radical d'un idéal, 90
rang d'un groupe abélien, 55
relation
  d'équivalence, 3
  d'ordre, 4
  réflexive, 3
  symétrique, 3
  transitive, 3
relation de dépendance algébrique, 139
représentation linéaire d'un groupe, 36

S
segment initial, 6
sous-corps
  premier, 82
sous-extension, 137
sous-groupe, 27
  caractéristique, 39
  de Sylow, 63
  distingué, 39
  engendré par une partie, 29
sous-magma, 10
  engendré par une partie, 10
sous-monoïde, 27
  engendré par une partie, 29
stabilisateur, 36
stathme euclidien, 115
suite de composition, 70
suite de Jordan-Hölder, 70
support d'une permutation, 57

T
théorème
  de d'Alembert–Gauß, 145
  de Steinitz, 147
  de Wedderburn, 150
  de Zermelo, 19
  de Zorn, 6
Théorème de Hilbert, 106
torsion, 28

ALGÈBRE

Antoine Chambert-Loir

Antoine Chambert-Loir
Université Paris-Diderot.
E-mail : Antoine.Chambert-Loir@math.univ-paris-diderot.fr

Version du 4 décembre 2016, 17h57
La version la plus récente de ce texte devrait être accessible en ligne, à l'adresse
http://webusers.imj-prg.fr/~antoine.chambert-loir/enseignement/2015-16/algebre/algebre.pdf

de Zassenhaus, 69
loi de composition, 9
associative, 10
commutative, 10

M
magma, 9
associatif, 11
commutatif, 11
quotient, 12
unifère, 11
majorant, 4
minorant, 4
module, 14
monoïde, 13, 23
abélien, 23
commutatif, 23
libre, 45
morphisme
de groupes, 13, 30
de magmas, 10
de monoïdes, 13, 30
d'extensions, 137
multiplicité d'une racine, 138

N
nilradical, 90
normalisateur, 27

O
objet d'une catégorie, 16
opération
par conjugaison, 36
par translation, 36
opération transitive, 37
orbite, 37
d'une permutation, 57
ordinal, 20
ordre
d'un élément dans un groupe, 24
ordre total, 4

P
partie stable, 36
permutation, 26
p-groupe, 63
plongement de Cayley, 36
plus grand diviseur commun, 121
plus grand élément, 5
plus petit élément, 5
plus petit multiple commun, 122
polynôme
cyclotomique, 135
primitif, 123
séparable, 144
polynôme cyclotomique, 149
polynôme homogène, 103
polynôme minimal, 140
produit
d'une famille d'anneaux, 85
d'une suite finie d'éléments d'un monoïde, 23
produit de convolution, 86
produit direct, 33
produit semi-direct, 33, 34
propriété universelle, 50
de l'ensemble quotient, 3
du groupe quotient, 42
du magma quotient, 12
du produit d'une famille de groupes, 33

Q
quaternions, 14

R
racine, 138
simple, 138
racine de l'unité, 25
radical de Jacobson, 132

distributivité de la multiplication par rapport à l'addition, 13

E
élément
  inversible d'un anneau, 80
  régulier d'un anneau, 80
  simplifiable d'un anneau, 80
élément algébrique, 139
élément inversible, 11, 14
élément maximal, 4
élément minimal, 4
élément neutre, 11
élément simplifiable, 11, 14
éléments algébriquement indépendants, 139
éléments premiers entre eux, 122
endomorphisme
  d'un groupe, 30
  d'un monoïde, 30
ensemble algébrique, 113
ensemble bien ordonné, 5
ensemble inductif, 6
ensemble quotient, 3
entiers de Gauß, 128
espace vectoriel, 15
extension
  algébrique, 139
  de rupture, 142
  galoisienne, 155
extension de corps, 137
extension de décomposition, 143
extension finie, 137

F
facteurs invariants d'un groupe abélien, 55
fixateur, 36
flèche d'une catégorie, 16
Frobenius, 84

G
graphe
  d'une application, 2
  d'une relation, 2
groupe, 13, 23
  abélien, 23
  commutatif, 23
  cyclique, 51
  de type fini, 51
  dérivé, 44
  des permutations d'un ensemble, 26
  monogène, 51
  quaternionique, 26
  simple, 44, 61
groupe alterné, 60
groupe de Galois, 155
groupoïde, 17
  de Poincaré d'un espace topologique, 17

H
homomorphisme de Frobenius, 151

I
idéal, 89
  à droite, 89
  à gauche, 89
  bilatère, 89
  maximal, 107
  premier, 107
idéaux comaximaux, 94
indéterminée, 101
indicateur d'Euler, 26
inverse, 11

L
lemme

TABLE DES MATIÈRES

1. Structures algébriques — aperçu 1
1.1. Ensembles, relations, applications 1
1.2. Magmas 9
1.3. Structures algébriques 13
1.4. Catégories 15
1.5. Exercices 18

2. Groupes 23
2.1. Définitions 23
2.2. Exemples 25
2.3. Sous-groupes 27
2.4. Morphismes 30
2.5. Produit d'une famille de groupes 32
2.6. Opérations d'un groupe dans un ensemble 34
2.7. Sous-groupes distingués et groupes quotients 39
2.8. Groupes et monoïdes libres, coproduits 45
2.9. Groupes abéliens 51
2.10. Le groupe des permutations $\mathfrak{S}_n$ 57
2.11. Théorèmes de Sylow 63
2.12. Exercices 67

3. Anneaux 79
3.1. Définitions 79
3.2. Sous-anneaux, sous-corps 80
3.3. Morphismes 83
3.4. Exemples 84
3.5. Algèbres de monoïdes, de groupes 86

3.6. Idéaux, anneaux quotients 89
3.7. Anneaux de fractions 95
3.8. Polynômes 100
3.9. Idéaux premiers, idéaux maximaux 107
3.10. Le théorème des zéros de Hilbert 111
3.11. Anneaux euclidiens, principaux, factoriels 115
3.12. Caractère factoriel des anneaux de polynômes 123
3.13. Exercices 126

4. Corps 137
4.1. Extensions de corps 137
4.2. Extensions de rupture, extensions de décomposition 142
4.3. Clôture algébrique 145
4.4. Corps finis 149
4.5. Théorie de Galois 152
4.6. Exercices 157

Bibliographie 167

Index 169

INDEX

A
algèbre, 15
  associative, 15
  commutative, 15
  de Lie, 15
  d'un monoïde, 87
  unifère, 15
anneau, 13
  euclidien, 115
  factoriel, 118
  intègre, 14, 80
  noethérien, 90
  nul, 13
  principal, 116
anneau total des fractions, 99
application orbitale, 37
automorphisme
  d'un groupe, 30
  d'un monoïde, 30
  intérieur, 31, 84
axiome du choix, 7

B
bon ordre, 5
borne inférieure, 5
borne supérieure, 5

C
caractéristique d'un corps, 82
catégorie, 16
centralisateur d'un élément, 27
centre, 27, 82
classe à gauche, à droite, 37
classe d'équivalence, 3
clôture algébrique, 146
commutateur, 24
conjugués d'un élément algébrique, 140
contenu d'un polynôme, 123
coproduit d'une famille de groupes, 50
corps, 14, 80
corps algébriquement clos, 145
corps des fractions, 99
corps fini, 149
correspondance de Galois, 155
critère d'Eisenstein, 134
crochet de Lie, 15
cycle, 57

D
degré
  d'un élément algébrique, 140
  d'une extension, 137
diagonale, 2

CHAPITRE 1

STRUCTURES ALGÉBRIQUES — APERÇU

Ce premier chapitre vise à donner un aperçu rapide des diverses structures algébriques que nous allons étudier dans ce cours, et aussi d'autres qui n'y joueront qu'un rôle d'illustration. Les chapitres suivant les reprendront avec plus de détail.

1.1. Ensembles, relations, applications

1.1.1. Ensembles. — Les présentations formelles des mathématiques couramment utilisées reposent sur la notion d'ensemble dont je supposerai une compréhension intuitive. Un ensemble possède des éléments, qui peuvent d'ailleurs eux-mêmes être des ensembles; on écrit $x \in \mathrm{A}$ pour dire qu'un élément x appartient à l'ensemble A, et $x \notin \mathrm{A}$ pour dire qu'il n'y appartient pas. La théorie des ensembles est guidée par deux principes :

a) Deux ensembles qui ont les mêmes éléments sont égaux (*extension*);
b) Si $\boldsymbol{P}(x)$ est une propriété d'un objet, on peut former l'ensemble $\{x\,;\,\mathbf{P}(x)\}$ des objets qui la vérifient (*compréhension*).

Comme l'a observé G. Russell, les choses ne peuvent pas être aussi simples.

Théorème **(1.1.2)** (Paradoxe de Russell). — *Il n'existe pas d'ensemble dont les éléments soient les ensembles vérifiant la propriété $x \notin x$.*

Je renvoie à l'excellent Doxiadis & Papadimitriou (2009) (page 162 et suivantes) pour un récit savoureux de la découverte de ce paradoxe.

Démonstration. — Raisonnons par l'absurde en supposant qu'un tel ensemble existe et notons-le R. La contradiction apparaît lorsqu'on cherche à savoir si R appartient à R ou pas.

Si R appartient à R, on a $R \in R$, donc $R \notin R$ par définition de l'ensemble R ; c'est une contradiction. Donc R n'appartient pas à R, c'est-à-dire que $R \notin R$, donc $R \in R$ par définition de R ; apparaît de nouveau une contradiction. □

Les constructions axiomatiques de la théorie des ensembles, telle celle de Zermelo–Fraenkel (ZFC), requièrent ainsi une grande attention. Au niveau de ce cours, et de la plupart des théories mathématiques, le paradoxe est éliminé par une *restriction* du principe de compréhension : si A est un ensemble et $\boldsymbol{P}(x)$ une propriété d'un objet, on peut former $\{x \in A\,;\, \boldsymbol{P}(x)\}$ l'ensemble des éléments de A qui vérifient cette propriété.

1.1.3. Relations. — Soit A un ensemble. Une relation dans l'ensemble A est une partie de A. Si R est cette relation et $a \in A$, on écrit $R(a)$ pour exprimer que a est un élément de R.

Soit n un entier naturel ; on définit plus généralement la notion de relation n-aire dans l'ensemble A : c'est une partie de l'ensemble A^n. Si R est une telle relation et si $a_1, \dots, a_n$ sont des éléments de A respectivement, on écrit $R(a_1, \dots, a_n)$ pour exprimer que le n-uplet $(a_1, \dots, a_n)$ est un élément de R.

Surtout pour les relations binaires ($n = 2$), la pratique mathématique a suggéré une notation plus concise, « infixe », consistant à écrire $a \bullet b$ pour écrire que le couple (a, b) est un élément de la relation correspondant au symbole $\bullet$. L'ensemble des couples (a, b) tels que $a \bullet b$, c'est-à-dire l'ensemble des éléments de cette relation, est alors appelé le *graphe* de la relation $\bullet$.

Par exemple, la relation d'égalité (symbole =) dans un ensemble A a pour graphe la *diagonale* du produit $A \times A$, qui est l'ensemble des couples (a, a), pour $a \in A$.

1.1.4. Applications. — Les applications forment un exemple important de relations, pour lesquelles on introduit une notation plus suggestive. Soit A et B des ensembles. Une application f de A dans B est une relation, disons R, dans l'ensemble $A \times B$ vérifiant la propriété suivante : pour tout $a \in A$, il existe un unique élément $b \in B$ tel que $R(a, b)$. On note $f : A \to B$ pour dire que f est une application de A dans B ; pour tout $a \in A$, on note $f(a)$ l'unique élément de B tel que $(a, f(a))$ appartient à R. On dit que la partie R de $A \times B$ est le graphe de l'application f.

BIBLIOGRAPHIE

N. Alon (1999), « Combinatorial Nullstellensatz ». *Combin. Probab. Comput.*, **8** (1-2), p. 7–29. URL http://dx.doi.org/10.1017/S0963548398003411, recent trends in combinatorics (Mátraháza, 1995).

N. Bourbaki (1970), *Éléments de mathématique. Théorie des ensembles*, Hermann, Paris.

A. Doxiadis & C. H. Papadimitriou (2009), *Logicomix—An epic search for truth*, Bloomsbury Press, New York. Character design and drawings by Alecos Papadatos, color by Annie Di Donna.

J. Lewin (1991), « A simple proof of Zorn's lemma ». *Amer. Math. Monthly*, **98** (4), p. 353–354. URL http://dx.doi.org/10.2307/2323807.

D. Perrin (1996), *Cours d'algèbre*, Ellipses.

H. Wielandt (1959), « Ein Beweis für die Existenz der Sylowgruppen ». *Arch. Math. (Basel)*, **10**, p. 401–402.

1.1.5. Relations binaires. — Soit $\bullet$ une relation binaire dans un ensemble A. On dit qu'elle est

- *réflexive* si $a \bullet a$ pour tout $a \in \mathrm{A}$;
- *symétrique* si $a \bullet b$ entraîne $b \bullet a$ pour tous a et b dans A ;
- *transitive* si $a \bullet b$ et $b \bullet c$ entraînent $a \bullet c$ pour tous $a, b, c \in \mathrm{A}$.

1.1.6. Relations d'équivalence. — Une *relation d'équivalence* est une relation réflexive, symétrique et transitive.

Soit $\sim$ une relation d'équivalence dans un ensemble A. Pour tout $a \in \mathrm{A}$, on appelle *classe d'équivalence* de a l'ensemble C_a des $b \in \mathrm{A}$ tels que $a \sim b$.

Lemme **(1.1.7)**. — *Soit $\sim$ une relation d'équivalence dans un ensemble* A

a) *Pour tout $a \in \mathrm{A}$, on a $a \in \mathrm{C}_a$;*
b) *Pour $a, b \in \mathrm{A}$, on a soit $\mathrm{C}_a = \mathrm{C}_b$, soit $\mathrm{C}_a \cap \mathrm{C}_b = \varnothing$;*
c) *L'ensemble des parties C_a, pour $a \in \mathrm{A}$, définit une partition de* A.

