé la ***résolvante*** de Y^3+pY+q.

8. *Montrer que $u = \sqrt[3]{\frac{1}{2}(-27q+3\sqrt{-3}\sqrt{D})}$ et $v = \sqrt[3]{\frac{1}{2}(-27q-3\sqrt{-3}\sqrt{D})}$, avec $D=-4p^3-27q^2$.*

Les formules donnant u, v, et y_1, y_2, y_3 en fonction de u et v, sont appelées les ***formules de Cardan***.

Soient $f(X) = X^3+pX+q \in K[X]$, où K est un sous-corps de $\mathbb{R}$, et $D=-4p^3-27q^2$ son discriminant.

9. *Montrer que :*

- *Si $D<0$, $f(X)$ a une unique racine réelle.*
- *Si $D=0$, $f(X)$ a trois racines réelles dont au moins deux sont confondues.*
- *Si $D>0$, $f(X)$ a trois racines réelles distinctes.*

On suppose que $D>0$ et que le groupe le Galois, $Gal(f)$ est isomorphe à A_3.

10. *On note L un corps de décomposition de $f(X)$ sur K. Montrer qu'il n'existe aucun sous-corps de $\mathbb{R}$ qui contienne L et qui soit une extension de K par radicaux.*

Ce résultat signifie que, sous les hypothèses faites, les racines de $f(X)$ sont réelles, mais que les expressions de ces racines données par les formules de Cardan font intervenir un nombre non réel, à savoir j. Autrement dit, il n'existe pas de formules purement réelles donnant les racines réelles de l'équation $f(X)=0$.

B - Résolution des équations polynomiales de degré 4 – Méthode de Ferrari

D'après la question 2, il suffit d'avoir un procédé de résolution pour l'équation $f(X) = X^4 - t_1X^3 + t_2X^2 - t_3X + t_4 = 0$, où t_1, t_2, t_3, t_4 sont des éléments d'une extension de K, algébriquement libres sur K.

11. *Montrer que le polynôme $f(X)$ peut s'écrire Y^4+pY^2+qY+r, dont les racines y_1, y_2, y_3, y_4 vérifient $y_1+y_2+y_3+y_4 = 0$, $y_1y_2+y_2y_3+y_3y_4+y_4y_1+y_1y_3+y_3y_2 = p$, $y_1y_2y_3 + y_2y_3y_4 + y_3y_4y_1 + y_4y_1y_2 = -q$, $y_1y_2y_3y_4 = r$.* (Faire la transformation $Y = X - \frac{1}{4}t_1$.)

12. *Montrer que le groupe de Galois de $Y^4 + pY^2 + qY + r$ sur $K(p, q, r)$ est isomorphe à S_4.*

On sait que le groupe S_4 possède la suite de composition $\{id\} \triangleleft V \triangleleft A_4 \triangleleft S_4$.

On pose

$$\begin{cases} z_1 = y_1y_2 + y_3y_4 \\ z_2 = y_1y_3 + y_2y_4 \\ z_3 = y_1y_4 + y_2y_3. \end{cases}$$

13. *En déduire que l'on a*

$$\begin{cases} 2y_1 = \sqrt{z_1 - p} + \sqrt{z_2 - p} + \sqrt{z_3 - p} \\ 2y_2 = \sqrt{z_1 - p} - \sqrt{z_2 - p} - \sqrt{z_3 - p} \\ 2y_3 = -\sqrt{z_1 - p} + \sqrt{z_2 - p} - \sqrt{z_3 - p} \\ 2y_4 = -\sqrt{z_1 - p} + \sqrt{z_2 - p} + \sqrt{z_3 - p} \end{cases}$$

où les racines carrées sont prises de telle sorte que $\sqrt{z_1 - p}\sqrt{z_2 - p}\sqrt{z_3 - p} = -q$.

Ces expressions s'appellent les ***formules de Ferrari***.

14. *Montrer que les polynômes symétriques élémentaires en z_1, z_2, z_3 appartiennent à $K(p, q, r)$.* (On montrera que z_1, z_2, z_3 sont globalement invariants sous l'action de S_4.)

15. *Vérifier que*

$$\begin{cases} z_1 + z_2 + z_3 = p \\ z_1z_2 + z_1z_3 + z_2z_3 = -4r \\ z_1z_2z_3 = q^2 - 4pr. \end{cases}$$

16. *En déduire que z_1, z_2, z_3 sont racines du polynôme*

$$Z^3 - pZ^2 - 4rZ + 4pr - q^2.$$

Ce polynôme s'appelle la ***résolvante cubique*** de $Y^4 + pY^2 + qY + r$.

On sait résoudre la résolvante cubique par la méthode de Cardan, d'où les racines de l'équation $Y^4 + pY^2 + qY + r = 0$ par les formules de Ferrari.

This page intentionally left blank

TRAVAUX PRATIQUES

TP.XVI. Théorie de Galois constructive

Le but de ce TP est d'aborder des aspects effectifs de la théorie de Galois des corps de nombres tout en manipulant et en illustrant la théorie. En effet, puisque MAPLE parvient à calculer les groupes de Galois des polynômes $P \in \mathbb{Z}[x]$ de petits degrés, quels sont les algorithmes que cache la commande `galois` ?

Nous allons voir que les ingrédients sont de deux types : d'une part, on réduit P modulo différents nombres premiers p et l'on exploite l'information dont on dispose sur $Gal(\overline{P})$. MAPLE prédit alors de quel groupe il s'agit : il utilise pour cela un théorème remarquable de Chebotarev qui constitue une méthode « probabiliste » de calcul du groupe de Galois. D'autre part, on calcule des « résolvantes », ces dernières remontant aux travaux de Lagrange (voir également le TR.XVI.A). Nous formaliserons la théorie générale des résolvantes, ce qui nous amènera entre autres, lors de l'implémentation, à écrire un programme exprimant un polynôme en n indéterminées invariant sous l'action de S_n comme polynôme en les fonctions symétriques élémentaires.

Pour finir, mentionnons que nos calculs fournissent des réponses partielles au problème de galois inverse, c'est-à-dire celui de savoir si tout groupe fini est (isomorphe au) groupe de Galois d'un polynôme à coefficients rationnels. En se restreignant aux polynômes irréductibles, cela revient à se demander si tout sous-groupe transitif (voir ci-dessous) du groupe symétrique S_n est groupe de Galois d'un polynôme de degré n. C'est vrai jusqu'à $n = 7$ d'après nos calculs. À la connaissance des auteurs, la réponse est encore positive jusqu'à $n = 18$, la vérification nécessitant l'élaboration d'algorithmes plus sophistiqués que les nôtres. Nous nous heurtons en effet très tôt aux limitations liées à la puissance de calcul des machines, ce qui nous oblige déjà à recourir, par exemple pour le calcul des résolvantes, à des méthodes numériques d'approximation des racines complexes de P.

Remarques préliminaires

Soit P un polynôme de degré n de $\mathbb{Q}[x]$ dont on désire calculer le groupe de Galois $Gal(P) = Gal(K/\mathbb{Q})$, où $K \subset \mathbb{C}$ désigne le corps de décomposition de P. On peut supposer, quitte à remplacer P par son quotient par $\text{pgcd}(P, P')$, ce qui ne change pas le corps de décomposition K, que toutes les racines sont simples. Ensuite, en multipliant P par un entier suffisamment grand, on peut supposer que P appartient à $\mathbb{Z}[x]$. Enfin, on se ramène au cas d'un polynôme unitaire comme suit : si $P = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$, on pose $\widetilde{P} = x^n + \sum_{k=0}^{n-1} a_k a_n^{n-k-1} x^k$. Comme $\widetilde{P}(a_n x) = a_n^{n-1} P(x)$, les deux polynômes ont bien même groupe de Galois, et $\widetilde{P}$ est unitaire à coefficients entiers.

Dans ce qui suit, nous supposerons que P est irréductible. Si l'on dispose d'un algorithme efficace décomposant P en produit de facteurs irréductibles (voir TP IX.A), il n'est par contre pas toujours facile d'exprimer le groupe $Gal(P)$ en fonction du groupe de Galois des facteurs irréductibles. Par exemple, Maple renvoie un message d'erreur lorsque P n'est pas irréductible. De plus, si l'on désire calculer le groupe de Galois des corps de nombres, c'est-à-dire des extensions finies de $\mathbb{Q}$, alors il est inutile de traiter le cas des polynômes réductibles, puisque tout corps de nombres est corps de décomposition sur $\mathbb{Q}$ d'un polynôme irréductible.

Le groupe de Galois $Gal(P)$ agit naturellement sur l'ensemble $\{\alpha_1, \ldots, \alpha_n\}$ des racines, qui sont permutées, et l'action est fidèle. Se donner une telle numérotation, arbitraire, des racines identifie donc $Gal(P)$ à un sous-groupe de S_n. Changer l'ordre de numérotation transforme $Gal(P)$ en un conjugué sous S_n ; ainsi, lorsqu'il s'agit d'identifier le groupe de Galois, les objets naturels à considérer sont les sous-groupes de S_n à conjugaison près.

De plus, on a supposé P irréductible : l'action de $Gal(P)$ sur les racines est alors transitive. En effet, comme α_i et α_j ont même polynôme minimal P, ils sont conjugués sur $\mathbb{Q}$: il existe d'après la proposition XIII.1.1 un $\mathbb{Q}$-automorphisme de $\mathbb{C}$ tel que $\sigma(\alpha_i) = \alpha_j$. Notant $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subset \mathbb{C}$ le corps de décomposition de P, l'extension $K/\mathbb{Q}$ est normale, donc $\sigma(K) = K$ (proposition XIII.2.1) et σ induit par restriction à K un élément du groupe de Galois. Il s'agit donc de regarder les sous-groupes transitifs de S_n. C'est une question non triviale de théorie des groupes qui a été résolue au moins jusqu'à $n = 32$. La classification des sous-groupes transitifs de S_n à conjugaison près a été donnée au TP.IV.B jusqu'au rang $n = 7$. Par exemple, pour les degrés 4 et 5, ce sont :

```
C4:=permgroup(4,{[[1,2,3,4]]}):
S4:=permgroup(4,{[[1,2,3,4]],[[1,2]]}):
D4:=permgroup(4,{[[1,2,3,4]],[[1,3]]}):
V4:=permgroup(4,{[[1,2],[3,4]],[[1,3],[2,4]]}):
```

```
A4:=permgroup(4,{[[1,2,3]],[[1,2],[3,4]]}):
C5:=permgroup(5,{[[1,2,3,4,5]]}):
S5:=permgroup(5,{[[1,2,3,4,5]],[[1,2]]}):
D5:=permgroup(5,{[[1,2,3,4,5]],[[2,5],[3,4]]}):
A5:=permgroup(5,{[[1,2,3,4,5]],[[1,2,3]]}):
M20:=permgroup(5,{[[1,2,3,4,5]],[[2,3,5,4]]}):
```

On reconnaît des groupes cycliques, diédraux, des groupes symétriques et alternés, enfin le groupe métacyclique M_{20} d'ordre 20. Ils sont définis ci-dessus par un système de générateurs en notation Maple. Prendre soin de charger la librairie `group` ; le cardinal et la liste des éléments s'obtiennent alors en appliquant les commandes `grouporder` et `elements` respectivement.

La commande `galois`

Le but de cette première partie est d'observer les résultats de la commande `galois` sur des polynômes de petits degrés (jusqu'à $n = 7$). Mais nos exemples ne sont pas issus du hasard : la liste ci-dessous, tirée de [9], fournit un exemple pour chaque groupe transitif de la classification à conjugaison près que nous avons mentionnée. Autrement dit, la réponse au problème de Galois inverse est positive jusqu'au rang 7.