Démonstration. — a) C'est évident car la relation $\sim$ est réflexive.

b) Supposons que $\mathrm{C}_a \cap \mathrm{C}_b$ n'est pas vide et soit $c \in \mathrm{C}_a \cap \mathrm{C}_b$; on a donc $a \sim c$ et $b \sim c$. Comme la relation $\sim$ est symétrique, il vient $c \sim b$. Alors, pour tout $x \in \mathrm{C}_b$, on a $b \sim x$, puis, la relation $\sim$ étant transitive, $a \sim x$; cela prouve que $x \in \mathrm{C}_a$, d'où $\mathrm{C}_b \subset \mathrm{C}_a$. Par symétrie, on a aussi $\mathrm{C}_a \subset \mathrm{C}_b$, d'où l'égalité $\mathrm{C}_a = \mathrm{C}_b$.

c) Soit A' l'ensemble des parties C_a, pour $a \in \mathrm{A}$. D'après ce qui précède, deux éléments distincts de A' sont des parties de A qui sont disjointes. D'autre part, pour tout $a \in \mathrm{A}$, l'élement a appartient à C_a, donc les ensembles C_a ne sont pas vides et la réunion des ensembles appartenant à A' est égale à A.

□

1.1.8. — Soit $\sim$ une relation d'équivalence dans un ensemble A. L'ensemble des classes d'équivalence est appelé *ensemble quotient* et noté $\mathrm{A}/\sim$. L'application $c : \mathrm{A} \to \mathrm{A}/\sim$ qui associe à tout élément a de C sa classe C_a est une surjection, dite surjection canonique. Pour $a, b \in \mathrm{A}$, $c(a) = c(b)$ si et seulement si $\mathrm{C}_a = \mathrm{C}_b$, si et seulement si $a \sim b$.

Lemme **(1.1.9)** (Propriété universelle de l'ensemble quotient)

Soit A *et* B *des ensembles et soit $\sim$ une relation d'équivalence dans* A. *Soit $f : \mathrm{A} \to \mathrm{B}$ une application telle que $f(a) = f(b)$ pour tout couple (a, b) d'éléments de* A *tels que $a \sim b$. Il existe une unique application $\bar{f} : \mathrm{A}/\sim \to \mathrm{B}$ telle que $f = \bar{f} \circ c$.*

Malgré son apparence abstraite, cette propriété doit être considérée comme une véritable règle de calcul permettant de définir une application de source un ensemble quotient. Celle-ci est très élémentaire, nous verrons dans ce cours de nombreuses autres propriétés universelles, parfois plus subtiles. C'est un des buts de ce cours que d'amener le lecteur à en apprécier l'intérêt.

Démonstration. — Soit C un élément de A/∼. Soit a, b des éléments de C ; on a $a \sim b$, donc $f(a) = f(b)$; notons $\bar{f}(\mathrm{C})$ cet élément de B, égal à $f(a)$, pour n'importe quel élément de l'ensemble non vide C. Pour tout $a \in \mathrm{A}$, on a donc $f(a) = \bar{f}(\mathrm{C}_a) = \bar{f} \circ c(a)$, donc $\bar{f} \circ c = f$. Cela prouve l'existence d'une application $\bar{f} : \mathrm{A}/\!\sim \to \mathrm{B}$ telle que $\bar{f} \circ c = f$.

Soit alors $g : \mathrm{A}/\!\sim \to \mathrm{B}$ une application telle que $g \circ c = f$ et démontrons que $g = \bar{f}$. Soit $\mathrm{C} \in \mathrm{A}/\!\sim$ et soit $a \in \mathrm{C}$; on a $c(a) = \mathrm{C}_a = \mathrm{C}$, donc $g(\mathrm{C}) = g \circ c(a) = f(a) = \bar{f}(\mathrm{C}_a) = \bar{f}(\mathrm{C})$; par suite, $g = \bar{f}$. □

1.1.10. Relations d'ordre. — On dit qu'une relation binaire est une *relation d'ordre* si elle est réflexive, transitive et si, de plus,

– les conditions $a \bullet b$ et $b \bullet a$ entraînent que $a = b$.

Exemples : la relation d'ordre usuelle sur les nombres entiers, sur les nombres réels ; la relation de divisibilité sur les nombres entiers, ou sur les polynômes ; la relation d'inclusion sur les parties d'un ensemble ; la relation opposée à une relation d'ordre ; l'ordre lexicographique sur le produit de deux ensembles ordonnés, ou sur l'ensemble des suites finies à valeurs dans un ensemble ordonné.

Soit $\preceq$ une relation d'ordre dans un ensemble A. Soit (a, b) un couple d'éléments de A ; on dit qu'ils sont comparables si l'on a $a \preceq b$ ou $b \preceq a$. On dit qu'une partie S de A est totalement ordonnée si deux éléments quelconques de A sont comparables. Lorsque A est totalement ordonné, on dit aussi que la relation d'ordre $\preceq$ est totale.

1.1.11. Minorants, plus petit élément, borne inférieure. — Soit S une partie de A et soit a un élément de A.

On dit que a minore (*resp.* majore) S, ou est un minorant (*resp.* un majorant) de S si l'on a $a \preceq s$ (*resp.* $s \preceq a$) pour tout $s \in \mathrm{S}$.

On dit que a est un élément minimal (*resp.* maximal) de S si l'on a $a \in \mathrm{S}$ et si a est le seul élément $s \in \mathrm{S}$ tel que $s \preceq a$ (*resp.* tel que $a \preceq s$). Attention, cela n'entraîne pas que a minore (*resp.* majore) S, car il peut exister des éléments de S

Exercice **(4.6.24).** — Soit E un corps commutatif. Soit $\mathrm{P} \in \mathrm{E}[\mathrm{T}]$ un polynôme unitaire, soit $n = \deg(\mathrm{P})$; on note $\mathrm{P} = \mathrm{T}^n + c_1\mathrm{T}^{n-1} + \cdots + c_n$. Soit A le quotient de l'anneau des polynômes $\mathrm{E}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ par l'idéal engendré par les polynômes $\mathrm{S}_p - (-1)^p c_p$, où $\mathrm{S}_1, \ldots, \mathrm{S}_n$ sont les polynômes symétriques élémentaires.

a) Soit $a_1, \ldots, a_n$ les images de $\mathrm{T}_1, \ldots, \mathrm{T}_n$ dans A. Démontrer que l'on a l'égalité $\mathrm{P} = \prod_{p=1}^{n}(\mathrm{T} - a_p)$ dans $\mathrm{A}[\mathrm{T}]$.

b) Démontrer que A est un E-espace vectoriel de dimension $n!$.

c) Soit M un idéal maximal de A. Démontrer que A/M est une extension de décomposition de P sur E.

d) Démontrer qu'il existe une action du groupe symétrique $\mathfrak{S}_n$ dans A (par automorphismes de E-algèbres) tel que $\sigma(a_i) = a_{\sigma(i)}$.

e) On suppose que P est séparable. Identifier le groupe de Galois de A/M sur E au stabilisateur de M dans $\mathfrak{S}_n$.

f) On suppose toujours que P est séparable. Démontrer que l'ensemble des idéaux maximaux de A est fini. Si on les note $\mathrm{M}_1, \ldots, \mathrm{M}_r$, démontrer que A est isomorphe au produit des corps $\mathrm{A}/\mathrm{M}_1, \ldots, \mathrm{A}/\mathrm{M}_r$.

Exercice **(4.6.20)**. — Soit E l'extension de $\mathbf{Q}$ engendrée par $a = \sqrt{2+\sqrt{3}}$.

a) Calculer le polynôme minimal P de a ? Quelles sont ses racines ?

b) En déduire que E est une extension de décomposition du polynôme P.

c) Prouver que $\mathrm{Gal}(\mathrm{E}/\mathbf{Q})$ est isomorphe à $\mathbf{Z}/4\mathbf{Z}$ et en déterminer un générateur.

Exercice **(4.6.21)**. — Soit $\mathrm{P} \in \mathbf{Q}[\mathrm{T}]$ un polynôme irréductible dont le degré est un nombre premier p. Soit A l'ensemble des racines de P dans $\mathbf{C}$; on suppose que $\mathrm{Card}(\mathrm{A} \cap \mathbf{R}) = p - 2$. Soit E le sous-corps de $\mathbf{C}$ engendré par A.

a) Démontrer que l'extension E de $\mathbf{Q}$ est galoisienne.

b) Démontrer que $\mathrm{Gal}(\mathrm{E}/\mathbf{Q})$ agit transitivement sur A.

c) Soit G l'image de l'homomorphisme injectif de $\mathrm{Gal}(\mathrm{E}/\mathbf{Q})$ dans $\mathfrak{S}_\mathrm{A}$ donné par $\sigma \mapsto \sigma|_\mathrm{A}$.

d) Démontrer que G contient une transposition.

e) Démontrer que G contient un élément d'ordre p.

f) Démontrer que $\mathrm{G} = \mathfrak{S}_\mathrm{A}$.

g) Soit $\mathrm{Q}_1 = (\mathrm{T}^2+1)\prod_{a=1}^{p-2}(\mathrm{T}-a)$ et soit $\mathrm{Q}_2 \in \mathbf{Z}[\mathrm{T}]$ un polynôme unitaire de degré p. On suppose que l'image de Q_2 dans $(\mathbf{Z}/2\mathbf{Z})[\mathrm{T}]$ est irréductible. Démontrer que pour tout entier n assez grand, le polynôme $\mathrm{P} = \mathrm{Q}_2 + 2^n\mathrm{Q}_1$ vérifie les conditions de l'exercice.

Exercice **(4.6.22)**. — Soit E le sous-corps de $\mathbf{C}$ engendré par les racines du polynôme $\mathrm{P} = \mathrm{T}^3 - 2$.

a) Démontrer que P est le polynôme minimal de $\sqrt[3]{2}$.

b) Démontrer que $\mathrm{E} \neq \mathbf{Q}(\sqrt[3]{2})$.

c) En déduire que $[\mathrm{E} : \mathbf{Q}] = 6$ et que $\mathrm{Gal}(\mathrm{E}/\mathbf{Q}) \simeq \mathfrak{S}_3$.

Exercice **(4.6.23)**. — Soit E un corps commutatif et soit F une extension finie de E.

a) On suppose que F est une extension galoisienne de E. Soit $a \in \mathrm{F}$. Expliciter à l'aide du groupe $\mathrm{Gal}(\mathrm{F}/\mathrm{E})$ le polynôme minimal de a. En déduire qu'il est scindé dans F.

b) On suppose que pour tout $a \in \mathrm{F}$, le polynôme minimal de a sur E est séparable et scindé dans F. Démontrer que l'extension F de E est galoisienne.

qui ne sont pas comparables avec a. Il peut exister plusieurs éléments minimaux (*resp.* maximaux) ; par exemple si l'ensemble des nombres entiers $\geqslant 2$ est muni de la relation de divisibilité, les éléments minimaux sont les nombres premiers.

On dit que S possède un plus petit (*resp.* un plus grand) élément s'il existe un minorant (*resp.* un majorant) de S qui est un élément de S ; on dit alors naturellement que c'est le plus petit (*resp.* le plus grand) élément de S et on le note éventuellement $\min(\mathrm{S})$ (*resp.* $\max(\mathrm{S})$).

On dit que S possède une borne inférieure (*resp.* une borne supérieure) si l'ensemble des minorants de S possède un plus grand élément (*resp.* si l'ensemble des majorants de S possède un plus petit élément) ; on le note alors $\inf(\mathrm{S})$ (*resp.* $\sup(\mathrm{S})$).

1.1.12. Ensembles bien ordonnés. — On dit qu'une relation d'ordre $\preceq$ sur un ensemble A est un bon ordre, ou que l'ensemble A est bien ordonné, si toute partie non vide de A possède un plus petit élément.

Exemple fondamental : les entiers naturels. Si A et B sont des ensembles bien ordonnés, l'ordre lexicographique sur le produit $\mathrm{A} \times \mathrm{B}$ est bien ordonné.

Un bon ordre est un ordre total ; en effet, pour $a, b \in \mathrm{A}$, le plus petit élément de la partie non vide $\{a, b\}$ est comparable à l'autre.

Proposition **(1.1.13)** (Principe de récurrence transfinie)

Soit A *un ensemble bien ordonné et soit* S *une partie de* A. *On suppose que pour tout* $a \in \mathrm{A}$, *la condition suivante est vérifiée : si* $x \in \mathrm{S}$ *pour tout tout* $x \in \mathrm{A}$ *tel que* $x \prec a$, *alors* $a \in \mathrm{S}$. *Alors,* $\mathrm{A} = \mathrm{S}$.

Démonstration. — Raisonnons par l'absurde et supposons que $\mathrm{A} \neq \mathrm{S}$. Soit alors a le plus petit élément de l'ensemble non vide $\mathrm{A} - \mathrm{S}$. Par définition du plus petit élément, on a $x \notin \mathrm{A} - \mathrm{S}$ pour tout $x \in \mathrm{A}$ tel que $x \prec a$, c'est-à-dire $x \in \mathrm{S}$. L'hypothèse de la proposition entraîne alors que $a \in \mathrm{S}$, contradiction. □

1.1.14. — On peut analyser un peu plus précisément le principe de récurrence transfinie. Supposons A non vide. Alors, A possède un plus petit élément, $\min(\mathrm{A})$. De plus pour tout élément $a \in \mathrm{A}$ qui n'est pas le plus grand élément de A, l'ensemble $\{x \in \mathrm{A} \,;\, a \prec x\}$ n'est pas vide, donc possède un plus petit élément. Notons $s(a)$ cet élément. On dit que c'est le successeur de a. Les éléments de $\mathrm{A} - \{\min(\mathrm{A})\}$ qui ne sont pas successeur d'un élément de A sont appelés

limites. En effet, pour tout tel élément $a \in A$ et tout $x \in A$ tel que $x \prec a$, on a $x \prec s(x) \prec a$ (sinon, on aurait $s(x) = a$, et a serait un successeur).