- degrés 1 à 3 : $P_1 = x$, $P_2 = x^2 + x + 1$, $P_3 = x^3 + x^2 - 2x - 1$, $P_4 = x^3 + 2$;
- degré 4 : $P_5 = x^4+x^3+x^2+x+1$, $P_6 = x^4+1$, $P_7 = x^4-2$, $P_8 = x^4+8x+12$, $P_9 = x^4 + x + 1$;
- degré 5 : $P_{10} = x^5+x^4-4x^3-3x^2+3x+1$, $P_{11} = x^5-5x+12$, $P_{12} = x^5+2$, $P_{13} = x^5 + 20x + 16$, $P_{14} = x^5 - x + 1$;
- degré 6 : $P_{15} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $P_{16} = x^6 + 108$, $P_{17} = x^6 + 2$, $P_{18} = x^6 - 3x^2 - 1$, $P_{19} = x^6 + 3x^3 + 3$, $P_{20} = x^6 - 3x^2 + 1$, $P_{21} = x^6-4x^2-1$, $P_{22} = x^6-3x^5+6x^4-7x^3+2x^2+x-4$, $P_{23} = x^6+2x^3-2$, $P_{24} = x^6 + 6x^4 + 2x^3 + 9x^2 + 6x - 4$, $P_{25} = x^6 + 2x^2 + 2$, $P_{26} = x^6 - 2x^5 - 5x^2 - 2x - 1$, $P_{27} = x^6 + 2x^4 + 2x^3 + x^2 + 2x + 2$, $P_{28} = x^6 - x^5 - 10x^4 + 30x^3 - 31x^2 + 7x + 9$, $P_{29} = x^6 + 24x - 20$, $P_{30} = x^6 + x + 1$;
- degré 7 : $P_{31} = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$, $P_{32} = x^7+7x^3+7x^2+7x-1$, $P_{33} = x^7-14x^5+56x^3-56x+22$, $P_{34} = x^7+2$, $P_{35} = x^7 - 7x^3 + 14x^2 - 7x + 1$, $P_{36} = x^7 + 7x^4 + 14x + 3$, $P_{37} = x^7 + x + 1$.

1. Calculer les groupes de Galois des polynômes de la liste jusqu'au degré 5 inclus, puis de quelques exemples de votre choix parmi ceux du degré 6 et 7. Observer le résultat affiché, comme sur l'exemple ci-dessous :

```
> galois(x^5-5*x+12);
```

"5T2", {"5 :2", "D(5)"}, "+", 10, {"(1 2 3 4 5)", "(1 4)(2 3)"}

Il s'agit du groupe diédral D_5 (nommé également 5T2 dans la nomenclature utilisée par Maple), de cardinal 10 et engendré par le 5-cycle (1 2 3 4 5) et l'élément (1 4)(2 3) d'ordre 2 (pour le choix de numérotation fait par Maple). Le signe + signifie que le discriminant $\Delta(P) = (-1)^{\frac{n(n-1)}{2}} Res(P, P') = d^2$, où $d = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)$ (voir TR.XVI.A) est un carré (ou encore que $d \in \mathbb{Z}$). On verra plus loin, comme cas particulier de la théorie des résolvantes, que c'est équivalent au fait que $Gal(P)$ est un sous-groupe de A_n. Noter que ce résultat a déjà été vu pour le degré 3 (*cf.* exercice XIV.1).

Vérifier que tous les dix groupes transitifs de degrés 4 et 5 rappelés dans les préliminaires apparaissent bien, à conjugaison près.

2. Les théorèmes XVI.2.1 et XVI.3.1 montrent que l'équation $P(x) = 0$ est résoluble par radicaux si et seulement si $G = Gal(P)$ est résoluble. La proposition XII.3.1 fournit alors un critère algorithmiquement vérifiable : il suffit de regarder si la suite décroissante des groupes dérivés $G_n = D_n(G) = [G_{n-1}, G_{n-1}]$ se termine par $\{e\}$ (groupe trivial réduit à l'identité). La commande Maple correspondante est `DerivedS`.

Parmi les groupes transitifs de degrés 4 et 5, lesquels sont résolubles ? Tester les commandes `DerivedS(G)` et `solve(P)` pour $P = x^5 - x + 1$ et $P = x^5 + 2$.

3. On va maintenant ouvrir la boîte noire et demander à Maple d'afficher les différentes étapes du calcul. Pour cela, taper :

```
> restart; infolevel[galois]:=2;
```

Puis traiter le cas du degré 4 ainsi que les polynômes $x^5 + 2$ et $x^6 + 12$. Par exemple :

```
> galois(x^4+x^3+x^2+x+1;

galois: Computing the Galois group of    x^4+x^3+x^2+x+1
galois/absres: 125 = 125, (nonsquare)
```

```
galois/absres: Possible groups:   {"4T1", "4T3", "4T5"}
galois/absres: p = 2   gives shape   4
galois/absres: p = 3   gives shape   4
galois/absres: p = 7   gives shape   4
galois/absres: p = 11   gives shape   1, 1, 1, 1
galois/absres: p = 13   gives shape   4
galois/absres: p = 17   gives shape   4
galois/absres: p = 19   gives shape   2, 2
galois/absres: p = 23   gives shape   4
galois/absres: The Galois group is probably one of   {"4T1"}
galois/respol: Using the orbit-length partition of 2-sequences.
galois/respol: Calculating a resolvent polynomial...
galois/respol: Factoring the resolvent polynomial...
galois/respol: Orbit-length partition is   4, 4, 4
galois/respol: Removing   {"4T3", "4T5"}
galois/respol: Possible groups left:   {"4T1"}
```

“4T1”, {“C(4)”}, “-”, 4, {“(1 2 3 4)”}.

Tout d'abord, Maple calcule le discriminant (le vérifier avec la commande `discrim(P,x)`) et dire si c'est un carré. Il y a ensuite deux types d'arguments :

– Le recours à la réduction modulo différents nombres premiers p, par exemple :

  ```
  galois/absres:   p = 19   gives shape   2, 2
  ```

  Ce sont les méthodes modulaires.

– Le recours à la théorie des résolvantes, par exemple :

  ```
  galois/respol: Using the orbit-length partition of 2-sequences.
  galois/respol: Calculating a resolvent polynomial...
  galois/respol: Factoring the resolvent polynomial...
  galois/respol: Orbit-length partition is   4, 4, 4
  ```

  ou bien :

  ```
  galois/special5: Calculating a S5/F20 resolvent...
  galois/special5: Factoring this S5/F20 resolvent...
  ```

Y a-t-il des cas où Maple peut conclure sans calculer de résolvante ? Sauriez-vous calculer au papier-crayon par vos propres méthodes le groupe de Galois ?

Par exemple, le cas de x^4-2 a été traité au chapitre XIV. Noter également que $Gal(x^6+12)$ a déjà été calculé au cours du TP.XIV, sachant que ce polynôme est normal.

Pour la suite du TP, revenir à l'affichage standard en tapant :

```
infolevel[galois]:=0
```

Les méthodes modulaires

4. Nous avons besoin d'un préliminaire de théorie des groupes. On rappelle que le type d'une permutation est la liste ordonnée des longueurs des cycles qui figurent dans sa décomposition canonique (voir TP.II). Il s'agit de donner la liste des différents types apparaissant dans chacun des groupes de permutations G considérés (notamment les dix groupes correspondant aux degrés 4 et 5), ainsi que la proportion d'éléments de chaque type.

Commencer par écrire une procédure `listetypes:=proc(n)` renvoyant les différents types possibles dans S_n (Indication : On pourra écrire une procédure récursive, puisqu'un type $[i_1,\dots,i_r]$ (avec $\sum_j i_j = n$) est tel que $[i_2,\dots,i_r]$ est un type de S_{n-i_1}).

☞ *Pour soigner l'affichage et trier la liste de listes, on peut procéder comme suit* : On définit un ordre *via* la procédure

```
>ordre:=proc(a,b) local i;
   for i from 1 to min(nops(a),nops(b))
     do if a[i]<>b[i] then return(evalb(a[i]<b[i])); fi;
     od;
   if nops(a)<=nops(b) then return(true) else return(false); fi;
 end:
```

puis `sort([[1,3],[1,1,1,1],[1,1,2]],ordre)` trie la liste selon l'ordre prescrit.

Écrire ensuite une procédure `typesG:=proc(G)` renvoyant, pour $G \subset S_n$, un groupe de permutations défini par une commande `permgroup`, une liste $[[t_1,q_1],\dots,[t_r,q_r]]$, où les t_i sont les différents types de S_n et q_i la proportion d'éléments de type t_i (ainsi $\sum_i q_i = 1$). On utilisera la procédure `type` écrite au cours du TP.II. Appliquer enfin `typesG` à chacun des dix groupes.

Les méthodes modulaires sont basées sur le théorème XVI.2.3 que nous rappelons ci-dessous :

Théorème 1. *Soient $P \in \mathbb{Z}[x]$ un polynôme unitaire à racines simples (dans $\mathbb{C}$) et p un nombre premier tels que la réduction $\overline{P}$ de P modulo p soit également à racines simples (dans $\overline{\mathbb{F}}_p$), alors $Gal(\overline{P})$ est isomorphe à un sous-groupe de $Gal(P)$.*

De plus, notant α_i les n racines simples de P et reprenant les notations de la preuve de ce théorème, l'application $Gal(\overline{P}) \hookrightarrow Gal(P)$ associe à $\bar{\sigma}$ un élément σ tel que $\bar{\sigma} \circ \phi = \phi \circ \sigma$, où $\phi : A = \mathbb{Z}[\alpha_i, 1 \leqslant i \leqslant n] \to K_p = \mathbb{F}_p(\phi(\alpha_i), 1 \leqslant i \leqslant n)$ et $\overline{P} = \prod_{i=1}^{n}(x - \phi(\alpha_i))$. Avec ce choix de numérotation des racines de $\overline{P}$ (induite *via* ϕ par la numérotation choisie pour P), il est clair que $\bar{\sigma}$ et σ ont même type. En fait, cela ne dépend pas de la numérotation, car un autre choix revient à conjuguer la permutation, or le type est invariant par conjugaison.

Par ailleurs, on démontre (*cf.* exercice XV.4) :

Proposition 1. *Soit $\overline{P} \in \mathbb{F}_p[x]$ un polynôme de degré n et $\overline{P} = \overline{P}_1 \dots \overline{P}_r$ sa décomposition en irréductibles, chaque facteur étant supposé de multiplicité un. Notant $n_i = \deg \overline{P}_i$ (ordonnés par ordre croissant, quitte à changer l'ordre des facteurs), alors $Gal(\overline{P})$ est engendré par un élément de type $[n_1, \dots, n_r]$.*

En définitive, en choisissant des p convenables, on démontre l'existence dans $Gal(P)$ d'éléments de certains types, et l'on compare les types obtenus à ceux apparaissant dans la liste des groupes transitifs à conjugaison près. Comme on va le voir sur des exemples, cela permet de conclure dans certains cas. Notamment, on s'intéresse au cas des degrés 4 et 5 que nous détaillons ci-dessous.

– En degré 4, les sous-groupes transitifs (à conjugaison près) sont C_4, D_4, S_4, $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et A_4. On a le diagramme d'inclusions :

$$\begin{array}{ccccc} C_4 & \subset & D_4 & \subset & S_4 \\ & & \cup & & \cup \\ & & V_4 & \subset & A_4 \end{array}$$

Avec les choix faits (*cf.* définition de ces groupes dans les remarques préliminaires), ce sont de véritables inclusions, mais puisque nous regardons les groupes à conjugaison près, une inclusion $G_1 \subset G_2$ signifiera plutôt que G_1 est contenu dans un conjugué de G_2 (sous S_4). La liste des types sont :

$$\begin{array}{ll} C_4 & : [1,1,1,1], [2,2], [4] \\ D_4 & : [1,1,1,1], [1,1,2], [2,2], [4] \\ S_4 & : [1,1,1,1], [1,1,2], [1,3], [2,2], [4] \\ A_4 & : [1,1,1,1], [1,3], [2,2] \\ V_4 & : [1,1,1,1], [2,2]. \end{array}$$

– En degré 5, les sous-groupes transitifs (à conjugaison près) sont C_5, D_5, A_5, S_5 et le groupe métacyclique M_{20}. On a le diagramme d'inclusions :

$$\begin{array}{ccccc} & & M_{20} & \subset & S_5 \\ & & \cup & & \cup \\ C_5 & \subset & D_5 & \subset & A_5 \end{array}$$

et la liste des types :

$$\begin{array}{ll} C_5 & : [1,1,1,1,1],[5] \\ D_5 & : [1,1,1,1,1],[1,2,2],[5] \\ A_5 & : [1,1,1,1,1],[1,1,3],[1,2,2],[5] \\ M_{20} & : [1,1,1,1,1],[1,2,2],[1,4],[5] \\ S_5 & : [1,1,1,1,1],[1,1,1,2],[1,1,3],[1,2,2],[1,4],[2,3],[5]. \end{array}$$

5. On va appliquer deux tests : le premier permettant de vérifier si $Gal(P)$ est inclus dans A_n et l'autre donnant une liste de types présents dans $Gal(P)$. Il s'agira alors de conclure quant aux différents groupes possibles pour $Gal(P)$.

Écrire une procédure `testAn:=proc(P)` renvoyant $+$ ou $-$ selon que $Gal(P)$ est un sous-groupe de A_n ou non. On utilisera le critère du déterminant, admis pour l'instant, et on pourra tester si un complexe z donné est un entier par la commande Maple `type(z,integer)`.

Écrire également une procédure `typeMod:=proc(P,N)` donnant la liste des types obtenus par la méthode modulaire décrite précédemment, en prenant les nombres premiers p jusqu'à N. Pour cela, on obtiendra les facteurs de $\overline{P}$ par la commande `Factors(P) mod p` et on notera que la condition sur les racines de $\overline{P}$ dans la proposition 1 ci-dessus est équivalente à dire que p ne divise pas le discriminant de P (*cf.* TP.IX.B).

Enfin, appliquer ces deux procédures aux dix polynômes de degrés 4 et 5 de la liste figurant dans la première partie du TP. On donnera, pour chaque cas, les différents groupes possibles et remarquera que les cas où ces deux tests permettent de déterminer le groupe de Galois correspondent aux cas, relevés en degré 4 dans la première partie, où Maple conclut sans calculer de résolvante. Précisément, c'est le cas lorsque le groupe de Galois est A_n ou S_n, tous les types finissant par apparaître en prenant des premiers suffisamment grands.

Il est suprenant de constater que Maple « devine » pourtant la réponse, au vu des types obtenus modulo différents premiers p, et que cette réponse s'avère correcte par la suite :

```
galois/absres:   The Galois group is probably one of   {"4T1"}
[...]
galois/respol:   Possible groups left:   {"4T1"}
```

Quel heuristique ou théorème se cache derrière ce scénario ? Nous allons maintenant y répondre.

Soit $\mathcal{P}(P,N)$ l'ensemble des nombres premiers $p \leqslant N$ qui ne divisent pas le discriminant de P. Pour $p \in \mathcal{P}(P,N)$, on note $t_p(P) = [n_1, \ldots, n_r]$ la partition de n obtenue en décomposant $\overline{P}$ en irréductibles sur $\mathbb{F}_p$. Soit alors

$$\mu_N(t,P) = \frac{\text{Card}\{p \in \mathcal{P}(P,N) \text{ tel que } t_p(P) = t\}}{\text{Card}\,\mathcal{P}(P,N)}$$

et $\mu(t,P)$ la proportion d'éléments de $Gal(P)$ qui sont de type t.

***Théorème 2* (Chebotarev).** *Quand N tend vers l'infini, la proportion $\mu_N(t,P)$ tend vers la proportion $\mu(t,P)$.*

Le lecteur particulièrement motivé pourra consulter [18] pour une preuve de ce théorème remarquable mais difficile. Il s'agit d'une méthode probabiliste de calcul du groupe de Galois, cependant les calculs menés jusqu'à un nombre fini N ne peuvent servir de preuve du fait que le résultat attendu est le bon.

6. Écrire une procédure `typeMod2:=proc(P,N)` renvoyant la liste $[[t_1, \mu_N(t_1,P)], \ldots, [t_r, \mu_N(t_r,P)]]$, où les t_i sont les différents types de S_n. Comme le fait Maple, en prenant $N = 31$, deviner le résultat pour les dix polynômes habituels (degrés 4 et 5).

7. Si d désigne le cardinal de $G = Gal(P)$ et d_t le nombre d'éléments de G de type t, alors $d\mu_N(t,P)$ tend vers l'entier d_t. La partie entière $E(d\mu_N(t,P))$ (commande `round` en Maple) de $d\mu_N(t,P)$ est donc constante à partir d'un rang N assez grand, de valeur d_t. Modifier `typeMod2` en une procédure `typeMod3` renvoyant la liste $[[t_1, \mu'_N(t_1,P)], \ldots, [t_r, \mu'_N(t_r,P)]]$, où $\mu'_N(t,P) = E(d\mu_N(t,P))/d$. Vérifier sur les exemples habituels que les résultats obtenus coïncident avec ceux de la question 4. Cela constitue une vérification expérimentale du théorème de Chebotarev.

La théorie des résolvantes

Soit $\mathbb{Q}(\underline{x}) = \mathbb{Q}(x_1, \ldots, x_n)$ le corps des fractions rationnelles en $x_1, \ldots, x_n$. Le groupe symétrique S_n agit sur $\mathbb{Q}(\underline{x})$ par permutation des x_i : on a donc $\sigma(f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ pour toute fraction rationnelle f et toute

permutation σ. D'après la proposition VIII.11.2, le sous-corps des invariants sous S_n est le corps des fractions rationnelles $\mathbb{Q}(\underline{s}) = \mathbb{Q}(s_1, \ldots, s_n)$ en les fonctions symétriques élémentaires s_i en les x_j, qui peuvent être définies par l'égalité

$$(x - x_1) \ldots (x - x_n) = x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n.$$

Le groupe de Galois de l'extension $\mathbb{Q}(\underline{x})/\mathbb{Q}(\underline{s})$ est donc S_n (théorème XIV.1.2).

Soit maintenant H un sous-groupe de S_n. Il lui correspond un sous-corps $\mathbb{Q}(\underline{x})^H$ contenant $\mathbb{Q}(\underline{s})$. L'extension $\mathbb{Q}(\underline{x})^H/\mathbb{Q}(\underline{s})$ est de degré fini et admet donc un élément primitif F.

Définition 1. Avec les notations précédentes, on appelle *résolvante générale de H relative à F* le polynôme minimal de F sur $\mathbb{Q}(\underline{s})$. C'est un polynôme de $\mathbb{Q}(\underline{s})[x]$ de degré $[S_n : H]$ qui vaut

$$Resolv_{F,H} = \prod_{\sigma \in S_n/H} (x - \sigma(F)).$$

Il s'agit en fait d'une définition-proposition. Noter que le polynôme $Resolv_{F,H}$ ci-dessus est bien défini car F est invariant sous H, donc $\sigma(F)$ a bien un sens : il ne dépend que de la classe σ dans S_n/H. Comme l'action de S_n par translation à gauche sur S_n/H permute les différentes classes, on voit que $Resolv_{F,H}$ est stable sous S_n : c'est donc un élément de $\mathbb{Q}(\underline{s})[x]$. Il est de degré $[S_n : H]$, qui est le degré de l'extension $\mathbb{Q}(\underline{x})^H/\mathbb{Q}(\underline{s})$ puisque $\mathbb{Q}(\underline{x})/\mathbb{Q}(\underline{x})^H$ est de degré $|H|$.

☞ *Quelques remarques concernant la manipulation des polynômes à plusieurs indéterminées sous* Maple : Définissant

```
P:=x[2]*x[3]^2+x[3]*x[1]+x[3]^2*x[1]+x[1]*x[4]
```

par exemple, la commande `sort(P,[seq(x[i],i=1..4)],tdeg)` permet de trier les monômes selon le degré total suivi de l'ordre « lexicographique » sur les monômes de même degré. Le degré total en les x_i s'obtient par `degree(P,{seq(x[i],i=1..n)})`. On effectue les substitutions $x_1 \leftarrow x_2$, $x_2 \leftarrow x_3, x_3 \leftarrow x_1$, par exemple, par la commande `subs` comme suit : `subs({x[1]=x[2],x[2]=x[3],x[3]=x[1]},P)`. Pour tester l'égalité de deux polynômes, il est nécessaire de les mettre au préalable sous une forme permettant la comparaison : par exemple `sort(expand(P),[seq(x[i],i=1..4)],tdeg)` (on développe puis on ordonne).

8. Écrire une procédure `action_poly:=proc(P,n,g)` renvoyant $g(P)$, où $P \in \mathbb{Q}[\underline{x}]$ et $g \in S_n$ (on pourra utiliser la procédure `image` du TP.IV.B).

Écrire ensuite une procédure `sym:=proc(G,P)`, utilisant `action_poly` et renvoyant

$$sym_G(P) = \sum_{g \in G} g(P),$$

pour G un groupe de permutations défini par une commande `permgroup`. On prendra soin d'afficher les résultats dans l'ordre croissant des monômes.

Par définition, $sym_G(P)$ est invariant sous G. On veut savoir s'il y a d'autres permutations laissant fixe P. Pour cela, écrire une procédure `invariant?:=proc(P,n,g)` testant si P est laissé fixe par $g \in S_n$, puis une procédure `invariantG?:=proc(P,G)` testant si P est invariant sous G (on notera qu'il suffit de vérifier que P est laissé fixe par les générateurs de G). Enfin, écrire une procédure `stab:=proc(P,n)` calculant le stabilisateur $Stab_{S_n}(P)$ de P, c'est-à-dire renvoyant l'ensemble des éléments de S_n laissant fixe P. Tester sur des exemples de votre choix.

9. On transforme un polynôme f en les s_i en un polynôme en les x_i comme suit : écrivant la procédure

```
>sym_elem:=proc(n)  local P,S,i;
   if n=1 then return({s[1]=x[1]});
     else P:=collect(expand(mul(x+x[i],i=1..n)),x);
     return({seq(s[i]=coeff(P,x,n-i),i=1..n)});
   fi;
 end:
```

la conversion s'effectue *via* la commande `subs(sym_elem(n),f)`. On désire maintenant écrire une procédure `convert_sym:=proc(P,n)` effectuant la transformation inverse, c'est-à-dire exprimant un polynôme symétrique P en les x_i comme un polynôme en les s_i. Le faire en remarquant que la preuve de la proposition VIII.11.2 est de nature algorithmique. Il suffit donc de l'implémenter : la procédure `convert_sym` sera de nature récursive (attention, il est nécessaire d'utiliser la conversion dans l'autre sens explicitée plus haut dans l'un des deux appels récursifs). On pourra utiliser la commande `normal(P,mul(x[i],i=1..n))` pour effectuer la division de P par $\prod_{i=1}^{n} x_i$.

10. On désire vérifier sur différents exemples que $F = sym_H(\prod_{i=1}^{n-1} x_i^{n-i})$ est un élément primitif de $\mathbb{Q}(\underline{x})^H/\mathbb{Q}(\underline{s})$. Pour cela, il suffit de vérifier que $Stab_{S_n}(F) = H$. En effet, on a alors $\mathbb{Q}(F) = \mathbb{Q}(\underline{x})^{Inv(\mathbb{Q}(F))} = \mathbb{Q}(\underline{x})^H$. Le faire pour $H = D_4$ et C_4 puis le démontrer au papier-crayon pour tout H.

Soit $d_n = \prod_{1\leqslant i<j\leqslant n}(x_i - x_j)$. Vérifier jusqu'à $n = 6$ que $Inv(d_n) = A_n$ et le démontrer pour tout n au papier-crayon. Ainsi d_n est un élément primitif de $\mathbb{Q}(\underline{x})^{A_n}$.

11. Écrire une procédure `resolvante:=proc(F,G)` calculant $Resolv_{F,G}$ (et renvoyant un message d'erreur si le polynôme F invariant sous G n'est pas un élément primitif de l'extension). On utilisera la commande `cosets` pour obtenir des représentants du quotient S_n/G. Prenant $H = D_4$ et $F = sym_{D_4}(x_1^3x_2^2x_3)$, calculer $Resolv_{F,H}$ et exprimer cette résolvante comme élément de $\mathbb{Q}(\underline{s})[x]$ (il faudra développer le polynôme avant d'appliquer `convert_sym`, procédure qui fonctionne encore si on l'applique à un élément de $\mathbb{Q}[x_1,\dots,x_n,x]$ et donne de surcroît le résultat souhaité). On peut utiliser la commande `collect(P,x)` pour soigner l'affichage.