Corollaire **(1.1.15)**. — *Soit* A *un ensemble bien ordonné non vide et soit* S *une partie de* A. *On fait les hypothèses suivantes :*

– *Le plus petit élément de* A *appartient à* S ;
– *Pour tout élément* $a \in S$ *qui n'est pas le plus grand élément de* A, *on a* $s(a) \in S$;
– *Pour tout élément limite* $a \in A$ *tel que* $x \in S$ *pour tout* $x \in A$ *satisfaisant* $x \prec a$, *on a* $a \in S$.

Alors, $S = A$.

Démonstration. — Vérifions que S satisfait la condition de la proposition 1.1.13. Soit $a \in A$ tel que $x \in S$ pour tout $x \in A$ tel que $x \prec a$, et prouvons que $a \in S$. Raisonnons suivant le type de a. Si $a = \min(A)$, alors $a \in S$ par hypothèse, et comme a est le seul élément de A inférieur à a, on a $a \in S'$. Supposons alors que a est successeur et soit $a' \in A$ tel que $a = s(a')$; par hypothèse, $a' \in S$, si bien que $a = s(a') \in S$. Lorsque a est limite, l'hypothèse du corollaire entraîne immédiatement que $a \in S$. Nous avons ainsi prouvé que $a \in S$ dans chaque cas, et la proposition 1.1.13 entraîne que $S = A$. □

1.1.16. — On appelle *segment initial* d'un ensemble ordonné S toute partie I de S tel que si $x \in I$ et $y \preceq x$, alors $y \in I$.

Si S est un ensemble totalement ordonné et $x \in S$, on note $S_x = \{a \in S\,;\, a \prec x\}$, où la relation $\prec$ est définie par $a \prec b$ si et seulement si $a \preceq b$ et $a \neq b$. ALors, S_x est un segment initial de S.

Lemme **(1.1.17)**. — *Soit* S *un ensemble bien ordonné et soit* I *un segment initial de* S, *distinct de* S. *Si* x *est le plus petit élément de* S ▬ I, *on a* $I = S_x$.

Démonstration. — Soit $a \in S_x$; on a $a \in S$ et $a \prec x$; comme x est le plus petit élément de S ▬ I, on en déduit que $a \in I$. Inversement, soit $a \in I$; si l'on avait $x \preceq a$, on en déduirait que $x \in I$ car x est un segment initial de S ; donc $a \prec x$ et $a \in S_x$. □

Théorème **(1.1.18)** (Zorn). — *Soit* A *un ensemble muni d'une relation d'ordre* $\preceq$. *On suppose que toute partie totalement ordonnée de* A *est majorée*[(1)]. *Alors,* A *possède un élément maximal.*

(1) On dit que A est *inductif*.

a) Démontrer que l'extension $F \subset EF$ est galoisienne, de même que l'extension $E \cap F \subset E$.

b) Démontrer que l'on définit un homomorphisme de groupes $\varphi : \mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/K)$ en posant $\varphi(\sigma) = \sigma|_E$ pour tout $\sigma \in \mathrm{Gal}(EF/F)$.

c) Démontrer que cet homomorphisme est injectif et que son image est $\mathrm{Gal}(E/E \cap F)$.

d) En déduire que $[EF : F] = [E : E \cap F]$, et que $[EF : K] = [E : K]\,[F : K]$ si et seulement si $K = E \cap F$.

Dans la suite de cet exercice, on suppose aussi que l'extension $K \subset F$ est galoisienne.

e) Démontrer que les extensions $K \subset EF$ et $K \subset E \cap F$ sont galoisiennes.

f) Démontrer que l'on définit un homomorphisme de groupes

$$\varphi : \mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$$

en posant $\varphi(\sigma) = (\sigma|_E, \sigma|_F)$ pour tout $\sigma \in \mathrm{Gal}(EF/K)$.

g) Prouver que cet homomorphisme est injectif et que son image est le sous groupe de $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ formé des couples (σ, τ) tels que $\sigma|_{E\cap F} = \tau|_{E\cap F}$.

h) Si $K = E \cap F$, en déduire que $\mathrm{Gal}(EF/K)$ est isomorphe à $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$.

Exercice **(4.6.18)**. — Soit K un corps commutatif, soit L une extension finie de K et soit E et F des extensions de K contenues dans L. On suppose que $[E : K]$ et $[F : K]$ sont premiers entre eux. Démontrer que $[EF : K] = [E : K]\,[F : K]$.

Exercice **(4.6.19)**. — Soit E un corps commutatif, soit $P \in E[T]$ un polynôme séparable (unitaire) et soit F une extension de décomposition de P. Soit A l'ensemble des racines de P dans F.

a) Démontrer que A est stable par $\mathrm{Gal}(F/E)$.

b) Démontrer que l'application $\sigma \mapsto \sigma|_A$ définit un homomorphisme injectif du groupe $\mathrm{Gal}(F/E)$ dans le groupe $\mathfrak{S}_A$ des permutations de A.

c) Démontrer que P est irréductible si et seulement si $\mathrm{Gal}(F/E)$ agit transitivement sur A.

d) Plus généralement, construire une bijection entre l'ensemble des facteurs irréductibles (unitaires) de P et l'ensemble des orbites de $\mathrm{Gal}(F/E)$ dans A.

Exercice **(4.6.13)**. — Soit E un corps commutatif, soit n un entier $\geqslant 1$ et soit $F = E(a)$ une extension de E engendrée par un élément d'ordre n.

a) Démontrer que la caractéristique de E ne divise pas n et que le polynôme $T^n - 1 \in E[T]$ est séparable.

b) Démontrer que F est une extension de décomposition du polynôme $T^n - 1 \in E[T]$.

c) Soit $\sigma \in \mathrm{Gal}(F/E)$. Démontrer qu'il existe un unique entier $d \in \{1, \dots, n\}$ tel que $\sigma(a) = a^d$.

d) Construire un homomorphisme de groupes injectifs de $\mathrm{Gal}(F/E)$ dans $(\mathbf{Z}/n\mathbf{Z})^\times$. En déduire que $\mathrm{Gal}(F/E)$ est un groupe commutatif.

Exercice **(4.6.14)**. — Soit $E \subset F$ une extension galoisienne et soit G son groupe de Galois. Soit H un sous-groupe de G et soit $K = F^H$. Démontrer qu'il existe une plus petite extension galoisienne L de E telle que $K \subset L \subset F$. Déterminer le sous-groupe de G qui lui est associé par la correspondance de Galois.

Exercice **(4.6.15)**. — Soit K un corps commutatif et soit $F = K(T_1, \dots, T_n)$ le corps des fractions rationnelles en n indéterminées $T_1, \dots, T_n$. Soit E le sous-corps de F engendré par les polynômes symétriques $S_1, \dots, S_n$.

a) Démontrer que l'extension $E \subset F$ est galoisienne et que $\mathrm{Gal}(F/E)$ est isomorphe à $\mathfrak{S}_n$.

b) Soit $a = T_1 + 2T_2 + \cdots + nT_n$. Démontrer que $F = E(a)$.

Exercice **(4.6.16)**. — Soit $E \subset F$ une extension finie galoisienne, soit G son groupe de Galois.

a) Soit $a \in F$ et soit $G_a = \{\sigma \in G;\ \sigma(a) = a\}$. Démontrer que l'extension $E(a)$ est associée au sous-groupe G_a de G par la correspondance de Galois.

b) Démontrer que $E(a) = F$ si et seulement si $G_a = \{\mathrm{id}\}$.

c) Soit b un élément de F tel que $G_a \subset G_b$. Démontrer qu'il existe un polynôme $P \in E[T]$ tel que $P(a) = b$.

Exercice **(4.6.17)**. — Soit K un corps commutatif; soit Ω une extension de K et soit E, F deux extensions de K contenues dans Ω. On note EF le sous-corps de Ω engendré par $E \cup F$.

On suppose que l'extension $K \subset E$ est galoisienne.

Démonstration, d'après Lewin *(1991)*. — Raisonnons par l'absurde en supposant que A ne possède pas d'élément maximal.

Soit C une partie totalement ordonnée de A et soit a un majorant de C. Comme a n'est pas un élément maximal de A, il existe un élément $b \in A$ tel que $a \preceq b$ et $b \neq a$; en particulier, $b \notin C$ (sinon, $b \preceq a$, d'où $a = b$). Soit T l'ensemble des parties totalement ordonnées de A et soit G l'ensemble des couples $(C, b) \in T \times A$ tel que b soit un majorant de C n'appartenant pas à C. D'après ce qui précède, la restriction à G de la première projection de $T \times A$ dans T est une application surjective. D'après l'*axiome du choix*, il existe donc une application $\mu : T \to A$ telle que pour tout $C \in T$, $\mu(C)$ est un majorant de C qui n'appartient pas à C.

On dit qu'une partie S de A est adéquate si elle est bien ordonnée et si l'on a $x = \mu(S_x)$ pour tout $x \in S$, où S_x est le segment initial $\{a \in S;\ a \prec x\}$.

Lemme **(1.1.19)**. — *Soit* S *et* S′ *des parties adéquates de* A*; alors* S *est un segment initial de* S′*, ou* S′ *est un segment initial de* S*, ou* $S = S'$.

Démonstration. — La réunion I des parties de A qui sont des segments initiaux de S et de S′ est à la fois un segment initial de S et un segment initial de S′; c'est même la plus grande partie de A qui ait cette propriété.

Si l'on a $I = S$, alors S est un segment initial de S′. Si l'on a $I = S'$, alors S′ est un segment initial de S. Supposons donc que $I \neq S$ et $I \neq S'$; notons x le plus petit élément de $S - I$ et y le plus petit élément de $S' - I$. On a donc $I = S_x = S'_y$. Comme S et S′ sont adéquates, il vient $x = \mu(S_x) = \mu(S'_y) = y$. Posons alors $J = I \cup \{x\} = I \cup \{y\}$; c'est un segment initial de S et de S′ tel que $I \subsetneq J$, ce qui contredit la définition de I. □

Notons W la réunion de toutes les parties adéquates de A; démontrons que c'est une partie adéquate de A. Il faut d'abord démontrer qu'elle est bien ordonnée. Considérons ainsi une partie non vide C de W; soit S une partie adéquate de A qui rencontre C et soit a le plus petit élément de $S \cap C$. Prouvons que a est le plus petit élément de C. Soit donc $x \in C$ et soit S′ une partie adéquate de A telle que $x \in S'$. Comme S est un segment initial de S′, ou le contraire, l'élément a, qui est le plus petit élément de $S \cap C$, est le plus petit élément de $S' \cap C$; en particulier $a \preceq x$, comme il fallait démontrer.

Soit maintenant x un élément de W et prouvons que $x = \mu(W_x)$. Soit S une partie adéquate de A qui contient x; on a donc $S \subset W$, d'où $S_x \subset W_x$. Inversement, soit y un élément de W tel que $y \prec x$ et soit S′ une partie adéquate

de A qui contient y. Si S′ est un segment initial de S, on a $y \in S$, donc $y \in S_x$. Sinon, S est un segment initial de S′, donc $S_x = S'_x$; comme $y \in S'_x$, on en déduit $y \in S_x$. Cela prouve l'égalité $S_x = W_x$. Par suite, $x = \mu(S_x) = \mu(W_x)$.

Cette partie W est la plus grande partie adéquate de A. Posons alors $W' = W \cup \{\mu(W)\}$. C'est encore une partie adéquate de W, et l'on a $W \subsetneq W'$ car $\mu(W) \notin W$. Cette contradiction termine la preuve du théorème. □

Remarque **(1.1.20)**. — Le « théorème de Zorn » est l'un des multiples « principes maximaux » développés dans les années 1900–1930 par divers mathématiciens (dont Hausdorff (1909), Kuratowski (1922), Zorn (1935)) pour contourner les « arguments transfinis » fondés sur le théorème de Zermelo (1904) selon lequel, pour tout ensemble S, il existe un bon ordre sur S. La forme générale sous laquelle nous l'avons énoncée, apparemment due à Chevalley, est celle de Bourbaki (1970).

Bien que l'existence d'un bon ordre avait initialement été présentée comme évidente par Cantor, c'est Zermelo (1904) qui en donna la première preuve. Cette preuve fut d'ailleurs immédiatement critiquée, en ce qu'elle recourait à un « principe de choix » selon lequel on peut choisir un élément privilégié de chaque partie non vide d'un ensemble donné. L'impossibilité d'expliciter effectivement un tel choix firent douter certains mathématiciens, tels Baire, Borel ou Lebesgue, de la validité de ce principe, alors que d'autres, comme Hilbert, le considéraient comme fondamental. Rappelons nous que l'immense effort de fondations dans lequel les mathématiques étaient en effet entraînées au début du XX^{e} siècle était nourri de controverses (*cf.* Doxiadis & Papadimitriou (2009)). Dans un second article, Zermelo (1908) proposa une seconde preuve à l'occasion de laquelle il explicita la première axiomatisation de la théorie des ensembles, dont l'axiome du choix qu'on peut formuler en disant que le produit d'une famille d'ensembles non vides n'est pas vide. Ou encore, de manière équivalente : pour toute application surjective $f : E \to F$, il existe une application $g : F \to E$ telle que $f \circ g = \mathrm{id}_F$.

La suspicion des mathématiciens à l'égard de cet axiome était renforcée par certains énoncés peu plausibles qu'il permet, tels les décompositions paradoxales de la sphère (Banach-Tarski, 1924) : on peut découper la boule unité de $\mathbf{R}^3$ en un nombre fini de parties et les déplacer dans l'espace de sorte à reconstituer *deux* boules de rayon unité !

b_n Un élément $x \in \mathbf{Q}$ est un carré dans $\mathbf{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ si et seulement s'il existe une partie I de $\{1, \dots, n\}$ telle que $x \prod_{i \in I}$ soit un carré dans $\mathbf{Q}$.