Pour finir, écrire une procédure `resolvante_f:=proc(f,G)` calculant $Resolv_{sym_G(f),G}$, exprimée comme élément de $\mathbb{Q}(\underline{s})[x]$. Tester avec $f = x_1x_2$ et $G = D_4$; constater que l'on obtient une résolvante pour D_4 bien plus simple qu'avec le précédent choix de F. Faire de même avec C_4 et V_4, en essayant d'obtenir un résultat aussi simple que possible.

Soit maintenant P un polynôme unitaire de $\mathbb{Z}[x]$ à racines simples α_i.

Définition 2. On appelle *H-résolvante de P relative à F* le polynôme de $\mathbb{Q}[x]$ obtenu à partir de la résolvante générale de H relative à F (qui est donc un élément primitif de $\mathbb{Q}(\underline{x})^H$) en remplaçant les x_i par les α_i, donc les s_i par les fonctions symétriques élémentaires en les α_i, c'est-à-dire par $(-1)^i a_{n-i}$ où $P = \sum_{i=1}^n a_i x^i$ ($a_n = 1$). On note $Resolv_{F;P}$ cette H-résolvante de P : le stabilisateur de F dans S_n est donc H et

$$Resolv_{F;P} = \prod_{\sigma\in S_n/H} (x - F(\alpha_{\sigma(1)},\dots,\alpha_{\sigma(n)})).$$

Par exemple, si $H = A_n$ et si l'on prend $F = d_n$, alors $Resolv_{F;P} = x^2 - \Delta(P)$ où $\Delta(P)$ est le discriminant de P (*cf.* TR.IX.A). Le lecteur pourra vérifier, par exemple avec les procédures que nous allons écrire, que la résolvante qui permet de résoudre l'équation de degré 4 dans le TR.XVI.A est la D_4-résolvante relative à $F = x_1x_3 + x_2x_4$, où $D_4 = \langle(1\ 2\ 3\ 4), (1\ 3)\rangle$ (attention, remplacer D_4 par un conjugué modifie le résultat).

On remarque qu'une H-résolvante de P est à coefficients entiers (lorsque $F \in \mathbb{Z}[\underline{x}]$). Afin d'expliquer pourquoi, nous avons besoin d'introduire l'anneau

des *entiers algébriques*, constitué des nombres algébriques dont le polynôme minimal est à coefficients entiers. Le fait qu'il s'agit bien d'un anneau signifie que le polynôme minimal d'une somme et d'un produit de deux entiers algébriques est encore à coefficients entiers, ce que l'on peut démontrer en utilisant nos méthodes effectives de calcul dans les corps de nombres (TP.XII), ou encore par un argument abstrait similaire à celui utilisé pour démontrer que les nombres algébriques forment un corps (voir [25], chapitre II). Les racines α_i de P sont des entiers algébriques, donc les $F(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ également, ainsi que les coefficients de $Resolv_{F;P}$. Comme ces coefficients sont de plus rationnels, on conclut en remarquant que les seuls entiers algébriques de $\mathbb{Q}$ sont les éléments de $\mathbb{Z}$.

Le calcul du groupe de Galois par la méthode des résolvantes est basé sur le théorème suivant :

Théorème 3. *Avec les notations précédentes, si $Gal(P)$ est contenu dans un conjugué de H alors $R = Resolv_{F;P}$ a une racine rationnelle. Réciproquement, si R n'a pas de racine multiple et si R a une racine rationnelle, alors $Gal(P)$ est un sous-groupe d'un conjugué de H.*

Appliquant ce résultat à $H = A_n$, on obtient le critère déjà utilisé : à supposer que le discriminant $\Delta(P)$ soit non nul (*i.e.* si P n'a pas de racine multiple, ce qui est le cas pour un polynôme irréductible), le groupe de Galois de P est contenu dans A_n (c'est une véritable inclusion, car A_n est distingué) si et seulement si $\Delta(P)$ est un carré entier.

Démonstration. Quitte à remplacer F par $\tau(F)$, avec $\tau \in S_n$, ce qui ne change pas $Resolv_{F;P}$ et revient juste à changer l'ordre des racines de P, on peut supposer que $Gal(P)$ est contenu dans H (et non dans un conjugué de H). On a alors $\sigma(F) = F$ pour tout $\sigma \in Gal(P)$, donc aussi

$$\sigma(F(\alpha_1, \ldots, \alpha_n)) = \sigma(F)(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n).$$

Cela montre que $F(\alpha_1, \ldots, \alpha_n)$ appartient à $\mathbb{Q}$, d'où l'existence d'une racine rationnelle de R.

Réciproquement, quitte à changer F en $\tau(F)$, on peut supposer que $F(\alpha_1, \ldots, \alpha_n)$ est rationnel, et donc que $\sigma(F)(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$ pour tout $\sigma \in Gal(P)$. Supposons $Gal(P)$ non contenu dans H et soit $\sigma \in Gal(P) - H$. Alors $(x - F)$ et $(x - \sigma(F))$ sont deux facteurs distincts de $Resolv_{F,H}$, donc $F(\alpha_1, \ldots, \alpha_n)$ est une racine double de $Resolv_{F;P}$, ce qui contredit l'hypothèse. □

12. Écrire une procédure `resolvanteP:=proc(P,f,G)`, utilisant `resolvante_f`, calculant $Resolv_{F;P}$ où $F = sym_G(f)$. Puis une procédure `test_resolvante:=proc(P,f,G)` testant si $Gal(P)$ est un sous-groupe d'un conjugué de G (et renvoyant un message d'erreur si la résolvante R calculée possède un facteur carré). Les racines rationnelles de R s'obtiennent avec la commande Maple `roots`.

Appliquer ce test aux cas de degré 4 qui n'ont pu être résolus par la méthode modulaire. On remarquera que pour $P = x^4 + 1$ par exemple, l'une des deux D_4-résolvantes $Resolv_{F;P}$ avec $f = x_1x_2$ et $f = x_1^3x_2^2x_3$ permet de conclure, mais pas l'autre.

On prend maintenant comme élément primitif $F = sym_H(\prod_{i=1}^{n-1} x_i^{n-i})$ dont on sait qu'il donne une H-résolvante (à défaut de mieux, cas par cas). Écrire une procédure `test_resolvante2:=proc(P,G)` calculant $Resolv_{F;P}$ avec ce choix pour F (on pourra même économiser la vérification de la primitivité de F et réécrire également des procédures

`resolvante2:=proc(G)` et `resolvante2P:=proc(P,G)`).

Que donne ce test en degré 5 ? En fait, Maple met énormément de temps, car les calculs formels pour la conversion en polynôme en les fonctions symétriques élémentaires sont coûteux. Pour y remédier, on va utiliser des méthodes numériques.

En effet, on a vu au TP.XI que Maple sait calculer des approximations numériques des racines complexes de P

(commande `evalf(allvalues(RootOf(P)))`).

On remplace alors les α_i par ces approximations dans la formule de la définition 2 (en prenant soin de garder cette forme factorisée lors de l'évaluation). De plus, on sait que les coefficients de $Resolv_{F;P}$ sont des entiers. En travaillant avec un nombre suffisant N de chiffres significatifs (commande `Digits:=N`) et en prenant la partie entière, on peut donc espérer (si le contrôle numérique est bon) obtenir la résolvante souhaitée.

Écrire une procédure `resolvante3P:=proc(P,G,N)` calculant la résolvante avec cette méthode, puis une procédure de test

`test_resolvante3:=proc(P,G,N)`.

Traiter enfin le cas du degré 5.

13. On ne peut conclure que lorsque la résolvante ne possède pas de racine double (rationnelle). Par exemple, 40 est racine double de la M_{20}-résolvante de

$P = x^5 + 2$ obtenue à la question précédente, et la méthode échoue. On y remédie en introduisant la transformée de Tschirnhausen de P.

L'idée est la suivante : Soit a de polynôme minimal P et $b = Q(a)$, où $Q \in \mathbb{Z}[x]$ est de degré inférieur strictement au degré de P. On a vu au TP.XI que le polynôme minimal de b est la partie sans facteur carré du résultant $P_1 = Res_y(P(y), x - Q(y))$ qui est de même degré (en x) que P. Donc si P_1 est sans facteur carré, alors b est un élément primitif de $\mathbb{Q}(a)/\mathbb{Q}$, de polynôme minimal $P_1 \in \mathbb{Z}[x]$. On remplace alors P par P_1, ce qui ne change pas le corps de décomposition, puisque ce dernier est la clôture galoisienne de $\mathbb{Q}(a)$ dans $\mathbb{C}$ et $\mathbb{Q}(a) = \mathbb{Q}(b)$. C'est ce que l'on appelle une transformée de Tschirnhausen. On peut démontrer (mais nous ne le ferons pas, l'essentiel étant de prouver l'exactitude de la méthode, ce qui vient d'être dit) qu'il existe des choix de Q qui conviennent. En pratique, nous verrons que la méthode aboutit très rapidement, avec Q pris au hasard.

Écrire une procédure `tschirn:=proc(P)` effectuant une transformation de Tschirnhausen. On tirera Q au hasard par une commande `randpoly(x,degree=d)`, d étant lui-même pris au hasard (commande `d:=rand(0..degree(P)-1)()`). Faire un essai avec $P = x^4 + 1$ et en déduire le groupe de Galois $Gal(P)$ en appliquant `test_resolvante2`.

Poursuivre et écrire une procédure `tschirnR:=proc(P,G,N)` renvoyant la résolvante d'une transformée de Tschirnhausen de P, calculée *via* `resolvante3P`. Oberserver la résultante obtenue sur l'exemple précédent : il y a explosion de la taille des coefficients. Enfin, écrire une procédure `test_resolvante4:=proc(P,G,N)`, utilisant `tschirnR`, décidant à tous les coups si $Gal(P)$ est un sous-groupe d'un conjugué de G.

Qu'obtient-on avec $P = x^5 + 2$ et $G = M_{20}$? Comparer avec le résultat de la commande `galois`. Comprenez-vous ce qui se passe ? ! (Afficher la résolvante.) Essayer d'y remédier en augmentant la précision N des calculs (vous risquez de dépasser les capacités de Maple).

Il s'agit de travailler, sur ce cas particulier, avec une meilleure résolvante. Prendre $f = x_1^2(x_2x_5 + x_3x_4)$ (après avoir vérifié) et calculer la résolvante générale R *via* `resolvante`, puis la M_{20}-résolvante de P correspondante. On pourra écrire une dernière procédure `resolvante5P:=proc(P,G,R,N)` calculant la G-résolvante de P correspondant à la résolvante générale R à l'aide des approximations numériques des racines. Conclure.

Remarque. Il est donc possible de calculer les groupes de Galois de polynômes de petits degrés en utilisant uniquement des résolvantes. Le lecteur trouvera dans [9]

des algorithmes efficaces jusqu'en degré 7 inclus. Ce ne sont pas ceux qu'utilise Maple.

Nous venons d'expliquer les lignes :

```
galois/special5:   Calculating a S5/F20 resolvent...
galois/special5:   Factoring this S5/F20 resolvent...
```

Il reste à expliquer les phrases suivantes dans le dialogue de Maple :

```
galois/respol:   Using the orbit-length partition of 2-sequences.
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Factoring the resolvent polynomial...
galois/respol:   Orbit-length partition is   4, 4, 4
```

Soit $\Omega = \{1, \ldots, n\}$, $\Omega^{\{k\}}$ l'ensemble des sous-ensembles à k éléments de Ω et $\Omega^{[k]}$ l'ensemble des listes ordonnées de k éléments de Ω. Après choix d'une numérotation des n racines distinctes, le groupe de Galois $Gal(P)$ agit sur ces trois ensembles. On pose

$$R_P^{\{k\}} = Resolv_{x_1+\ldots+x_k;P} \quad \text{et} \quad R_P^{[k]} = Resolv_{x_1+2x_2+\ldots+kx_k;P}.$$

Ce sont deux cas particuliers de résolvantes linéaires.

On va calculer ces dernières pour $k = 2$. Noter que $R_P^{[2]}$ est une H-résolvante, où le stabilisateur H de $x_1 + 2x_2$ est S_{n-2} identifié aux permutations laissant fixe 1 et 2. On en déduit

$$R_P^{[2]} = \prod_{i,j}(x - \alpha_i - \alpha_j). \tag{XVI.1}$$

De même, $R_P^{\{2\}}$ est une H-résolvante, où $H = S_{n-2} \cup (1\ 2)S_{n-2}$. On en déduit

$$R_P^{\{2\}} = \prod_{i<j}(x - \alpha_i - \alpha_j) \tag{XVI.2}$$

(les classes S_n/H sont représentées par des éléments σ tels que $\sigma(1) = i$ et $\sigma(2) = j$ avec $i < j$).

On utilise alors la propriété suivante des résultants (voir TR.VIII.C) : si $P = \prod_i(x-\alpha_i)$ et $Q = \prod_i(x-\beta_i)$, alors $\prod_{i,j}(x-\alpha_i-\beta_j) = Res_y(P(y), Q(x-y))$. On en déduit :

$$2^{\deg(P)} P\left(\frac{x}{2}\right) \left(R_P^{\{2\}}\right)^2 = Res_y(P(y), P(x-y)) \tag{XVI.3}$$

$$3^{\deg(P)} P\left(\frac{x}{3}\right) R_P^{[2]} = Res_y\left(P(y), 2^{\deg(P)} P\left(\frac{x-y}{2}\right)\right). \tag{XVI.4}$$

Revenons au calcul du groupe de Galois : lorsque $R_P^{\{2\}}$ est sans facteur multiple, la formule (XVI.2) montre que les facteurs de $R_P^{\{2\}}$ dans la décomposition en irréductibles sur $\mathbb{Q}$ correspondent aux différentes orbites de l'action du groupe $Gal(P)$ sur $\Omega^{\{2\}}$. Ainsi la liste ordonnée $L_P^{\{2\}}$ des degrés de ces facteurs est ce que Maple appelle « orbit-length partition of 2-sets ». Dans le second cas, la liste $L_P^{[2]}$ ordonnée des degrés des facteurs irréductibles dans $\mathbb{Q}[x]$ de $R_P^{[2]}$ correspond au terme « orbit-length partition of 2-sequences ». La formule (XVI.1) montre qu'il s'agit bien, lorsque $R_P^{[2]}$ est sans facteur multiple, des cardinaux des orbites de l'action du groupe $Gal(P)$ sur $\Omega^{[2]}$. En particulier, $R_P^{[2]}$ est irréductible si et seulement si $Gal(P)$ agit 2-transitivement.

La méthode consiste à comparer $L_P^{\{2\}}$ et $L_P^{[2]}$ aux résultats que l'on obtient en faisant agir les différents groupes sur $\Omega^{\{2\}}$ et $\Omega^{[2]}$.

14. D'une part, écrire des procédures `RP2a, RP2b, testa, testb` calculant respectivement, pour P donné, $R_P^{\{2\}}$ et $R_P^{[2]}$ (à l'aide des formules (XVI.3) et (XVI.4)), $L_P^{\{2\}}$ et $L_P^{[2]}$.

D'autre part, reprendre les procédures `orbite` et `orbite2G` du TP.IV.B et écrire des procédures `orbite2a` et `orbite2b` calculant, pour un groupe de permutations G défini par une commande `permgroup`, la liste ordonnée des cardinaux des orbites pour l'action de G sur $\Omega^{\{2\}}$ et $\Omega^{[2]}$ respectivement. Appliquer ces procédures à la liste habituelle des dix groupes.

Finalement, utiliser cette méthode pour décider des cas (en degrés 4 et 5) non tranchés par les méthodes modulaires. Bien entendu, on appliquera une transformation de Tschirnhausen lorsqu'une résolvante possède un facteur multiple. Peut-on conclure dans tous les cas ? Noter par exemple que Maple n'emploie pas cette méthode pour calculer $Gal(x^5 + 2)$.

This page intentionally left blank

XVII

POLYGONES RÉGULIERS CONSTRUCTIBLES ET NOMBRES DE FERMAT

On dit qu'un polygone régulier à n côtés est constructible, s'il est constructible à la règle et au compas. Le problème que nous allons étudier dans ce chapitre est le suivant : les polygones réguliers à n côtés sont-ils constructibles pour toute valeur de n ? Sinon, peut-on caractériser les entiers n pour lesquels c'est possible ?

Il est clair que, à partir d'un polygone, on peut en construire d'autres par certaines constructions géométriques simples. Par exemple, si on peut construire un polygone régulier à n côtés, on peut construire un polygone régulier à $2n$ côtés, au moyen des bissectrices des angles au centre.

Nous allons montrer comment la théorie de Galois permet de caractériser les entiers n tels que les polygones réguliers à n côtés soient constructibles. Ces entiers sont très fortement reliés aux **nombres de Fermat**.

Nous allons d'abord formaliser le problème, en précisant les notions introduites dans le TR.XI.A auquel nous renvoyons le lecteur pour les définitions et résultats.

XVII.1. Points constructibles

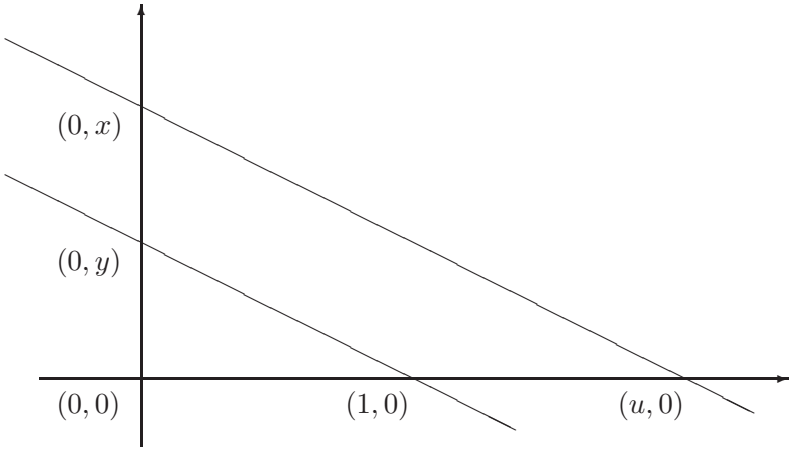
Soient $\mathcal{P}$ un ensemble fini de points du plan euclidien, de coordonnées (x_i, y_i), et K le sous-corps de $\mathbb{R}$ engendré par les x_i et y_i. On sait que si un point (x, y) est constructible à partir de $\mathcal{P}$, alors $[K(x) : K] = 2^p$ et $[K(y) : K] = 2^q$.

Le problème est maintenant de déterminer les points qui sont constructibles.

Lemme XVII.1.1. *Soit $\mathcal{P}$ un sous-ensemble fini de points de $\mathbb{R}^2$ contenant les points $(0,0)$ et $(1,0)$. Si x et y appartiennent au sous-corps de $\mathbb{R}$ engendré par les coordonnées des points de $\mathcal{P}$, le point (x,y) est constructible à partir de $\mathcal{P}$.*

Démonstration. Il est clair que, à partir de $(0,0)$ et $(1,0)$, on peut construire les axes de coordonnées. De plus, se donner les points $(0,x_0)$ et $(0,y_0)$ est équivalent à se donner le point (x_0,y_0).

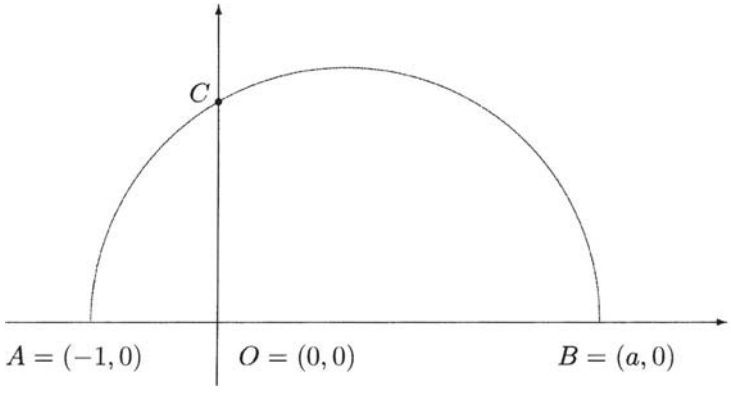
Pour démontrer le lemme il suffit de prouver que $(0,x)$ et $(0,y)$ étant donnés, on peut construire les points $(0,x+y)$, $(0,x-y)$, $(0,xy)$ et $(0,x/y)$. En ce qui concerne les points $(0,x+y)$ et $(0,x-y)$, c'est évident. Pour les points $(0,xy)$ et $(0,x/y)$, considérons la figure ci-dessous :



Les triangles $((0,0),(0,y),(1,0))$ et $((0,0),(0,x),(u,0))$ sont semblables, d'où $u/x = 1/y$, *i.e.* $u = x/y$. On peut donc construire le point $(0,x/y)$. En prenant $x = 1$, on obtient $1/y$ et en faisant la même construction, en remplacant y par $1/y$, on obtient xy, d'où la construction du point $(0,xy)$. □

Lemme XVII.1.2. *Si un point $(0,a)$, avec $a \geqslant 0$, est constructible, le point $(0,\sqrt{a})$ est constructible.*

Démonstration. Dans le dessin ci-dessous, les points A et B étant constructibles, le demi-cercle est constructible.



Les relations métriques dans le triangle rectangle ABC montrent que la longueur de OC est égale à $\sqrt{a}$. □

Lemme XVII.1.3. *Soient K le sous-corps de $\mathbb{R}$ engendré par les coordonnées d'un ensemble fini $\mathcal{P}$ de points de $\mathbb{R}^2$ contenant $(0,0)$ et $(0,1)$ et $K(\alpha)/K$, $(K(\alpha) \subset \mathbb{R})$, une extension de degré 2. Alors, tout point $(x,y) \in \mathbb{R}^2$ tel que $x \in K(\alpha)$ et $y \in K(\alpha)$ peut être construit à partir de $\mathcal{P}$.*

Démonstration. Le polynôme minimal de α s'écrit $M_\alpha(X) = X^2 + bX + c$, où $b, c \in K$, d'où $\alpha = \frac{-b\sqrt{\Delta}}{2}$, avec $\Delta = b^2 - 4c$. Puisque $K(\alpha) \subset \mathbb{R}$, Δ est positif et $(0,\Delta)$ est constructible, d'après le lemme (XVII.1.1), donc aussi $(0,\sqrt{\Delta})$, d'après le lemme (XVII.1.2). Ainsi on peut construire $(0,\alpha)$ et, par conséquent, d'après le lemme (XVII.1.1), tout point dont les coordonnées sont dans $K(\alpha)$. □

Théorème XVII.1.1. *Soit K le sous-corps de $\mathbb{R}$ engendré par les coordonnées d'un ensemble fini $\mathcal{P}$ de points de $\mathbb{R}^2$ contenant $(0,0)$ et $(0,1)$. Si α et β sont des éléments d'une extension L/K, $(L \subset \mathbb{R})$, telle que $K = K_0 \subset K_1 \subset \ldots \subset K_r = L$, avec $[K_{i+1} : K_i] = 2$, $0 \leqslant i \leqslant r-1$, alors le point (α,β) est constructible à partir de $\mathcal{P}$.*

Démonstration. On fait un raisonnement par récurrence sur r. Le lemme (XVII.1.1) donne le cas $r = 0$ et le lemme (XVII.1.3) donne le passage du rang i au rang $i+1$. □

Théorème XVII.1.2. *Soit K le sous-corps de $\mathbb{R}$ engendré par les coordonnées d'un ensemble fini $\mathcal{P}$ de points de $\mathbb{R}^2$ contenant $(0,0)$ et $(0,1)$. Si α et β sont des éléments d'une extension normale L/K, $(L \subset \mathbb{R})$, telle que $[L : K] = 2^r$, alors le point (α,β) est constructible à partir de $\mathcal{P}$.*

Démonstration. La caractéristique de K étant nulle, l'extension L/K est séparable. Soit $G = Gal(L/K)$: on a $|G| = 2^r$, d'où, d'après le lemme (VII.4.1), G possède une suite de composition

$$\{1\} = G_r \lhd G_{r-1} \lhd \ldots \lhd G_0 = G$$

telle que $|G_i| = 2^{r-i}$. Soit $K_i = Inv(G_i)$: alors $[K_{i+1} : K_i] = 2$ et le résultat découle du théorème (XVII.1.1). □

XVII.2. Constructibilité des polygones réguliers

Définition XVII.2.1.

a) On appellera ***n-gone*** un polygone régulier à n côtés.

b) Un entier n est ***constructible*** si le n-gône est constructible à partir de $(0,0)$ et $(0,1)$.