Démontrer que la conjonction de (a_n) et (b_n) implique (a_{n+1}) et que la conjonction de (a_n) et (b_{n-1}) implique (b_n). En déduire que ces deux propriétés sont vraies pour tout entier n.

c) Démontrer que les racines carrées $\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots$ des nombres premiers sont linéairement indépendantes sur $\mathbf{Q}$.

Exercice **(4.6.11)**. — Soit E un corps commutatif et soit F une extension finie de E. On dit qu'un élément de F est séparable sur E si son polynôme minimal est séparable.

Soit Ω une extension algébriquement close de E.

a) On suppose que F est une extension galoisienne de E. Démontrer que tout élément de F est séparable sur E.

On suppose dans la suite de l'exercice qu'il existe une partie A de F formée d'éléments séparables sur A telle que $F = E(A)$.

b) Démontrer qu'il existe une extension F′ de F qui est une extension galoisienne de E.

c) Démontrer que l'ensemble $\mathrm{Hom}_E(F, \Omega)$ est de cardinal $[F : E]$. Inversement, prouver que cette propriété entraîne que tout élément de F est séparable sur E.

d) Démontrer que l'ensemble des sous-corps K tels que $E \subset K \subset F$ est fini.

e) Démontrer qu'il existe un élément $a \in F$ tel que $F = K(a)$.

Exercice **(4.6.12)**. — Soit E le sous-corps de $\mathbf{C}$ engendré par i et $\sqrt{2}$.

a) Démontrer que $[E : \mathbf{Q}] = 4$.

b) Démontrer que E est une extension galoisienne de $\mathbf{Q}$.

c) Soit A l'ensemble $\{\pm i, \pm\sqrt{2}\}$. Démontrer que pour tout $a \in A$ et tout $\sigma \in \mathrm{Gal}(E/\mathbf{Q})$, on a $\sigma(a) \in A$. Démontrer que l'homomorphisme de $\mathrm{Gal}(E/\mathbf{Q})$ dans $\mathfrak{S}_A$ donné par $\sigma \mapsto \sigma|_A$ est injectif.

d) Quelle est l'image de cet homomorphisme ? En déduire que $\mathrm{Gal}(E/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

e) Déterminer un élément $a \in E$ tel que $E = \mathbf{Q}(a)$ et calculer son polynôme minimal.

b) Soit $P \in E[T]$ un polynôme unitaire qui divise P et soit $n = \deg(P)$. On suppose que $1 \leqslant n < \deg(P)$ et on note b le terme constant de P. Démontrer que $(-1)^{np} b^p = a^n$.

c) En déduire que P est irréductible dans $E[T]$ si et seulement s'il n'a pas de racine dans E.

Exercice **(4.6.8)**. — Soit E un corps commutatif.

a) On suppose que E est de caractéristique 0. Démontrer que tout polynôme irréductible est séparable.

On suppose dans la suite de cet exercice que p est un nombre premier et que E est de caractéristique p.

b) Soit $a \in E$ un élément qui n'est pas la puissance p-ième d'un élément de E ; démontrer que le polynôme $T^p - a$ est irréductible dans $E[T]$ mais n'est pas séparable.

c) Soit $P \in E[T]$ un polynôme irréductible qui n'est pas séparable. Démontrer que $P' = 0$. En déduire qu'il existe un polynôme séparable $Q \in E[T]$ et un entier $n \geqslant 1$ tels que $P = Q(T^{p^n})$.

d) Prouver que tout polynôme irréductible de $E[T]$ est séparable si et seulement si tout élément de E est une puissance p-ième.

Exercice **(4.6.9)**. — *a*) Soit G un groupe et soit F un corps commutatif. Soit Σ un ensemble d'homomorphismes de groupes de G dans $F^\times$. Démontrer que les éléments de Σ sont linéairement indépendants dans le F-espace vectoriel F^G. (Considérer une relation de dépendance linéaire $a_1\sigma_1 + \cdots + a_n\sigma_n = 0$, où n est minimal.)

b) Soit E et F des corps commutatifs et soit Σ l'ensemble des homomorphismes de corps de E dans F. Démontrer que les éléments de Σ sont linéairement indépendants dans le F-espace vectoriel F^E.

Exercice **(4.6.10)**. — *a*) Soit E un corps commutatif et soit F une extension de degré 2 de E. Soit $x \in F - E$ tel que $x^2 \in E$. Soit $a \in E$; on suppose que a est un carré dans F. Démontrer que a est un carré dans E, ou ax^2 est un carré dans E.

b) Soit $p_1, \ldots, p_n$ des nombres premiers distincts. On considère les deux propriétés :

a_n Le corps $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ est de degré 2^n sur $\mathbf{Q}$;

En introduisant ces « principes maximaux », leurs auteurs voulaient ainsi proposer un principe alternatif, moins sujet à controverse, à l'axiome du choix et au théorème de Zermelo. Il semble qu'Artin observa aussitôt que l'on pouvait déduire l'axiome du choix du principe maximal de Zorn. Expliquons comment, c'est un exemple simple mais caractéristique d'utilisation de ce principe.

Considérons donc une application surjective $f : E \to F$ et soit G l'ensemble des couples (S, g), où S est une partie de F et $g : S \to E$ une application telle que $f \circ g = \mathrm{id}_S$. On munit l'ensemble G de la relation d'ordre pour laquelle $(S, g) \leq (S', g')$ si $S \subset S'$ et si $g'|_S = g$. On vérifie que l'ensemble G est inductif ; il possède donc un élément maximal, disons (S, g). Si $S = F$, l'application g vérifie la propriété voulue. Sinon, on considère un élément $y \in F - S$; il existe par hypothèse un élément $x \in E$ tel que $f(y) = x$ et on considère l'application g' de $S' = S \cup \{y\}$ dans E qui prolonge g et telle que $g'(y) = x$. On a $(S', g') \in G$ et $(S, g) \leq (S', g')$, mais $S \neq S'$ ce qui contredit l'hypothèse que (S, g) était un élément maximal de G.

Ainsi, l'axiome du choix, le théorème de Zorn et celui de Zermelo sont des énoncés équivalents (voir l'exercice 1.5.5), même si on ne peut réellement apprécier cette équivalence qu'avec une compréhension un peu sérieuse de l'axiomatique des ensembles de Zermelo-Fraenkel.

Le théorème de Zorn est à la base de nombreux théorèmes d'existence du cours d'algèbre (idéaux maximaux d'un anneau, bases d'espaces vectoriels, clôture algébrique d'un corps,...) mais aussi d'analyse (théorèmes de Tychonov ou de Hahn-Banach, par exemple). Son ineffectivité (il affirme l'existence d'un objet sans permettre d'en expliciter un) reste problématique. Il est aussi intéressant de savoir que dans des formalisations « constructivistes »des mathématiques, où l'axiome du choix est exclu, ces théorèmes d'existence ne sont plus valables.

1.2. Magmas

1.2.1. Loi de composition. — Soit A un ensemble. Une loi de composition (binaire) dans A est une application $m : A \times A \to A$. Un tel ensemble muni d'une loi de composition est appelé *magma*. Si on le note parfois comme le couple (A, m) formé de l'ensemble de base et de sa loi de composition,on écrit le plus souvent informellement que A est un magma, la notation pour la loi de composition étant supposée claire.

Du reste, certaines lois de compositions binaires méritent une notation plus consise ; si $*$ est le symbole choisi pour cette loi m de composition binaire, on écrit $a * b$ au lieu de $m(a, b)$.

1.2.2. Morphismes. — Soit $(A, *)$ et $(B, \square)$ deux magmas. On dit qu'une application $f : A \to B$ est un morphisme de magmas si l'on a $f(a*b) = f(a)\square f(b)$ pour tous $a, b \in A$.

Lemme **(1.2.3).** — *Soit* A, B, C *des magmas et soit* $f : A \to B$ *et* $g : B \to C$ *des morphismes de magmas.*

a) *L'application identique de* A *est un morphisme de magmas.*

b) *La composition* $g \circ f$ *est un morphisme de magmas.*

c) *Si l'application* f *est bijective, sa bijection réciproque* $f^{-1} : B \to A$ *est un morphisme de magmas.*

Démonstration. — La première assertion est évidente, et la seconde l'est presque autant, puisque (notant $*$, $\square$ et $\triangle$ les lois de A, B, C), on a

$$\begin{aligned}(g \circ f)(a * b) = g(f(a * b)) &= g(f(a) \square f(b)) \\ &= g(f(a)) \triangle g(f(b)) = (g \circ f)(a) \triangle (g \circ f)(b).\end{aligned}$$

Démontrons enfin la troisième assertion. Soit $a', b' \in B$ et posons $a = f^{-1}(a')$ et $b = f^{-1}(b')$; on a $f(a) = a'$, $f(b) = b'$, de sorte que $f(a * b) = a' \square b'$; par suite, $a * b = f^{-1}(a' \square b')$, ce qui prouve que f^{-1} est un morphisme de magmas. □

1.2.4. Sous-magma. — Soit A un magma dont on note $*$ la loi de composition.

Un sous-magma de A est une partie B de A telle que $a * b \in B$ pour tout couple (a, b) d'éléments de B.

Si $(B_i)_{i\in I}$ est une famille de sous-magmas de A, son intersection $B = \bigcap_{i\in I} B_i$ est un sous-magma de A.

Si S est une partie de A, on appelle sous-magma de A engendré par S l'intersection de la famille de tous les sous-magmas de A qui contiennent S. C'est un sous-magma de A qui contient S et c'est le plus petit tel sous-magma.

1.2.5. Propriétés. — Soit A un magma, dont on note $*$ la loi de composition.

On dit que la loi $*$ est

- *commutative* si $a * b = b * a$ pour tous $a, b \in A$;
- *associative* si $(a * b) * c = a * (b * c)$ pour tous $a, b, c \in A$.

d) Soit d un entier tel que $1 \leqslant d < n$ et soit $P \in E[T_1, \dots, T_n]$ un polynôme homogène de degré d. Démontrer qu'il existe $a \in E^n$ tel que $a \neq 0$ et $P(a) = 0$.

Exercice **(4.6.5).** — Le but de l'exercice est de démontrer que le corps **C** des nombres complexes est algébriquement clos.

Si $P = a_n T^n + \cdots + a_0 \in \mathbf{C}[T]$ est un polynôme à coefficients complexes, on note $\bar{P}$ le polynôme conjugué défini par $\bar{P} = \bar{a_n} T^n + \cdots + \bar{a_0}$.

a) Démontrer que tout nombre complexe a une racine carrée dans **C**. En déduire que toute équation du second degré à coefficients dans **C** a ses racines dans **C**.

b) Soit $P \in \mathbf{R}[T]$ un polynôme de degré impair. Démontrer qu'il a une racine dans **R**.

c) Soit P un polynôme irréductible de $\mathbf{R}[T]$. Démontrer qu'il existe une extension finie Ω de **C** dans laquelle P est scindé et séparable. On note $d = \deg(P)$ et $a_1, \dots, a_d$ les racines de P dans Ω.

d) Soit $c \in \mathbf{R}$. Démontrer que le polynôme de $\Omega[T]$ donné par

$$P_c = \prod_{1\leqslant j<k\leqslant d} (T - (a_j + a_k + c a_j a_k))$$

appartient à $\mathbf{R}[T]$. (Utiliser le théorème sur les polynômes symétriques élémentaires.)

e) On suppose que tout polynôme Q de $\mathbf{R}[T]$ tel que $v_2(\deg(Q)) < v_2(\deg(P))$ possède une racine dans **C**. Démmontrer que pour tout $c \in \mathbf{R}$, le polynôme P_c a une racine dans **C**. En choisissant convenablement plusieurs valeurs de c, montrer qu'il existe deux indices distincts j et k tels que $a_j + a_k$ et $a_j a_k$ appartiennent à **C**. En déduire que a_j et a_k sont des éléments de **C**.

f) Démontrer que tout polynôme non constant dans $\mathbf{C}[T]$ a une racine dans **C**.

Exercice **(4.6.6).** — Soit E un corps commutatif, soit F une extension finie de E et soit $a \in F$. On suppose que $[E(a) : E]$ est impair. Démontrer que $E(a^2) = E(a)$.

Exercice **(4.6.7).** — Soit E un corps commutatif, soit p un nombre premier et soit $a \in E$. Soit F une extension de E dans laquelle le polynôme $T^p - a$ est scindé.

a) Quelles sont les racines du polynôme $T^p - a$ dans F ?

raisonner par récurrence sur n, puis sur $\deg(P)$; pour l'unicité, raisonner par récurrence sur n, puis sur $\deg(Q)$.)

Exercice **(4.6.2)** (Nullstellensatz combinatoire ALON (1999))

Soit K un corps commutatif, soit n un entier $\geqslant 1$, et soit $f \in K[T_1, \dots, T_n]$. Pour $i \in \{1, \dots, n\}$, soit A_i une partie de K et soit $g_i = \prod_{a \in A_i} (T_i - a)$.

a) On suppose que f s'annule en tout point de $A_1 \times \cdots \times A_n$. On suppose que $\mathrm{Card}(A_i) > \deg_{T_i}(f)$ pour tout i, alors $f = 0$. (Traiter d'abord le cas $n = 1$ puis raisonner par récurrence sur n.)

b) On suppose encore que f s'annule en tout point de $A_1 \times \cdots \times A_n$. Démontrer qu'il existe des polynômes $h_1, \dots, h_n \in K[T_1, \dots, T_n]$ tels que $f = \sum_{i=1}^{n} g_i h_i$ et $\deg(g_i) + \deg(h_i) \leqslant \deg(f)$ pour tout i.

c) Soit $m = (m_1, \dots, m_n) \in \mathbf{N}^n$ tel que le coefficient de T^m dans f soit non nul et tel que $\deg(f) = m_1 + \cdots + m_n$. On suppose que $\mathrm{Card}(A_i) > m_i$ pour tout i. Démontrer qu'il existe $a \in A_1 \times \cdots \times A_n$ tel que $f(a) \neq 0$.