Le problème posé au début de ce chapitre est donc équivalent au suivant : « Peut-on caractériser les entiers constructibles » ?

Première étape : ***Réduction aux entiers premiers***

Lemme XVII.2.1.

(i) *Tout diviseur d'un entier constructible est constructible.*

(ii) *Si m et n sont deux entiers constructibles tels que $(m,n) = 1$, alors l'entier mn est constructible.*

Démonstration. (i). Soient n un entier constructible et m un diviseur de n. On peut faire une partition de l'ensemble des sommets d'un polygone régulier à n côtés par des sous-ensembles de $d = n/m$ sommets consécutifs et, en joignant le premier sommet de chacun de ces sous-ensembles au premier sommet du sous-ensemble adjacent, on obtient un polygone régulier à m côtés.

(ii). Si les entiers m et n sont premiers entre eux, d'après l'identité de Bezout, il existe des entiers a et b tels que $am + bn = 1$, d'où

$$\frac{1}{mn} = a\frac{1}{n} + b\frac{1}{m}\cdot$$

Donc, à partir des angles $2\pi/m$ et $2\pi/n$, on peut construire l'angle $2\pi/mn$. □

Corollaire XVII.2.1. *Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition en facteurs premiers d'un entier n. L'entier n est constructible si et seulement si chaque entier $p_i^{\alpha_i}$, $i = 1, \dots, r$, est constructible.* □

Deuxième étape : *Constructibilité des entiers p^n, p premier*

Si $p = 2$, le problème se ramène à construire les bissectrices d'un angle. On suppose donc que le nombre premier p est impair.

Lemme XVII.2.2. *Soit ζ une racine primitive p^n-ième de l'unité. Si p^n est constructible, le polynôme minimal de ζ sur $\mathbb{Q}$ est de degré une puissance de 2.*

Démonstration. Posons $\zeta = e^{2i\pi/p^n}$, $\alpha = cos(2\pi/p^n)$ et $\beta = sin(2\pi/p^n)$. Puisque p^n est constructible, le point (α, β) est constructible (c'est un sommet du p^n-gône). On en déduit que $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^n$ puis $[\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}] = 2^{n+1}$. Mais $\zeta \in \mathbb{Q}(\alpha, \beta, i)$, donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^q$ et le polynôme minimal de ζ sur $\mathbb{Q}$ est de degré une puissance de 2. □

Pour déterminer les p^n, p premier, qui sont constructibles, on doit donc déterminer les degrés des polynômes minimaux des racines primitives p^n-ième de l'unité.

Remarques XVII.2.1. Soit ζ une racine primitive p^n-ième de l'unité.

a) Si $n = 1$, le polynôme minimal de ζ est $M_\zeta(X) = 1 + X + \dots + X^{p-1}$.

b) Si $n = 2$, le polynôme minimal de ζ est $M_\zeta(X) = 1 + X^p + \dots + X^{p(p-1)}$: en effet, ce polynôme est irréductible d'après le critère d'Eisenstein et $M_\zeta(\zeta) = 0$ car $M_\zeta(X) = (X^{p^2} - 1)/(X^p - 1)$.

Théorème XVII.2.1. *L'entier n est constructible si et seulement si $n = 2^r p_1 \dots p_s$, où les entiers p_i sont des nombres premiers distincts de la forme $p_i = 1 + 2^{2^{r_i}}$, $i = 1, \dots, s$.*

Démonstration. La condition est nécessaire. Supposons que l'entier n soit constructible et soit $n = 2^r p_1^{\alpha_1} \dots p_s^{\alpha_s}$ sa décomposition en facteurs premiers. D'après le corollaire (XVII.2.1), les entiers $p_i^{\alpha_i}$, $i = 1, \dots, s$, sont constructibles. Si $\alpha_i \geqslant 2$, alors, d'après le lemme (XVII.2.1.(i)), l'entier p_i^2 est constructible ; on en déduit, d'après le lemme (XVII.2.2), que le degré du polynôme minimal d'une racine primitive p_i^2-ième de l'unité est une puissance de 2. Mais, d'après la remarque (XVII.2.1.b), il existerait β tel que $2^\beta = p_i(p_i - 1)$, ce qui est impossible puisque p_i est impair. On a donc $\alpha_i = 1$, *i.e.* p_i est constructible

pour tout $i = 1, \ldots, s$. On en déduit, d'après le lemme (XVII.2.2) et la remarque (XVII.2.1.a), que $p_i - 1 = 2^{s_i}$, *i.e.* $p_i = 1 + 2^{s_i}$. Supposons que s_i soit divisible par un entier a impair, $s_i = ab$; alors $p_i = (2^b)^a + 1$. Puisque a est impair, on a $X^a + 1 = (X + 1)(X^{a-1} - X^{a-2} + \ldots + 1)$, donc p_i est divisible par $2^b + 1$, ce qui est impossible puisqu'il est premier. D'où $s_i = 2^{r_i}$ et $p_i = 1 + 2^{2^{r_i}}$.

La condition est suffisante. D'après le corollaire (XVII.2.1), il suffit de considérer les facteurs premiers de n. Il est clair que 2^r est un entier constructible. Montrons que les entiers p_i, $i = 1, \ldots, s$, sont constructibles. Fixons un i, $1 \leqslant i \leqslant s$, et posons $a = 2^{r_i}$, $\zeta = e^{2i\pi/p_i}$. On a $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p_i - 1 = 2^a$. Posons $K = \mathbb{R} \cap \mathbb{Q}(\zeta)$; alors $\alpha = cos(2\pi/p_i) = (\zeta + \zeta^{-1})/2$ appartient à K, donc 2α aussi. Mais $2\alpha = (\zeta^2 + 1)/\zeta$, d'où $\zeta^2 - 2\alpha\zeta + 1 = 0$ et $[\mathbb{Q}(\zeta) : K] = 2$. On a $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta)$ et le groupe $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ est abélien (théorème XV.2.1) : donc $Gal(K/\mathbb{Q}) \simeq Gal(\mathbb{Q}(\zeta)/\mathbb{Q})/Gal(\mathbb{Q}(\zeta)/K)$ (exemple VI.3.1). Mais $|Gal(\mathbb{Q}(\zeta)/\mathbb{Q})| = 2^a$ et $|Gal(\mathbb{Q}(\zeta)/K)| = 2$, donc $|Gal(K/\mathbb{Q})| = 2^{a-1}$: comme l'extension $K/\mathbb{Q}$ est normale (car $Gal(\mathbb{Q}(\zeta)/K) \triangleleft Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$), d'après le théorème (XVII.1.2) le point $(cos(2\pi/p_i), 0)$ est constructible, donc l'entier p_i est constructible. □

Les nombres du type $1+2^{2^n}$ sont appelés ***nombres de Fermat***. On ne connaît que peu de ces nombres qui soient premiers. Par exemple, 3, 5, 17, 257, 65 537 sont les seuls nombres premiers de Fermat inférieurs à $10^{40\,000}$.

Construction de l'heptadécagône

La construction à la règle et au compas du polygône régulier à 17 côtés, réalisée par Gauss à l'âge de 18 ans, revient à celle du point $\zeta_{17} = e^{\frac{2i\pi}{17}}$ sur le cercle unité, ou encore d'un autre sommet qui correspond à un générateur du groupe $\mathcal{U}_{17} \simeq \mathbb{Z}/17\mathbb{Z}$ des racines $17^{\text{èmes}}$ de l'unité.

L'équation

$$\mu_{\zeta_{17}}(x) = \sum_{k=1}^{16} x^k = 0$$

admet pour groupe de Galois

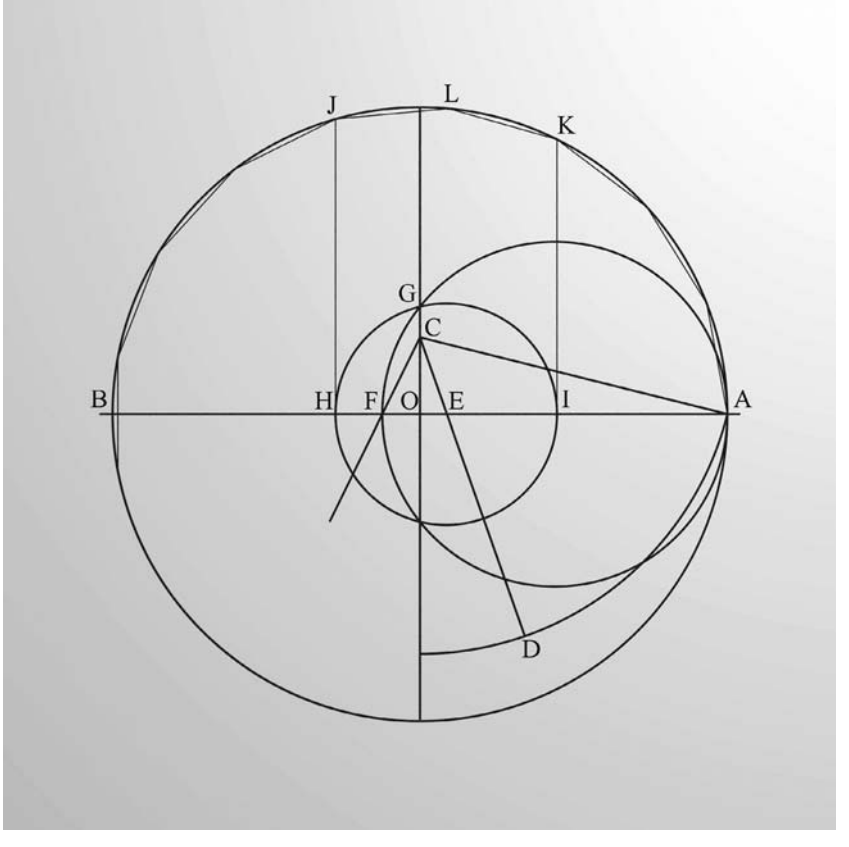
$$G = Gal(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) = (\mathbb{Z}/17\mathbb{Z})^\times,$$

qui est encore isomorphe au groupe cyclique $C_{16} = \mathbb{Z}/16\mathbb{Z}$. En effet, toutes les racines de $\mu_{\zeta_{17}}$ s'expriment comme des puissances ζ_{17}^k, $1 \leqslant k \leqslant 16$, de ζ_{17}.

Les nombres constructibles à la règle et au compas forment un corps. La construction d'un nouveau point engendre une extension de corps, qui est triviale

ou de degré 2, car déterminer l'intersection d'un cercle avec une droite, par exemple, revient à extraire une racine carrée.

La construction de Gauss est la suivante : « Tracer deux diamètres perpendiculaires AB et OC, où O est le centre et OC le quart du rayon. Tracer AC puis sur le cercle de centre C un arc de A jusqu'au diamètre OC. Prendre le point D aux trois quarts de cet arc. Tracer CD qui coupe AB au point E. Tracer CF à 45 degrés de CE. Prendre le cercle ayant AF pour diamètre. Il intersecte le diamètre OC en un point G. Tracer le cercle de centre E passant par G. Il intersecte la droite AB en H et I. Tracer les perpendiculaires à AB aux points H et I. Elles coupent le grand cercle en J et K. Soit L le milieu de l'arc JK. Alors les points J,K,L et A sont des sommets du polygône régulier à 17 côtés. les autres sommets s'en déduisent facilement. »



En fait, la construction de l'heptadécagône est rendue possible par l'existence de la suite de décomposition

$$\{e\} \lhd C_2 \lhd C_4 \lhd C_8 \lhd G,$$

à laquelle correspond, par la théorie de Galois, une tour d'extensions de degré 2. Cela permet de suivre la construction de Gauss pas à pas, chaque cercle induisant une extension (le premier est utilisé deux fois pour construire D).

Puisque G est résoluble, on dispose même de formules par radicaux. La construction géométrique s'exprime en termes algébriques par la formule suivante :

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\left(\sqrt{17} - 1 + \sqrt{2}\left(\sqrt{34 + 6\sqrt{17} + \sqrt{2}(\sqrt{17}-1)\sqrt{17-\sqrt{17}} - 8\sqrt{2}\sqrt{17+\sqrt{17}}} + \sqrt{17-\sqrt{17}}\right)\right).$$

APPENDICE

L'objet de cet appendice est un exposé des résultats généraux de la théorie des ensembles utilisés dans certaines démonstrations de cet ouvrage. Un exposé complet de ces questions nécessiterait à lui seul un livre. On ne trouvera donc ici que les rappels nécessaires à une bonne compréhension des démonstrations contenues dans ce livre. Pour plus de détails, le lecteur pourra consulter [4]. Certains points sont développés en appendice de [1].

1. Ensembles ordonnés

Définition 1.1. Une **relation d'ordre** sur un ensemble E est une relation binaire $\mathcal{R}$ satisfaisant aux conditions suivantes :

(i) $\forall x \in E,\ x\mathcal{R}x$ (**réflexivité**).

(ii) $\forall x \in E,\ \forall y \in E,\ [x\mathcal{R}y] \text{ et } [y\mathcal{R}x] \Longrightarrow [x = y]$ (***antisymétrie***).

(iii) $\forall x \in E,\ \forall y \in E,\ \forall z \in E,\ [x\mathcal{R}y] \text{ et } [y\mathcal{R}z] \Longrightarrow [x\mathcal{R}z]$ (**transitivité**).

Un **ensemble ordonné** est la donnée d'un couple $(E, \mathcal{R})$, où E est un ensemble et $\mathcal{R}$ une relation d'ordre définie sur E.

Exemples 1.1.

a) La relation $\leqslant$ sur l'ensemble $\mathbb{N}$ est une relation d'ordre.

b) Pour tout ensemble E, la relation d'inclusion est une relation d'ordre sur l'ensemble $\mathcal{P}(E)$, ensemble des parties de E.

c) La relation $\mathcal{R}$ définie sur $\mathbb{N}^*$ par « $x\mathcal{R}y$ si x est un diviseur de y » est une relation d'ordre.

d) Soient E un ensemble et $(F, \mathcal{R})$ un ensemble ordonné. On définit sur $G = \mathcal{F}(E, F)$, ensemble des applications de E dans F, une relation d'ordre, notée $\mathcal{R}'$, par

$$\forall f \in G,\ \forall g \in G,\ f\mathcal{R}'g \text{ si et seulement si } \forall x \in E,\ f(x)\mathcal{R}g(x).$$

e) Soit E un ensemble muni d'une relation d'ordre, que l'on notera $\leqslant$. Pour tous éléments $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ de E^n, on pose $x \leqslant y$ si et seulement si $x = y$ ou s'il existe $k \in \{0, 1, \ldots, n-1\}$ tel que $x_1 = y_1, \ldots, x_k = y_k, x_{k+1} \leqslant y_{k+1}$. Ceci définit une relation d'ordre sur E^n, appelé ***ordre lexicographique***.

Pour plus de commodité, sauf mention explicite, nous noterons une relation d'ordre définie sur un ensemble E par $\leqslant$ et nous écrirons « soit E un ensemble ordonné ».

Définition 1.2. Soit E un ensemble ordonné. Un élément a de E est un élément **minimal** (resp. **maximal**) de E si la relation $x \leqslant a$ (resp. $a \leqslant x$), $x \in E$, entraîne $x = a$.

Exemples 1.2.

a) Soient E un ensemble et $\mathcal{F}$ le sous-ensemble de $\mathcal{P}(E)$ formé des parties non vides de E. Les éléments minimaux de $\mathcal{F}$ sont les parties à un élément.

b) Dans l'ensemble des entiers naturels strictement plus grands que 1, ordonné par la relation « m divise n », les éléments minimaux sont les nombres premiers.

c) L'ensemble $\mathbb{R}$ muni de l'ordre usuel n'a pas d'élément minimal ou maximal.

Définition 1.3. Soit E un ensemble ordonné. Un élément a de E est le **plus petit** (resp. **plus grand**) élément de E si, pour tout $x \in E$, on a $a \leqslant x$ (resp. $x \leqslant a$).

Exemples 1.3.

a) Dans l'exemple (1.1.a), 0 est le plus petit élément de $\mathbb{N}$ et il n'y a pas de plus grand élément.

b) Dans l'exemple (1.1.b), $\emptyset$ et E sont, respectivement, le plus petit élément et le plus grand élément de $\mathcal{P}(E)$.

c) Dans l'exemple (1.2.c), il n'y a ni plus petit, ni plus grand élément.

Définition 1.4. Soient E un ensemble ordonné et X une partie de E. On appelle **minorant** (resp. **majorant**) de X dans E tout élément m (resp. M) de E tel que, pour tout $x \in X$, on ait $m \leqslant x$ (resp. $x \leqslant M$).

Définition 1.5. Une partie X d'un ensemble ordonné E est ***totalement ordonnée*** si, pour tous éléments x et y de X, on a $x \leqslant y$ ou $y \leqslant x$. Si c'est le cas pour $X = E$, on dit que la relation d'ordre sur E est ***totale***, ou que E est totalement ordonné.

Exemples 1.4.

a) La relation d'ordre usuelle sur les ensembles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ est totale.

b) La partie vide et toute partie réduite à un élément sont totalement ordonnées.

c) Si l'ensemble E admet au moins deux éléments, la relation d'ordre sur l'ensemble $\mathcal{P}(E)$, induite par inclusion, n'est pas totale.

Définition 1.6. Un ensemble ordonné E est **inductif** si toute partie non vide totalement ordonnée de E possède un majorant.

Ces ensembles possèdent l'importante propriété suivante, qui est utilisée très souvent dans cet ouvrage :

Théorème 1.1 **(lemme de Zorn).** *Tout ensemble ordonné inductif possède un élément maximal.* □

Remarques 1.1.

a) Ce théorème est équivalent à **l'axiome du choix**, dont des énoncés équivalents sont (entre autres) :

Tout produit cartésien non vide d'ensembles non vides est un ensemble non vide,

ou

Pour tout ensemble E, il existe une application

$$f : \mathcal{P}(E) \setminus \{\emptyset\} \longrightarrow E$$

telle que

$$\forall A \in \mathcal{P}(E) \setminus \{\emptyset\}, f(A) \in A.$$

b) Le lemme de Zorn est également équivalent au théorème de Zermelo énoncé ci-dessous.

Définition 1.7. Un ensemble E est ***bien ordonné*** s'il est ordonné et si, pour l'ordre considéré, toute partie non vide de E admet un plus petit élément.

***Théorème 1.2* (de Zermelo).** *Tout ensemble peut être bien ordonné.* □

Remarque 1.2. Si une relation d'ordre définie sur un ensemble E le munit d'une structure d'ensemble bien ordonné, cette relation d'ordre est totale (car toute partie à deux éléments $\{x, y\}$ a un plus petit élément). On en déduit donc que tout ensemble peut être muni d'une relation d'ordre totale. Mais attention, toute relation d'ordre définie sur un ensemble n'est pas nécessairement totale (comme on l'a vu avec l'inclusion sur l'ensemble des parties d'un ensemble), de même que toute relation d'ordre n'est pas nécessairement une relation de bon ordre. L'existence d'une relation d'ordre totale qui ne soit pas une relation de bon ordre est équivalente à l'axiome de l'infini énoncé ci-dessous.

2. Cardinaux – Ensembles infinis

Définition 2.1. Deux ensembles X et Y ont même ***cardinal***, ou sont ***équipotents***, s'il existe une application bijective de X sur Y.

On écrit alors $Card(X) = Card(Y)$.

Attention. *On vient de définir l'égalité de deux cardinaux, mais on n'a pas défini la notion de cardinal. Il s'agit « intuitivement » du nombre d'éléments de l'ensemble. Il est clair que l'égalité des cardinaux définit une relation d'équivalence sur la « classe » des ensembles. On peut alors considérer le cardinal d'un ensemble comme un représentant de sa classe d'équivalence.*

On remarquera que dans la phrase ci-dessus, on parle de la « classe » des ensembles, car parler de « l'ensemble » des ensembles conduirait à une contradiction (cet ensemble devant alors se contenir lui-même comme élément).

On remarquera que si les ensembles $\{1, \ldots, n\}$ et $\{1, \ldots, p\}$ sont équipotents, alors $n = p$. Ceci rend consistante la définition suivante :

Définition 2.2. Un ensemble E est dit ***fini*** s'il existe un entier n tel que E soit équipotent à l'ensemble $\{1, \ldots, n\}$. On écrit alors $Card(E) = n$. On dit qu'un ensemble est ***infini*** s'il n'est pas fini.

En particulier, un cardinal est infini s'il n'est pas entier.

Axiome de l'Infini. ***Il existe un ensemble infini.***

On définit maintenant une relation d'ordre sur les cardinaux, de la façon suivante :

Définition 2.3. Si E et F sont deux ensembles, on écrit $Card(E) \leqslant Card(F)$ si E est équipotent à une partie de F, ou encore s'il existe une application injective de E dans F.

Ceci définit une relation d'ordre total sur les cardinaux. La réflexivité et la transitivité sont évidentes. Par contre l'antisymétrie, loin d'être évidente, est donnée par le théorème suivant :

***Théorème 2.1* (de Cantor-Bernstein).** *Soient E et F deux ensembles. Si $Card(E) \leqslant Card(F)$ et $Card(F) \leqslant Card(E)$, alors $Card(E) = Card(F)$. (Pour une démonstration* cf. *[1].)* □

Attention. *On peut avoir $E \subset F$, $E \neq F$ et $Card(E) = Card(F)$. Par exemple, l'ensemble des nombres pairs est un sous-ensemble strict de $\mathbb{N}$ qui a même cardinal que $\mathbb{N}$, puisque ces deux ensembles se correspondent par l'application bijective $n \mapsto 2n$.*

Exercice .1. Montrer que si E et F sont deux ensembles non vides, il existe une application injective de E dans F si et seulement s'il existe une application surjective de F dans E. (Noter que la réciproque utilise l'axiome du choix.)

Proposition 2.1. *L'ensemble $\mathbb{N}$ des entiers naturels est infini.*

Démonstration. Pour tout entier n, l'ensemble $\{0, 1, \ldots, n\}$ est une partie de $\mathbb{N}$ à $n+1$ éléments. Donc $Card(\mathbb{N}) \geqslant (n+1) > n$ est différent de n. Le cardinal de $\mathbb{N}$ n'étant pas entier, $\mathbb{N}$ est un ensemble infini. □

On note $\aleph_0$ (qui se prononce aleph 0) le cardinal de $\mathbb{N}$.

Définition 2.4. Un ensemble est ***dénombrable*** s'il est équipotent à $\mathbb{N}$.

Si E est un ensemble dénombrable, une bijection f de $\mathbb{N}$ sur E permet d'écrire les éléments de E sous forme de suite $a_n = f(n)$.

Proposition 2.2. *Tout ensemble infini E contient un sous-ensemble équipotent à $\mathbb{N}$.*

Démonstration. Il suffit de montrer que si E est un ensemble infini, il existe une application injective de $\mathbb{N}$ dans E. Puisque E est un ensemble infini, pour tout $n \in \mathbb{N}$, il existe une partie de E de cardinal n (construction par récurrence). Soit n un entier : on fixe des éléments de E, deux à deux distincts, $a_{n,0}, \ldots, a_{n,n}$. On ordonne lexicographiquement $\mathbb{N}^2$ et on pose : $b_0 = a_{0,0}$ et $b_1 = a_{r,s}$, où (r, s) est le plus petit élément de $\mathbb{N}^2$ tel que $a_{r,s} \neq b_0$. Par récurrence, de la même façon, on construit $a_{p,q} \notin \{b_0, b_1, \ldots, b_n\}$. L'application définie par $f(n) = b_n$ est une application injective de $\mathbb{N}$ dans E. □

Ce qui précède montre que tout ensemble infini est au moins dénombrable, ou que $\aleph_0$ est le plus petit cardinal infini.