Exercice **(4.6.3)**. — Soit p un nombre premier.

a) Soit C une partie de $\mathbf{Z}/p\mathbf{Z}$, distincte de $\mathbf{Z}/p\mathbf{Z}$, et soit $f_C \in (\mathbf{Z}/p\mathbf{Z})[X, Y]$ le polynôme $\prod_{c \in C}(X + Y - c)$. Soit $m, n \in \mathbf{N}$ tels que $\mathrm{Card}(C) = m + n$. Démontrer que le coefficient de $X^m Y^n$ dans f n'est pas nul.

b) Soit A, B des sous-ensembles non vides de $\mathbf{Z}/p\mathbf{Z}$; on pose $C = A + B$. On suppose que $\mathrm{Card}(A) + \mathrm{Card}(B) > p$; démontrer que $C = \mathbf{Z}/p\mathbf{Z}$.

c) On suppose que $\mathrm{Card}(A) + \mathrm{Card}(B) \leqslant p$. Observer que $f_C(a, b) = 0$ pour tout $(a, b) \in A \times B$. Utiliser le résultat de l'exercice 4.6.2 pour démontrer l'*inégalité de Cauchy–Davenport :*

$$\mathrm{Card}(A + B) \geqslant \mathrm{Card}(A) + \mathrm{Card}(B) - 1.$$

Exercice **(4.6.4)**. — Soit E un corps fini, soit p sa caractéristique et soit q son cardinal. Pour tout polynôme $P \in E[T_1, \dots, T_n]$, on pose $s(P) = \sum_{a \in E^n} P(a)$.

a) Calculer $s(T^m)$ pour tout entier m.

b) Soit $P \in E[T_1, \dots, T_n]$ tel que $\deg(P) < n(q-1)$. Démontrer que $s(P) = 0$.

c) Soit $P_1, \dots, P_r$ des polynômes de $E[T_1, \dots, T_n]$. Soit $V = \{a \in E^n ; P_1(a) = \cdots = P_r(a) = 0\}$.

On pose $P = \prod_{i=1}^{r}(1 - P_i^{q-1})$. Démontrer que $\mathrm{Card}(V) \cdot 1_E = s(P)$. En déduire que $\mathrm{Card}(V)$ est multiple de p si $\sum_{i=1}^{r} \deg(P_i) < n$.

On dit aussi que le magma A est commutatif (resp. associatif) pour dire que sa loi est commutative (resp. associative).

Dans un magma associatif, on peut sans ambiguïté enlever les parenthèses et écrire $a * b * c$ au lieu de $(a * b) * c$ ou $a * (b * c)$.

On dit qu'un élément a est un élément simplifiable à gauche pour la loi $*$ si $a * b = a * b'$ entraîne que $b = b'$, pour tous $b, b' \in A$. On définit de manière analogue la notion d'élément simplifiable à droite ; un élément est dit simplifiable s'il est simplifiable à gauche et à droite.

On dit qu'un élément e est un élément neutre à gauche pour la loi $*$ si $e * b = b$ pour tout $b \in A$; on définit de manière analogue la notion d'élément neutre à droite.

Lemme **(1.2.6)**. — *Soit* A *un magma possédant un élément neutre à gauche, e et un élément neutre à droite, f. Alors* $e = f$.

Sous les conditions du lemme, on dit que e est l'élément neutre du magma A et que A est un magma unifère.

Démonstration. — On calcule de deux manières la composition $e * f$. Comme e est un élément neutre à gauche, on a $e * f = e$; comme f est un élément neutre à droite, on a $e * f = f$; par suite, $e = f$. □

Soit A un magma associatif et unifère ; soit e son élément neutre. On dit qu'un élément a de A est inversible à droite s'il existe un élément $b \in B$ tel que $a * b = e$; un tel élément b est appelé *inverse à droite* de a. On définit de même la notion d'élément inversible à gauche, et d'inverse à gauche.

Lemme **(1.2.7)**. — *Soit* $(A, *)$ *un magma associatif et unifère ; notons e son élément neutre. Soit a un élément de* A.

a) *Si a est inversible à droite, alors il est simplifiable à droite ;*
b) *Si a est inversible à gauche, il est simplifiable à gauche ;*
c) *Supposons que a soit inversible à droite et à gauche ; soit b un inverse à droite et soit c un inverse à gauche de a. On a* $b = c$.

Par suite, si un élément a est inversible à droite et à gauche, on dit qu'il est inversible, et que l'unique élément b de A tel que $a * b = b * a = e$ est son *inverse*.

Démonstration. — a) Supposons que a est inversible à droite et soit b un inverse à droite de a. Soit $c, c' \in A$ tels que $c * a = c' * a$; on a $c = c * e =$

$c * (a * b) = (c * a) * b = (c' * a) * b = c' * (a * b) = c' * e = c'$. Cela prouve que a est simplifiable à droite.

b) L'assertion se démontre de même que la précédente.

c) Avec les notations de l'assertion, on a $c * a = a * b = e$. Par suite, $b = e * b = (c * a) * b = c * (a * b) = c * e = c$. □

1.2.8. — Soit $(A, *)$ un magma et soit $\sim$ une relation d'équivalence dans A. On dit que la relation $\sim$ est compatible avec la loi de composition de A si les relations $a \sim a'$ et $b \sim b'$ entraînent $a * b \sim a' * b'$. Il existe alors une unique loi de composition sur l'ensemble quotient $A/\sim$ pour laquelle la surjection canonique $c : A \to A/\sim$ est un morphisme de magmas ; on dit que $A/\sim$, muni de cette loi de composition, est le magma quotient de A par la relation d'équivalence $\sim$.

Si le magma A est associatif (*resp.* commutatif) il en est de même du magma $A/\sim$. Si A est unifère, alors $A/\sim$ l'est aussi et son élément neutre est l'image $c(e)$ de l'élément neutre e de A.

Supposons que A soit associatif et unifère. L'image $c(a)$ d'un élément a de A qui est inversible à droite (*resp.* à gauche) est inversible à droite (*resp.* à gauche) ; en effet, si b est un inverse à droite (*resp.* à gauche) de a, son image est un inverse à droite (*resp.* à gauche) de $c(a)$.

En particulier, si A est un groupe, le magma quotient $A/\sim$ est un groupe.

Lemme **(1.2.9)** (Propriété universelle du magma quotient)

Soit A *un magma et soit* $\sim$ *une relation d'équivalence dans* A *qui est compatible avec sa loi de composition. Soit* B *un magma et soit* $f : A \to B$ *un morphisme de magmas tel que* $f(a) = f(a')$ *pour tout couple* (a, a') *d'éléments de* A *tel que* $a \sim a'$. *Il existe un unique morphisme de magmas* $\bar{f} : A/\sim \to B$ *tel que* $f = \bar{f} \circ c$.

Démonstration. — Soit $\bar{f}$ l'application de $A/\sim$ dans B telle que $f = \bar{f} \circ c$. Démontrons que c'est un morphisme de magmas. Soit x et y des éléments de $A/\sim$ et soit a, b des éléments de A tels que $x = c(a)$ et $y = c(b)$; on a $\bar{f}(x) = f(a)$ et $\bar{f}(y) = f(b)$. Par définition de la loi de composition de $A/\sim$, on a $x * y = c(a) * c(b) = c(a * b)$; on a alors

$$\bar{f}(x * y) = \bar{f}(c(a * b)) = f(a * b) = f(a) * f(b) = \bar{f}(x) * \bar{f}(y),$$

d'où le lemme. □

Pour tout $\sigma \in G - \{\mathrm{id}\}$, il existe $a \in F$ tel que $\sigma(a) \neq a$; soit A_1 une partie finie de F contenant un tel élément pour chaque $\sigma \in G - \{\mathrm{id}\}$. Soit $A = G \cdot A_1$; c'est une partie finie de F, stable par G.

Soit $K = E(A)$. Alors, l'extension $E \subset K$ est finie. Pour tout $\sigma \in G$, on a $\sigma(A) = A$, cela entraîne que $\sigma(K) = K$. De plus, pour tout $\sigma \in G - \{\mathrm{id}\}$, il existe $a \in K$ tel que $\sigma(a) \neq a$, donc l'application $\sigma \mapsto \sigma|_K$ de G dans $\mathrm{Aut}_E(K)$ est injective. Alors,

$$E \subset K^{\mathrm{Aut}_E(K)} \subset K^G \subset L^G = E,$$

si bien que $E = K^{\mathrm{Aut}_E(K)} = K^G$. La première égalité prouve que l'extension $E \subset K$ est galoisienne. D'après la correspondance de Galois, la seconde entraîne que $G = \mathrm{Aut}_E(K)$. En particulier, on a $[K : E] = \mathrm{Card}(G)$.

Soit $a \in F$. On peut reprendre l'argument précédent avec la partie $A' = A \cup G \cdot a$. En notant $K' = E(A')$, on a donc $[K' : E] = \mathrm{Card}(G) = [K : E]$. Puisque $K \subset K'$, cela entraîne $K = K'$, donc $a \in K$. Ainsi, $K = F$, l'extension $E \subset F$ est galoisienne et l'on a $G = \mathrm{Gal}(F/E)$.

4.6. Exercices

Exercice **(4.6.1)**. — Soit A un anneau commutatif et soit n un entier $\geqslant 1$.

a) Pour tout $\sigma \in \mathfrak{S}_n$, démontrer qu'il existe un unique automorphisme σ' de la A-algèbre $A[T_1, \ldots, T_n]$ tel que $\sigma'(T_i) = T_i$. Vérifier que l'application $\sigma \mapsto \sigma'$ est un homomorphisme de groupes de $\mathfrak{S}_n$ dans $\mathrm{Aut}_A(A[T_1, \ldots, T_n])$.

b) On dit qu'un polynôme $P \in A[T_1, \ldots, T_n]$ est symétrique si l'on a $\sigma'(P) = P$ pour tout $\sigma \in \mathfrak{S}_n$.

Pour tout $p \in \{1, \ldots, n\}$, on pose

$$S_p = \sum_{1 \leqslant i_1 < \cdots < i_p \leqslant n} T_{i_1} \ldots T_{i_p}.$$

Démontrer que les polynômes $S_1, \ldots, S_n$ sont symétriques.

c) Soit $P \in A[T_1, \ldots, T_n]$ un polynôme symétrique. Démontrer que le polynôme $P_0 \in A[T_1, \ldots, T_{n-1}]$ défini par $P_0 = P(T_1, \ldots, T_{n-1}, 0)$ est symétrique. Que deviennent les polynômes $S_1, \ldots, S_n$ lorsqu'on remplace T_n par 0 ?

d) Soit $P \in A[T_1, \ldots, T_n]$ un polynôme symétrique. Démontrer qu'il existe un unique polynôme $Q \in A[T_1, \ldots, T_n]$ tel que $P = Q(S_1, \ldots, S_n)$. (Pour l'existence,

Corollaire **(4.5.9)**. — *Soit* F *un corps commutatif et soit* E *un sous-corps de* F *tel que l'extension* $E \subset F$ *soit galoisienne. Soit* K *un sous-corps de* F *qui contient* E. *Alors l'extension* $K \subset F$ *est galoisienne. De plus, les conditions suivantes sont équivalentes :*

(i) *L'extension* $E \subset K$ *est galoisienne ;*
(ii) *Pour tout élément* $\sigma \in \mathrm{Gal}(F/E)$, *on a* $\sigma(K) = K$;
(iii) *Le groupe* $\mathrm{Gal}(F/K)$ *est un sous-groupe distingué de* $\mathrm{Gal}(F/E)$.

Démonstration. — Soit P un polynôme séparable de $E[T]$ dont F est une extension de décomposition. Si l'on considère P comme un polynôme de $K[T]$, on constate que F est une extension de décomposition de P sur K. Par suite, l'extension $K \subset F$ est galoisienne.

(i)⇒(ii). Supposons l'extension $E \subset K$ galoisienne. Soit $\sigma \in \mathrm{Gal}(F/E)$; démontrons que $\sigma(K) \subset K$. Par hypothèse, K est extension de décomposition d'un polynôme séparable $Q \in E[T]$. Pour toute racine a de Q, $\sigma(a)$ est racine de Q, donc $\sigma(a) \in K$. Comme l'extension K est engendrée par les racines de Q, on a $\sigma(K) \subset K$. On a aussi $\sigma^{-1}(K) \subset K$, d'où, en appliquant σ, l'inclusion $K \subset \sigma(K)$. Cela démontre que $\sigma(K) = K$.

(ii)⇒(i). Soit $p : \mathrm{Aut}_E(F) \to \mathrm{Aut}_E(K)$ l'homomorphisme de groupes donné par $p(\sigma) = \sigma|_F$. Son noyau est $\mathrm{Aut}_K(F)$, donc est de cardinal $[F : K]$. Comme $\mathrm{Card}(\mathrm{Aut}_E(F)) = [F : E]$, le cardinal de l'image de p est égal à $[F : E]/[F : K] = [K : E]$. Cela prouve que $\mathrm{Card}(\mathrm{Aut}_E(K)) \geqslant [K : E]$. On a donc égalité et l'extension K de E est galoisienne.

(ii)⇒(iii). Soit $\sigma \in \mathrm{Gal}(F/K)$ et $\tau \in \mathrm{Gal}(F/E)$; démontrons que $\tau^{-1}\sigma\tau \in \mathrm{Gal}(F/K)$. Soit $a \in K$; par hypothèse, on a $\tau(a) \in K$; par suite, $\sigma(\tau(a)) = \tau(a)$, d'où $\tau^{-1}\sigma\tau(a) = \tau^{-1}(\tau(a)) = a$. Cela démontre que $\tau^{-1}\sigma\tau \in \mathrm{Gal}(F/K)$. Ainsi, le sous-groupe $\mathrm{Gal}(F/K)$ est distingué dans $\mathrm{Gal}(F/E)$.