Nous allons maintenant définir des opérations sur les cardinaux.

Définition 2.5. Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux cardinaux et soient X et Y des ensembles tels que $\mathfrak{a} = Card(X)$ et $\mathfrak{b} = Card(Y)$.

a) On pose $\mathfrak{ab} = Card(X \times Y)$ et on l'appelle **produit** des cardinaux $\mathfrak{a}$ et $\mathfrak{b}$.

b) On choisit X et Y comme ci-dessus, vérifiant de plus $X \cap Y = \emptyset$. On pose alors $\mathfrak{a}+\mathfrak{b} = Card(X \cup Y)$, que l'on appelle **somme** des cardinaux $\mathfrak{a}$ et $\mathfrak{b}$.

c) On pose $\mathfrak{a}^{\mathfrak{b}} = Card(X^Y)$, où X^Y est l'ensemble des applications de Y dans X. Cette opération s'appelle l'**exponentiation** des cardinaux.

Remarque 2.1.

a) Lorsque les ensembles X et Y sont disjoints, $X \cap Y = \emptyset$, on note la réunion de X et Y de la façon suivante, $X \bigsqcup Y$, qu'on appelle **réunion disjointe** de X et Y.

b) Les définitions ci-dessus n'ont de sens que si elles ne dépendent pas du choix des ensembles X et Y. Le lecteur vérifiera qu'il en est bien ainsi.

Exercice .2. Montrer que, si $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ sont des cardinaux, on a les identités suivantes :

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a},\ \mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c},\ 0 + \mathfrak{a} = \mathfrak{a},$$

$$\mathfrak{ab} = \mathfrak{ba},\ \mathfrak{a}(\mathfrak{bc}) = (\mathfrak{ab})\mathfrak{c},\ 0\mathfrak{a} = 0,\ 1\mathfrak{a} = \mathfrak{a},$$

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$$

$$\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}}\mathfrak{a}^{\mathfrak{c}},\ (\mathfrak{ab})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}}\mathfrak{b}^{\mathfrak{c}},\ (\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{bc}},\ \mathfrak{a}^0 = 1,\ \mathfrak{a}^1 = \mathfrak{a},$$

avec $0 = Card(\emptyset)$ et $1 = Card(\{\emptyset\})$.

Attention. *Les égalités* $\mathfrak{a}+\mathfrak{c}=\mathfrak{b}+\mathfrak{c}$ *ou* $\mathfrak{ac}=\mathfrak{bc}$ *n'impliquent pas* $\mathfrak{a}=\mathfrak{b}$, *comme le montrent les résultats ci-dessous.*

Proposition 2.3. *L'ensemble* $\mathbb{N}\times\mathbb{N}$ *est équipotent à* $\mathbb{N}$.

Démonstration. Pour tout $n\in\mathbb{N}$, on pose $u_n=1+2+\ldots+n$. On considère l'application $f:\mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N}$ définie par $f(x,y)=y+u_{x+y}$. Montrons que f est bijective. L'application $n\mapsto u_n$ est strictement croissante. On en déduit que pour tout élément a de $\mathbb{N}$, il existe un unique entier p tel que $u_p\leqslant a<u_{p+1}$. Posons $y=a-u_p$: on a $0\leqslant y<u_{p+1}-u_p=p+1$. En posant $x=p-y$, on a $f(x,y)=a$, ce qui prouve que f est surjective. Soient x et y des entiers, $a=f(x,y)$, p l'unique entier tel que $u_p\leqslant a<u_{p+1}$. On a $u_{x+y}\leqslant a\leqslant a+x+1=u_{x+y+1}$, d'où $p=x+y$. Alors $y=a-u_p$ et $x=p-y$ et f est injective. □

On peut faire une autre démonstration, en utilisant l'ordre lexicogaphique sur $\mathbb{N}^2$ et la bijection « diagonale » (*cf.* [1]).

Théorème 2.2. *Pour tout cardinal infini* $\mathfrak{a}$, *on a* $\mathfrak{a}^2=\mathfrak{a}$.

Démonstration. Soit E un ensemble de cardinal $\mathfrak{a}$. D'après la proposition (2.2), il existe une partie F de E équipotente à $\mathbb{N}$ et, d'après la proposition (2.3), il existe une application bijective f de F sur $F\times F$. On considère l'ensemble des couples (X,g), où X est une partie de E contenant F et g est une application bijective de X sur $X\times X$ prolongeant f. Cet ensemble est non vide, car il contient (F,f), et est ordonné par la relation

$$[(X,g)\leqslant(X',g')]\Longleftrightarrow[X\subset X'\text{ et }g'\text{ est un prolongement de }g].$$

C'est un ensemble inductif ; il existe donc, d'après le lemme de Zorn (théorème 1.1), un élément maximal (Y,h). Posons $Card(Y)=\mathfrak{b}$.

Supposons que $\mathfrak{b}$ soit strictement inférieur à $\mathfrak{a}$.

Puisque $\mathfrak{b}=\mathfrak{b}^2$ est infini, on a $\mathfrak{b}\leqslant 2\mathfrak{b}\leqslant 3\mathfrak{b}\leqslant\mathfrak{b}^2=\mathfrak{b}$. En effet, il existe une application injective $Y\bigsqcup Y\hookrightarrow Y\times Y$, d'où $2\mathfrak{b}\leqslant\mathfrak{b}^2$ et, de même, $2\mathfrak{b}\leqslant 3\mathfrak{b}\leqslant\mathfrak{b}^3=\mathfrak{b}^2=\mathfrak{b}$. On a donc $\mathfrak{b}=2\mathfrak{b}$ et $\mathfrak{b}=3\mathfrak{b}$. L'hypothèse $\mathfrak{b}<\mathfrak{a}$ entraîne que $Card(E\setminus Y)>\mathfrak{b}$, car sinon on aurait $Card(E)\leqslant 2\mathfrak{b}=\mathfrak{b}$ ce qui est impossible (utiliser le fait que $E=Y\bigsqcup(E\setminus Y)$, d'où $Card(E)=Card(Y)+Card(E\setminus Y)$). Il existe donc une partie $Z\subset(E\setminus Y)$ équipotente à Y. Posons $T=Y\cup Z$. On a

$$T\times T=(Y\times Y)\cup(Y\times Z)\cup(Z\times Y)\cup(Z\times Z).$$

Les ensembles apparaissant dans le second membre sont deux à deux disjoints et, puisque Y et Z sont équipotents, on a

$$Card(Y \times Z) = Card(Z \times Z) = \mathfrak{b}^2 = \mathfrak{b},$$

d'où

$$Card((Y \times Z) \cup (Z \times Y) \cup (Z \times Z)) = 3\mathfrak{b} = \mathfrak{b}.$$

Il existe donc un application bijective k de Z sur $(Y \times Z) \cup (Z \times Y) \cup (Z \times Z)$. L'application égale à h sur Y et à k sur Z est une bijection de T sur $T \times T$ qui prolonge h, ce qui est contraire au caractère maximal du couple (Y, h). Par conséquent, $\mathfrak{b} = \mathfrak{a}$, ce qui prouve le théorème. □

Corollaire 2.1.

(i) *Si $\mathfrak{a}$ est un cardinal infini, pour tout entier $n \geqslant 1$, on a $\mathfrak{a}^n = \mathfrak{a}$.*

(ii) *Le produit d'une famille finie de cardinaux non nuls, dont le plus grand $\mathfrak{a}$ est infini, est égal à $\mathfrak{a}$.*

(iii) *Soient $\mathfrak{a}$ un cardinal infini, I un ensemble de cardinal inférieur ou égal à $\mathfrak{a}$, $(\mathfrak{a}_i)_{i \in I}$ une famille de cardinaux inférieurs ou égaux à $\mathfrak{a}$. Alors, $\sum_{i \in I} \mathfrak{a}_i \leqslant \mathfrak{a}$.*

Si de plus, $\mathfrak{a}_i = \mathfrak{a}$ pour un indice i, alors $\sum_{i \in I} \mathfrak{a}_i = \mathfrak{a}$.

(iv) *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux cardinaux non nuls dont l'un au moins est infini, alors*

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a} + \mathfrak{b} = sup(\mathfrak{a}, \mathfrak{b}).$$ □

Théorème 2.3.

(i) *Tout produit cartésien fini d'ensembles dénombrables est un ensemble dénombrable.*

(ii) *Soient I un ensemble dénombrable et, pour tout $i \in I$, E_i un ensemble dénombrable. Alors $\bigcup_{i \in I} E_i$ est un ensemble dénombrable.*

Démonstration. Ce sont des conséquences immédiates du corollaire (2.1). □

Remarque 2.2. On déduit immédiatement de la proposition (2.2) et du corollaire (2.1.(iv)), que si E est un ensemble infini, $Card(E) = Card(E)Card(\mathbb{N})$.

Proposition 2.4. *Si f est une application surjective d'un ensemble E sur un ensemble infini F telle que, pour tout élément x de F, l'ensemble $\{f^{-1}(x)\}$ est dénombrable, alors les ensembles E et F sont équipotents.*

Démonstration. Les ensembles $\{f^{-1}(x)\}$, pour $x \in F$, forment une partition de l'ensemble E par des sous-ensembles dénombrables. On en déduit donc que $Card(E) \leqslant Card(F)Card(\mathbb{N})$. D'après la remarque (2.2), on a $Card(F)Card(\mathbb{N}) = Card(F)$. L'application f étant surjective, $Card(F) \leqslant Card(E)$, d'où le résultat. □

Proposition 2.5. *Si E est un ensemble infini, l'ensemble $\mathcal{F}(E)$ des parties finies de E est équipotent à E.*

Démonstration. L'application $x \mapsto \{x\}$ est une application injective de E dans $\mathcal{F}(E)$, on a donc $Card(E) \leqslant Card(\mathcal{F}(E))$. Pour tout entier n, notons $\mathcal{F}_n(E)$ l'ensemble des parties de E à n éléments. On a $Card(\mathcal{F}_n(E)) \leqslant Card(E^n)$ et $Card(E^n) = Card(E)$, d'après le théorème (2.3.(i)). Par conséquent,

$$Card(\mathcal{F}(E)) = \sum_{n\in\mathbb{N}} Card(\mathcal{F}_n(E)) \leqslant Card(E)Card(\mathbb{N}) = Card(E).$$

On en déduit que $Card(\mathcal{F}(E)) = Card(E)$. □

Attention. *Ce résultat est faux pour l'ensemble $\mathcal{P}(E)$ des parties quelconques de E (*cf. *exercice ci-dessous).*

Exercice .3. Soit E un ensemble.

1. Montrer que
$$Card(E) < card(\mathcal{P}(E)).$$
(S'il existe une application bijective $f : E \longrightarrow \mathcal{P}(E)$, en considérant $A = \{x \in E \,|\, x \notin f(x)\}$ et $a \in A$ tel que $f(a) = A$, déduire une contradiction.)

2. Montrer que $Card(\mathcal{P}(E)) = 2^{Card(E)}$. (Considérer $A = \{0, 1\}$, f une application de X dans A : alors $f \mapsto f^{-1}(\{0\})$ est un application bijective de l'ensemble A^E sur $\mathcal{P}(E)$.)

Remarque 2.3. On peut démontrer que $Card(\mathcal{P}(\mathbb{N})) = Card(\mathbb{R})$ (*cf.* [1]). Le cardinal de $\mathbb{R}$, qui est donc strictement supérieur au cardinal de $\mathbb{N}$, s'appelle la ***puissance du continu***. Le problème suivant :

Toute partie infinie de $\mathbb{R}$ est-elle équipotente à $\mathbb{N}$ ou à $\mathbb{R}$?

est appelée ***hypothèse du continu***. Il a été démontré que cette question est ***indécidable***, c'est-à-dire que les axiomes de la théorie des ensembles ne permettent pas de démontrer que cette assertion est vraie ou qu'elle est fausse. Autrement dit, cela signifie qu'on peut ajouter aux axiomes de la théorie des ensembles l'hypothèse du continu, ou sa négation, sans aboutir à des contradictions.