(iii)⇒(ii). Soit $\sigma \in \mathrm{Gal}(F/E)$. Le sous-corps de F fixé par $\sigma\,\mathrm{Gal}(F/K)\sigma^{-1}$ est égal à $\sigma(K)$. Si $\mathrm{Gal}(F/K)$ est un sous-groupe distingué de $\mathrm{Gal}(F/E)$, on a donc $\sigma(K) = K$. □

Remarque **(4.5.10)**. — Soit F un corps commutatif, soit G un sous-groupe fini du groupe $\mathrm{Aut}(F)$ des automorphismes de F et soit $E = F^G$. Démontrons que l'extension $E \subset F$ est finie, et donc galoisienne (théorème 4.5.5, condition (iv)).

Soit $a \in F$; le polynôme $\prod_{\sigma \in G}(T - \sigma(a))$ est invariant par G donc appartient à $E[T]$, et possède a comme racine. Ainsi, tout élément de F est algébrique sur E.

1.3. Structures algébriques

1.3.1. Monoïdes. — Un monoïde est un ensemble muni d'une loi de composition associative et possédant un élément neutre.

Exemples : les ensembles usuels de nombres (entiers, réels, complexes) pour l'addition ou la multiplication ; les entiers positifs, les nombres réels positifs pour l'addition, ou la multiplication ; les matrices carrées de taille donnée à coefficients positifs ou nuls, pour la multiplication.

Un morphisme de monoïde est un morphisme de magmas qui applique l'élément neutre sur l'élément neutre.

Un sous-monoïde d'un monoïde M est un sous-magma qui contient l'élément neutre ; la loi de composition de M en fait alors un monoïde.

1.3.2. Groupes. — On dit qu'un monoïde est un groupe si tout élément est inversible.

Un morphisme de groupes est un morphisme de monoïdes.

Un sous-groupe d'un groupe G est un sous-monoïde qui est un groupe.

1.3.3. Anneaux. — Un *anneau* est un ensemble A muni de deux lois, une addition + et une multiplication ·, vérifiant les propriétés suivantes :

– Le magma $(A, +)$ est un groupe commutatif ; on note 0 son élément neutre.
– Le magma $(A, \cdot)$ est associatif et unifère ; on note 1 son élément neutre.
– La multiplication est *distributive* par rapport à l'addition : on a $a \cdot (b + c) = a \cdot b + a \cdot c$ et $(b + c) \cdot a = b \cdot a + c \cdot a$ pour tous a, b, c dans A.

On dit que l'anneau A est commutatif si sa multiplication est commutative.

On remarquera qu'un ensemble réduit à un élément, disons a, est un anneau commutatif lorsqu'on le munit de la seule addition et la seule multiplication possible ; dans cet anneau, $0 = 1$; on l'appelle l'anneau nul.

1.3.4. Exemples d'anneaux. — Les entiers relatifs, les nombres réels, complexes ; les matrices carrées de taille fixée à coefficients dans un anneau donné.

Lemme **(1.3.5)**. — *Soit* A *un anneau. Pour tout* $a \in A$, *on* $a - a = (-1) \cdot a = a \cdot (-1)$ *et* $0 = a \cdot 0 = 0 \cdot a$.

Démonstration. — On a $0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a$, donc $0 \cdot a = 0$; on démontre de même que $a \cdot 0 = 0$. Enfin, $a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a =$

$(1+(-1))\cdot a = (1-1)\cdot a = 0\cdot a = 0$, donc $(-1)\cdot a = -a$, et on prouve de même que $a\cdot(-1) = -a$. □

Soit A un anneau. On dit qu'un élément de A est simplifiable (resp. inversible) à droite (resp. à gauche, resp. sans précision) s'il l'est dans le magma associatif et unifère $(A,\cdot)$.

On dit qu'un anneau est *intègre* s'il n'est pas réduit à $\{0\}$ et si tout élément non nul est simplifiable.

On dit qu'un anneau est un *corps* s'il n'est pas réduit à $\{0\}$ et si tout élément non nul est inversible.[2]

Exemples : Les corps des nombres rationnels, des nombres réels, des nombres complexes; le corps des fractions rationnelles à coefficients dans un corps commutatif; l'ensemble **H** des matrices 2×2 à coefficients complexes de la forme $\left(\begin{smallmatrix} a & -b \\ \bar{b} & \bar{a}\end{smallmatrix}\right)$, pour $a, b \in \mathbf{C}$ (corps des *quaternions*).

1.3.6. Modules et espaces vectoriels. — Soit A un anneau.

Un A-*module à gauche* est un groupe abélien $(M,+)$ muni d'une « multiplication externe » $A\times M\to M$, notée $(a,m)\mapsto a\cdot m$, qui vérifie les propriétés suivantes :

- On a $a\cdot(m+n) = a\cdot m + a\cdot n$ pour tout $a\in A$ et tous $m,n\in M$;
- On a $(a+b)\cdot m = a\cdot m + b\cdot m$ pour tous $a,b\in A$ et tout $m\in M$;
- On a $a\cdot(b\cdot m) = (ab)\cdot m$ pour tous $a,b\in A$ et tout $m\in M$;
- On a $1\cdot m = m$ pour tout $m\in M$.

On note 0 l'élément neutre de M; on prendra garde à ne pas le confondre avec l'élément nul de A.

On définit aussi la notion de A-*module à droite;* la multiplication externe est une application de $M\times A$ dans M, notée $(m,a)\mapsto m\cdot a$, et vérifie des propriétés similaires aux précédentes :

- On a $(m+n)\cdot a = m\cdot a + n\cdot a$ pour tout $a\in A$ et tous $m,n\in M$;
- On a $m\cdot(a+b) = m\cdot a + m\cdot b$ pour tous $a,b\in A$ et tout $m\in M$;
- On a $(m\cdot a)\cdot b = m\cdot(ab)$ pour tous $a,b\in A$ et tout $m\in M$;
- On a $m\cdot 1 = m$ pour tout $m\in M$.

Cela revient à un module à gauche sur l'anneau opposé A^{o}.

[2] Certains auteurs appellent anneau à division un tel anneau, réservant le nom de corps à ceux qui sont commutatifs.

$[F:E]$. Tout E-morphisme $f: F\to F$ est injectif et son image est un sous-espace vectoriel de F de dimension $[F:E]$, donc est surjectif. On a ainsi démontré que $\mathrm{Card}(G) = [F:E]$. □

Définition **(4.5.6).** — *Soit* E *un corps commutatif et soit* F *une extension finie de* E. *On dit que c'est une* extension galoisienne *si les conditions équivalentes du théorème 4.5.5 sont satisfaites. Le groupe* $\mathrm{Aut}_E(F)$ *est alors appelé* groupe de Galois *de l'extension et est noté* $\mathrm{Gal}(F/E)$.

Exemple **(4.5.7).** — Soit E un corps fini et soit F une extension finie de E. Posons $q = \mathrm{Card}(E)$ et $n = [F:E]$. L'application $\varphi: F\to F$ définie par $\varphi(x) = x^q$ est un morphisme de corps. On a $\varphi(a) = a$ pour tout $a\in E$. Comme F est fini, φ est bijectif. C'est donc un élément de $\mathrm{Aut}_E(F)$. Pour tout entier $m\geqslant 1$ et tout $x\in F$, on a $\varphi^m(x) = x^{q^m}$. En particulier, $\varphi^n = \mathrm{id}_F$. Si $1\leqslant m<n$, on a $\varphi^m\neq \mathrm{id}$ car le polynôme $T^{q^m}-T$ a au plus q^m racines dans F. Cela prouve que φ est d'ordre n dans $\mathrm{Gal}(F/E)$. Puisque $[F:E] = n$, cela implique d'une part que l'extension F de E est galoisienne, et d'autre part que son groupe de Galois est engendré par φ, donc est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

Corollaire **(4.5.8)** (Correspondance de Galois). — *Soit* F *un corps commutatif, soit* E *un sous-corps de* F *tel que l'extension* $E\subset F$ *soit galoisienne.*

Les applications $H\mapsto F^H$ *et* $K\mapsto \mathrm{Aut}_K(F)$ *sont des bijections, inverses l'une de l'autre, entre sous-groupes* H *de* $\mathrm{Gal}(F/E)$ *et sous-corps* K *de* F *qui contiennent* E.

Démonstration. — Soit K un sous-corps de F qui contient E. D'après la propriété (iii), l'extension F/K est galoisienne. En particulier, $K = F^{\mathrm{Aut}_K(F)}$ et $\mathrm{Card}(\mathrm{Aut}_K(F)) = [F:K]$.

Soit H un sous-groupe de $\mathrm{Aut}_E(F)$ et soit $K = F^H$. Alors, l'extension F/K est galoisienne et $\mathrm{Card}(\mathrm{Gal}(F/K)) = [F:K]$. Démontrons que l'on a $H = \mathrm{Gal}(F/K)$. On a $H\subset \mathrm{Gal}(F/K)$ par construction de K. Inversement, soit $a\in F$ un élément dont le polynôme minimal P sur K est scindé et séparable dans F. On a donc $F = K(a)$, $\deg(P) = [F:K]$ et l'application $\sigma\mapsto\sigma(a)$ est une bijection de $\mathrm{Aut}_K(F)$ sur l'ensemble des racines de P dans F. Par suite, le polynôme $Q = \prod_{\sigma\in H}(T-\sigma(a))$ de $F[T]$ divise P; comme il est invariant par H, il appartient à $F^H[T] = K[T]$. Par définition du polynôme minimal, cela entraîne que $P = Q$, d'où $\mathrm{Card}(H) = \deg(Q) = \deg(P) = \mathrm{Card}(\mathrm{Gal}(F/K))$. On a donc l'égalité $H = \mathrm{Card}(F/K)$. □

donc $P(\sigma(a)) = 0$ pour tout $\sigma \in G$. En particulier, les éléments $\sigma_i(a)$ sont des racines de P, deux à deux distinctes, si bien que $\deg(P) \geqslant m$. Puisque $\deg(P) \leqslant [F : E]$, on en déduit que $m \leqslant [F : E]$. Cette inégalité valant pour tout entier m tel que $m \leqslant \mathrm{Card}(G)$, le groupe G est fini, et son cardinal vérifie $\mathrm{Card}(G) \leqslant [F : E]$.

Supposons que $\mathrm{Card}(G) = [F : E]$ et appliquons la construction précédente avec $m = [F : E]$. Il existe ainsi un polynôme irréductible $P \in E[T]$, de degré m, qui est scindé à racines simples dans F. Soit a une racine de P dans F. Comme P est irréductible, la sous-extension $E(a)$ de F engendrée par a est de degré m, donc est égale à F. Par suite, F est une extension de décomposition de P. Cela prouve l'implication (i)⇒(ii).

L'implication (ii)⇒(iii) est évidente.

Démontrons l'implication (i)⇒(iv). Soit $E' = F^G$. A priori, on a une inclusion $\mathrm{Aut}_{E'}(F) \subset \mathrm{Aut}_E(F) = G$, mais, par définition de E′, tout E-automorphisme de F est E′-linéaire, de sorte que $\mathrm{Aut}_{E'}(F) = G$. D'après la première partie du théorème, appliquée à l'extension $E' \subset F$, on a donc $\mathrm{Card}(G) \leqslant [F : E']$. Puisque $\mathrm{Card}(G) = [F : E] = [F : E'][E' : E]$, on a donc $[E' : E] = 1$, d'où $E' = E$.

Démontrons l'implication (iv)⇒(iii). Soit A une partie finie de F telle que $F = E(A)$; quitte à adjoindre à A les éléments $\sigma(a)$, pour $\sigma \in G$ et $a \in A$, on suppose que A est stable par G. Posons alors $P = \prod_{a \in A}(T - a)$. C'est un polynôme à coefficients dans F, scindé dans F, et ses racines engendrent F comme extension de E. Comme A est stable par G, on a $\sigma(P) = P$ pour tout $\sigma \in G$, de sorte que les coefficients de P appartiennent à F^G. Puisque $E = F^G$, on a donc $P \in E[T]$ et F est une extension de décomposition de P.

Démontrons que (iii)⇒(i). Soit $P \in E[T]$ un polynôme séparable dont F est une extension de décomposition et soit A l'ensemble des racines de P dans F. Démontrons par récurrence sur le cardinal d'une partie B de A que l'ensemble des E-morphismes de $E(B)$ dans F est de cardinal $[E(B) : E]$. C'est vrai si $B = \varnothing$, car $E(B) = E$. Supposons le résultat vrai pour B et soit alors $a \in A - B$. Par restriction à $E(B)$, un E-morphisme de $E(B \cup \{a\})$ dans F définit un E-morphisme de $E(B)$ dans F. Inversement, soit $f : E(B) \to F$ un E-morphisme et cherchons à le prolonger à $E(B \cup \{a\})$. Soit Q le polynôme minimal de a sur $E(B)$; c'est un diviseur de P dans $E(B)[T]$. En particulier, il est séparable et scindé dans F et chacune de ses racines dans F fournit un E-homomorphisme de $E(B \cup \{a\})$ dans F qui prolonge f. Par récurrence, on a donc $\mathrm{Card}(\mathrm{Hom}_E(F, F)) =$

Lemme **(1.3.7)**. — *Soit* A *un anneau et soit* M *un* A*-module à gauche. Pour tout* $m \in M$, *on* $a \cdot (-m) = (-1) \cdot m$ *et* $0 = 0 \cdot m$.

La preuve est laissée en exercice.

Lorsque l'anneau A est un corps, on parle d'*espace vectoriel* (à gauche ou à droite).

1.3.8. Algèbres. — Soit K un anneau commutatif. Une K-algèbre est un ensemble A muni de deux lois internes + et ·, et d'une multiplication externe de $K \times A$ dans A, vérifiant les propriétés suivantes :

– Le magma $(A, +)$ est un groupe abélien et la multiplication externe en fait un K-module ;

– La multiplication interne · de A est bilinéaire : on a $(am + bn) \cdot p = a(m \cdot p) + b(n \cdot p)$ et $m \cdot (an + bp) = a(m \cdot n) + b(m \cdot p)$ pour tous $a, b \in A$ et tous $m, n, p \in M$.

On dit que l'algèbre A est associative (*resp.* commutative, *resp.* unifère) si le magma $(A, \cdot)$ est associatif (*resp.* commutatif, *resp.* unifère).

Exemple : les matrices carrées de taille fixée à coefficients dans un corps commutatif K donné forment une K-algèbre associative et unifère (non commutative si la taille est > 1).

1.3.9. Algèbres de Lie. — Même s'il restera exotique dans ce cours, voici un exemple très important d'algèbre ; il devrait éclairer quelques exercices.

On dit que l'algèbre A est une *algèbre de Lie* si sa multiplication interne, notée $(a, b) \mapsto [a, b]$ et appelée *crochet*, vérifie les deux relations :

– On a $[a, a] = 0$ pour tout $a \in A$;

– On a $[[a, b], c] + [[b, c], a] + [[c, a], b] = 0$ pour tous $a, b, c \in A$ (identité de Jacobi).

Exemple : les matrices carrées de taille donnée à coefficients dans un corps commutatif fixé K, munies du « crochet de Lie » donné par $[A, B] = AB - BA$.

1.4. Catégories

Les catégories sont une sorte de structure algébrique très utile pour exprimer les interactions entre les diverses structures mathématiques usuelles.

1.4.1. Catégories. — Une *catégorie* C est la donnée :

– D'un ensemble X ;
– Pour tout couple (x, y) d'éléments de X, d'un ensemble $C(x, y)$;
– Pour tout $x \in X$, d'un élément 1_x de $C(x, x)$;
– Et pour tous x, y, z dans X, d'une loi $C(x, y) \times C(y, z) \to C(x, z)$;

vérifiant les deux propriétés suivantes :

– On a $u \cdot (v \cdot w) = (u \cdot v) \cdot w$ pour tous $x, y, z, t \in X$, tout $u \in C(x, y)$, $v \in C(y, z)$ et $w \in C(z, t)$ (associativité) ;
– On a $u \cdot 1_y = u = 1_x \cdot u$ pour tous $x, y \in X$ et tout $u \in C(x, y)$ (élément neutre).

L'ensemble X est noté $ob(C)$; ses éléments sont appelés objets de C ; les éléments de $C(x, y)$ sont appelés flèches de C de source x et terme y.

On peut observer que pour tout $x \in X$, la loi de composition de C fait de l'ensemble $C(x, x)$ un monoïde.

1.4.2. Quasi-exemples fondamentaux. — On prend pour X un ensemble d'ensembles et si x, y sont des éléments de X, on note $C(x, y)$ l'ensemble des applications de x dans y et 1_x l'application identique de X. Si x, y, z sont des ensembles, u une application de x dans y et v une application de y dans z, La loi de composition est donnée par $u \cdot v = v \circ u$.

À partir de cette exemple, les possibilités d'élaboration ne manquent pas. On peut prendre pour X un ensemble d'espaces topologiques, et, si $x, y \in X$, prendre pour $C(x, y)$ l'ensemble des applications continues de x dans y, avec la même loi de composition que précédemment.

Ou encore prendre pour X un ensemble d'espaces vectoriels sur un corps commutatif K fixé, et, pour $x, y \in X$, prendre pour $C(x, y)$ l'ensemble des applications linéaires de x dans y.

1.4.3. Grosses catégories. — En pratique, on voudrait prendre pour X « l'ensemble de tous les ensembles », etc., avec le souci que cet ensemble n'existe pas, comme le rappelle le paradoxe de Russell (théorème 1.1.2), pas plus que n'existe l'ensemble de tous les espaces topologiques... Il y a plusieurs voies pour résoudre cette difficulté, notamment :

– Se cantonner à une méta-mathématique où l'« ensemble » X n'est jamais jamais considéré comme ensemble ;

coïncident avec $g \circ f$ sur F et appliquent T sur T. On en déduit en particulier un homomorphisme de monoïdes de $\mathrm{Hom}(F, F)$ dans $\mathrm{Hom}(F[T], F[T])$ et un homomorphisme de groupes de $\mathrm{Aut}(F)$ dans $\mathrm{Aut}(F[T])$.

Si F et F′ sont des extensions de E et $f : F \to F'$ est un morphisme d'extensions, alors f' est un morphisme de E-algèbres. L'application $f \mapsto f'$ définit donc un homomorphisme de monoïdes de $\mathrm{Hom}_E(F, F)$ dans $\mathrm{Hom}_E(F[T], F[T])$ et un homomorphisme de groupes de $\mathrm{Aut}_E(F)$ dans $\mathrm{Aut}_E(F[T])$.

Pour $P = \sum_{m=0}^{n} c_m T^m \in F[T]$, on a $f'(P) = \sum_{m=0} f(c_m) T^m$. Pour $a \in F$, on a ${}^f P(f(a)) = f(P(a))$; en particulier, si a est racine de P, alors $f(a)$ est racine de ${}^f P$.

4.5.4. — Si E est un sous-corps de F et $P \in E[T]$, on a ${}^f P = P$. En particulier, l'ensemble des racines dans F d'un polynôme $P \in E[T]$ est invariant par tout élément de $\mathrm{Aut}_E(F)$.

Soit P un polynôme unitaire de $F[T]$ et soit $P = P_1 \dots P_r$ sa décomposition en facteurs irréductibles unitaires. Alors $\sigma(P) = \sigma(P_1) \dots \sigma(P_r)$. Pour qu'il existe une permutation τ de $\{1, \dots, r\}$ telle que $\sigma(P_i) = P_{\tau(i)}$ pour tout i, il faut et il suffit que $\sigma(P) = P$, c'est-à-dire que les coefficients de P soient fixés par σ. C'est en particulier le cas si P est scindé à racines simples dans P et si l'ensemble de ses racines est stable par σ.

Théorème **(4.5.5).** — *Soit* E *un corps commutatif, soit* F *une extension finie de* E *et soit* $G = \mathrm{Aut}_E(F)$ *Alors,* $\mathrm{Card}(G) \leqslant [F : E]$. *De plus, les conditions suivantes sont équivalentes :*

(i) *On a* $\mathrm{Card}(G) = [F : E]$;
(ii) *Il existe un polynôme irréductible et séparable* $P \in E[T]$ *tel que* $\deg(P) = [F : E]$ *qui est scindé dans* F ;
(iii) *L'extension* F *de* E *est une extension de décomposition d'un polynôme séparable de* $E[T]$;
(iv) *On a* $E = F^G$.

Démonstration. — Démontrons que $\mathrm{Card}(G) \leqslant [F : E]$. Soit $m \in \mathbf{N}$ tel que $m \leqslant \mathrm{Card}(G)$ et soit $\sigma_1, \dots, \sigma_m$ des éléments de G, deux à deux distincts. Pour tout couple (i, j) d'éléments de $\{1, \dots, n\}$ tels que $i < j$, l'ensemble $F_{i,j}$ des éléments $a \in F$ tels que $\sigma_i(a) = \sigma_j(a)$ est une sous-extension de F, distincte de F car $\sigma_i \neq \sigma_j$. D'après la proposition 4.5.1, il existe un élément $a \in F$ tel que $\sigma_i(a) \neq \sigma_j(a)$ si $i \neq j$. Soit P le polynôme minimal de a sur E. On a $P(a) = 0$,

4.5. Théorie de Galois

Proposition **(4.5.1).** — *Soit* E *un corps commutatif et soit* F *une extension finie de* E. *Soit* $(F_1, \dots, F_m)$ *une suite finie de sous-extensions de* F *telle que* $F = \bigcup_{i=1}^{m} F_i$. *Il existe alors* $i \in \{1, \dots, m\}$ *tel que* $F = F_i$.

Démonstration. — Supposons d'abord que E soit fini. Posons alors $q = \mathrm{Card}(E)$ et $d = [F : E]$. Le cardinal d'un sous-corps de F qui contient E est de la forme q^d, où d est un diviseur de n ; de plus, pour tout diviseur d de n, F contient exactement un tel sous-corps (l'ensemble des racines du polynôme $T^{q^d} - T$ dans F). Supposons les F_i deux à deux distincts, et distincts de F et posons $d_i = [F_i : E]$; les entiers d_i sont deux à deux distincts. Comme o appartient à chaque F_i, on a donc

$$\mathrm{Card}(\bigcup_{i=1}^{m} F_i) < \sum_{i=1}^{m} q^{d_i} \leqslant \sum_{d=1}^{n-1} q^d < q^n,$$

de sorte que $\bigcup_{i=1}^{m} F_i \neq F$.

On suppose maintenant que E est infini. Supposons $F_i \neq F$ pour tout i et démontrons par récurrence que $F \neq \bigcup_{i=1}^{m} F_i$. C'est évident si $m = 1$. Par récurrence, on peut aussi supposer qu'il existe un élément $a \in F$ tel que $a \notin \bigcup_{i=2}^{m} F_i$. Soit aussi $b \in F - F_1$. Soit $x, y \in E$ tels que $x \neq y$, et soit $i \in \{1, \dots, m\}$; au moins l'un des deux éléments, $a + xb$ ou $a + yb$, n'appartient pas à F_i, car sinon $(y - x)a = y(a + xb) - x(a + yb) \in F_i$, et $(y - x)b = (a + xb) - (a + yb) \in F_i$; comme $x \neq y$, on en déduit $a \in F_i$ et $b \in F_i$, ce qui contredit les choix de a (si $2 \leqslant i \leqslant m$) et b (si $i = 1$). Ainsi, l'ensemble des éléments $x \in E$ tels que $a + xb \in \bigcup_{i=1}^{m} F_i$ est de cardinal $\leqslant m$, d'où le lemme puisque E est infini. □

4.5.2. — Soit E un corps commutatif et soit F une extension de E. On note $\mathrm{Aut}_E(F)$, ou $\mathrm{Aut}(F/E)$, l'ensemble des automorphismes de F comme E-algèbre. C'est un sous-groupe de l'ensemble des permutations de F.

Soit G un sous-ensemble de $\mathrm{Aut}_E(F)$ et posons $F^G = \{a \in F ;\ \sigma(a) = a\ \forall \sigma \in G\}$. C'est une sous-extension de F.

4.5.3. — Soit $f : F \to F'$ un morphisme de corps commutatifs. Il existe un unique morphisme d'anneaux $f' : F[T] \to F'[T]$ tel que $f'(a) = f(a)$ pour $a \in F$ et $f'(T) = T$. On notera $f(P)$, ou ${}^f P$ l'image d'un polynôme P par cet automorphisme f'. Si F'' est un corps commutatif et $g : F' \to F''$ un morphisme de corps, on a $(g \circ f)' = g' \circ f'$ car ces deux homomorphismes de $F[T]$ dans $F''[T]$

– Considérer des ensembles d'ensembles assez gros (« univers de Grothendieck ») ;

– Considérer une axiomatique des mathématiques à plusieurs étages (ensembles, classes, etc.) qui permette de considérer la classe de tous les ensembles, etc ;

Chacune de ces solutions présente avantages et inconvénients ; dans ce cours, la première (la plus naïve) nous suffira largement.

1.4.4. Groupoïdes. — On dit qu'une catégorie C est un groupoïde si pour tout couple (x, y) d'objets et tout $u \in C(x, y)$ il existe $v \in C(y, x)$ tel que $u \cdot v = 1_x$ et $v \cdot u = 1_y$.

Dans ce cas, pour tout objet x de C, l'ensemble $C(x, x)$ muni de la loi de composition de la catégorie C est un groupe.

1.4.5. Groupoïde fondamental. — On définit en topologie algébrique le groupoïde de Poincaré ϖ_X d'un espace topologique X. Pour $x, y \in X$, on définit $\varpi_X(x, y)$ comme l'ensemble des « classes d'homotopie stricte »de chemins d'origine x et de terme y dans X, c'est-à-dire d'applications continues c de l'intervalle $[0, 1]$ dans X telles que $c(0) = x$ et $c(1) = y$. Par classe d'homotopie stricte, on entend qu'on identifie deux applications c et c' s'il existe une application continue $f : [0, 1] \times [0, 1] \to X$ telle que $f(0, t) = c(t)$, $f(1, t) = c'(t)$, $f(t, 0) = x$ et $f(t, 1) = y$ pour tout $t \in [0, 1]$. Pour $x, y, z \in X$, la loi de composition $\varpi_X(x, y) \times \varpi_X(y, z) \to \varpi_X(x, z)$ associe aux classes de $c : [0, 1] \to X$ et $c' : [0, 1] \to X$ (vérifiant $c(0) = x$, $c(1) = c'(0) = y$ et $c'(1) = z$) la classe de l'application $c * c'$ donnée par $t \mapsto c(2t)$ si $0 \leqslant t \leqslant \frac{1}{2}$ et $t \mapsto c'(2t - 1)$ si $\frac{1}{2} \leqslant t \leqslant 1$.

On vérifie que c'est une catégorie, l'élément neutre 1_x étant la classe du chemin constant de valeur x. De plus, pour tout chemin c d'origine x et de terme y, le chemin $\bar{c}$ donné par $t \mapsto c(1 - t)$ est d'origine y, de terme x et les classes des chemins $c * \bar{c}$ et $\bar{c} * c$ sont respectivement égales à 1_x et 1_y. Autrement dit, toute classe possède un inverse à droite et à gauche et la catégorie ϖ_X est un groupoïde, le *groupoïde de Poincaré* de l'espace topologique X.

1.4.6. Foncteurs. — Soit C et D des catégories. Un foncteur $F : C \to D$ est la donnée :

– D'une application $F : \mathrm{ob}(C) \to \mathrm{ob}(D)$;

– Pour tout couple (x, y) d'objets de C, d'une application $F : C(x, y) \to D(F(x), F(y))$

vérifiant les propriétés suivantes :

– Pour tout $x \in \mathrm{ob}(C)$, on a $F(1_x) = 1_{F(x)}$;
– Pour tous $x, y, z \in \mathrm{ob}(C)$, tout $u \in C(x, y)$ et tout $v \in C(y, z)$, on a $F(u \cdot v) = F(u) \cdot F(v)$.

1.5. Exercices

Exercice **(1.5.1)**. — Soit A et B des ensembles.

a) Soit E l'ensemble des couples (S, f) où S est une partie de A et $f : S \to B$ une application injective. On munit E de la relation d'ordre pour laquelle $(S, f) \preceq (S', f')$ si $S \subset S'$ et $f'|_S = f$. Démontrer que l'ensemble ordonné E est inductif, donc possède un élément maximal.

b) En considérant un élément maximal de E, démontrer qu'il existe une injection de A dans B ou une injection de B dans A.

c) (Théorème de Cantor-Bernstein) On suppose qu'il existe des injections $f : A \to B$ et $g : B \to A$. On définit des ensembles (A_n) et (B_n) par récurrence sur n en posant $A_0 = A$, $B_0 = B$, et, pour $n \geqslant 0$, $A_{n+1} = g(B_n)$ et $B_{n+1} = f(A_n)$; on pose aussi $A_n^* = A_n - A_{n+1}$ et $B_n^* = B_n - B_{n+1}$; soit enfin $A_\infty = \bigcap_{n\in\mathbf{N}} A_n$ et $B_\infty = \bigcap_{n\in\mathbf{N}} B_n$. Démontrer que f et g induisent des bijections de A_n^* sur B_{n+1}^* et de B_n^* sur A_{n+1}^* respectivement ; démontrer que f induit une bijection de A_∞ sur B_∞. En déduire qu'il existe une bijection de A sur B.

Exercice **(1.5.2)**. — La théorie des ensembles définit, pour tout ensemble A, un ensemble $\mathrm{Card}(A)$ qui est équipotent à A et tel que $\mathrm{Card}(A) = \mathrm{Card}(B)$ si et seulement si A et B sont équipotents. On appelle *cardinal* un ensemble de la forme $\mathrm{Card}(A)$.

a) Soit α et β des cardinaux. On note $\alpha \leqslant \beta$ s'il existe une injection de α dans β. Démontrer que la relation $\leqslant$ est un relation d'ordre total sur les cardinaux.

b) Démontrer que tout ensemble de cardinaux est majoré.

c) Démontrer que tout ensemble non vide de cardinaux possède un plus petit élément.

4.4.5. — Soit E un corps fini et soit p sa caractéristique. Soit $\Phi : E \to E$ l'application définie par $\Phi(x) = x^p$; c'est un homomorphisme de corps (homomorphisme de Frobenius). Il est injectif ; comme E est fini, il est aussi surjectif.

Notons que pour tout entier $n \geqslant 0$, on a $\Phi^n(x) = x^{p^n}$ pour tout $x \in E$.

4.4.6. — Soit F un corps fini, soit E son sous-coprps premier. Soit p sa caractéristique, q le cardinal de F et $n = [F : E]$. D'après ce qui précède, E est isomorphe à $\mathbf{Z}/p\mathbf{Z}$ et l'on a $q = p^n$.

Le groupe multiplicatif $F^\times$ de F est cyclique (théorème 2.9.6) et de cardinal $q-1$. En particulier, on a $x^{q-1} = 1$ pour tout $x \in F^\times$, donc $x^q = x$ pour tout $x \in F$. Le polynôme $T^q - T \in E[T]$ possède q racines (deux à deux distinctes), dans F ; comme il est de degré q, il est séparable et scindé dans F :

$$T^q - T = \prod_{a\in F}(T - a).$$

Cela montre aussi que F est une extension de décomposition du polynôme $T^q - T$ de $E[T]$.

4.4.7. — Inversement, soit p un nombre premier, soit $E = \mathbf{Z}/p\mathbf{Z}$, soit n un entier $\geqslant 1$, soit $q = p^n$ et soit F une extension de décomposition du polynôme $T^q - T$ de $E[T]$. Soit F_1 le sous-corps de F formé des éléments $a \in F$ tels que $a^q = a$; si Φ désigne l'homomorphisme de Frobenius de F, alors F_1 est le sous-corps de F fixé par l'homomorphisme Φ^n. Ainsi, F_1 est l'ensemble des racines du polynôme $T^q - T$ dans F ; puisque F est engendré par cet ensemble, on a donc $F_1 = F$. Le polynôme $T^q - T$ est séparable, car sa dérivée est égale à $qT^{q-1} - 1 = -1$ est première à $T^q - T$. On a donc $\mathrm{Card}(F) = q$ et F est un corps fini de cardinal q.

Théorème **(4.4.8)**. — *Soit* F *un corps fini. Alors* F *est commutatif, il existe un nombre premier* p *et un entier* $n \geqslant 1$ *tels que* $\mathrm{Card}(F) = p^n$, *et* F *est une extension de décomposition du polynôme* $T^{p^n} - T$ *de* $(\mathbf{Z}/p\mathbf{Z})[T]$.

Inversement, soit tout nombre premier p *et tout entier* $n \geqslant 1$, *toute extension de décomposition du polynôme* $T^{p^n} - T$ *de* $(\mathbf{Z}/p\mathbf{Z})[T]$ *est un corps fini de cardinal* p^n.

Soit q *un entier tel* $1 \leqslant q \leqslant \mathrm{Card}(F)$; *pour qu'il existe un sous-corps* E *de* F *de cardinal* q, *il faut et il suffit qu'il existe un entier* d *divisant* n *tel que* $q = p^d$; *alors* E *est l'ensemble des racines du polynôme* $T^q - T$ *dans* F.

Par récurrence, on déduit de cette relation que $\Phi_n \in \mathbf{Z}[T]$ pour tout $n \in \mathbf{N}^*$: c'est vrai pour $n = 1$; si c'est vrai pour tout entier <n, alors $P = \prod_{\substack{d|n \\ d<n}} \Phi_d$ est un polynôme unitaire de $\mathbf{Z}[T]$ qui divise $T^n - 1$ dans $\mathbf{C}[T]$, et le quotient est égal à Φ_n ; d'après le théorème de division euclidienne, on a $\Phi_n \in \mathbf{Z}[T]$.

Théorème **(4.4.4)** (Wedderburn). — *Tout corps fini est commutatif.*

a) *Démonstration.* — Soit F un corps fini. Notons Z son centre ; c'est un sous-corps de F ; posons $q = \mathrm{Card}(Z)$ et $n = \dim_Z(F)$; on a donc $\mathrm{Card}(F) = q^n$. Pour tout $a \in F$, notons Z_a le centralisateur de a dans F, ensemble des $x \in F$ tels que $xa = ax$; c'est un sous-corps de F qui contient Z ; notons $n_a = \dim_Z(Z_a)$ et $m_a = \dim_{Z_a}(F)$. On a donc $n_a m_a = n$; si $a \notin Z$, alors $Z_a \neq F$, donc $n_a < n$.

Écrivons l'équation aux classes dans le groupe multiplicatif $F^\times$. Par définition, pour tout $a \in F^\times$, le centralisateur de a dans le groupe $F^\times$ est égal à $Z_a^\times$; de même, le centre du groupe $F^\times$ est égal à $Z^\times$. Soit A une partie de $F^\times$ qui contient exactement un élément de chaque classe de conjugaison de cardinal $\geqslant 2$. On a donc

$$\mathrm{Card}(F^\times) = \mathrm{Card}(Z^\times) + \sum_{a \in A} \frac{\mathrm{Card}(F^\times)}{\mathrm{Card}(Z_a^\times)},$$

soit encore

$$q^n - 1 = q - 1 + \sum_{a \in A} \frac{q^n - 1}{q^{n_a} - 1}.$$

Comme n_a divise n et $n_a \neq n$, on a la relation suivante entre polynômes cyclotomiques :

$$T^n - 1 = \prod_{d|n} \Phi_d = \prod_{d|n_a} \Phi_d \prod_{\substack{d|n \\ d \nmid n_a}} \Phi_d = (T^{n_a} - 1)\Phi_n \prod_{\substack{d|n \\ d \nmid n_a \\ d<n}} \Phi_d.$$

En évaluant cette égalité en q, on en déduit que $(q^n - 1)/(q^{n_a} - 1)$ est multiple de $\Phi_n(q)$. Dans l'équation aux classes

$$q^n - 1 = q - 1 + \sum_{a \in A} \frac{q^n - 1}{q^{n_a} - 1},$$

tous les termes de la somme sur A sont donc multiples de $\Phi_n(q)$, ainsi que le membre de gauche. Par suite, $q - 1$ est multiple de $\Phi_n(q)$.

Si $n > 1$, chaque racine ξ de Φ_n vérifie $|q - \xi| > q - 1$, si bien que $|\Phi_n(q)| > (q-1)^{\varphi(n)} > q - 1$, ce qui contredit le fait que $q - 1$ soit multiple de $\Phi_n(q)$. On a donc $n = 1$ et $F = Z$ est un corps commutatif. □

Exercice **(1.5.3)**. — *a*) Soit A un ensemble et soit $f : A \to \mathfrak{P}(A)$ une application de A dans l'ensemble $\mathfrak{P}(A)$ des parties de A. Soit B l'ensemble des éléments $a \in A$ tels que $a \notin f(a)$. Démontrer que B n'appartient pas à l'image de f.

b) En déduire que l'ensemble $\mathfrak{P}(A)$ n'est pas équipotent à A.

Exercice **(1.5.4)** (Théorème de Knaster-Tarski). — On appelle treillis complet un ensemble ordonné A tel que toute partie de A possède une borne inférieure et une borne inférieure.

a) Démontrer que l'ensemble $[0, 1]$ (muni de la relation d'ordre usuelle des nombre réels) est un treillis complet.

b) Démontrer que l'ensemble des parties d'un ensemble, muni de la relation d'inclusion, est un treillis complet.

c) Démontrer que l'ensemble des sous-groupes d'un groupe, muni de la relation d'inclusion, est un treillis complet.

d) Démontrer qu'un treillis complet possède un plus petit et un plus grand élément.

e) Soit A un treillis complet, soit a, b des éléments de A tels que $a \leqslant b$ et soit $B = [a, b] = \{x \in A\,;\, a \leqslant x \leqslant b\}$. Démontrer que B est un treillis complet.

f) Démontrer que dans la définition d'un treillis complet, il suffit de supposer que toute partie de A possède une borne inférieure (*resp.* une borne supérieure).

g) Soit A un treillis complet et soit $f : A \to A$ une application monotone. Soit P l'ensemble des points-fixe de f, muni de la relation d'ordre induite par celle de A.

Soit S l'ensemble des $a \in A$ tels que $a \leqslant f(a)$; démontrer que $f(S) \subset S$. Soit s la borne supérieure de S ; démontrer que s est le plus grand point fixe de f.

h) (*suite*) Soit Q une partie de P, soit q sa borne supérieure de Q dans A et soit $a = \max(A)$. Démontrer que $f([q, a]) \subset [q, a]$. En déduire que f possède un plus petit point fixe appartenant $[q, a]$ qui est la borne supérieure de Q dans P.

i) (*suite*) Démontrer que P est un treillis complet.

Exercice **(1.5.5)** (Théorème de Zermelo). — Le théorème de Zermelo (1904) affirme que sur tout ensemble, il existe un bon ordre.

a) Déduire l'axiome du choix du théorème de Zermelo.

b) Déduire le théorème de Zorn du théorème de Zermelo. (*Soit* A *un ensemble ordonné; choisir un ensemble* I, *par exemple* $\mathrm{I} = \mathscr{P}(\mathrm{A})$, *tel qu'il n'existe pas de surjection de* A *sur* I *et le munir d'un bon ordre; définir alors par récurrence transfinie une suite strictement croissante maximale* $(a_i)_{i\in\mathrm{J}}$, *où* J *est un segment initial de* I; *démontrer que* J *n'a pas de plus grand élément; en déduire que l'ensemble* A *n'est pas inductif.*)

c) Utiliser le théorème de Zorn pour démontrer le théorème de Zermelo. (*Soit* A *un ensemble; considérer l'ensemble* $\mathscr{Z}$ *des couples* $(\mathrm{V}, \preceq_{\mathrm{V}})$, *où* V *est une partie de* A *et* $\preceq_{\mathrm{V}}$ *un bon ordre sur* V *et définir une relation* $(\mathrm{V}, \preceq_{\mathrm{V}}) \leqslant (\mathrm{W}, \preceq_{\mathrm{W}})$ *dans* $\mathscr{Z}$ *par « V est un segment initial de* W, *muni de l'ordre induit »; prouver que c'est une relation d'ordre pour laquelle* $\mathscr{Z}$ *est inductif; considérer un élément maximal* $(\mathrm{V}, \preceq_{\mathrm{V}})$ *de* $\mathscr{Z}$ *et démontrer que* V = A.)

Exercice **(1.5.6)** (Ordinaux de von Neumann). — On dit qu'un ensemble bien ordonné A est un *ordinal* si pour tout $a \in \mathrm{A}$, on a l'égalité $a = \{x \in \mathrm{A};\ x \prec a\}$.

a) Soit A un ordinal; soit a, b des éléments de A. Démontrer que l'on a $a \preceq b$ si et seulement si $a \subset b$.

b) Soit A un ordinal. Démontrer que $\mathrm{A}^+ = \mathrm{A} \cup \{\mathrm{A}\}$, muni de la relation d'inclusion, est un ordinal.

c) Soit A et B deux ordinaux. Démontrer que l'on a $\mathrm{A} \subset \mathrm{B}$ ou $\mathrm{B} \subset \mathrm{A}$.

d) Démontrer que toute famille non vide d'ordinaux possède un plus petit élément. (« Pour la relation d'inclusion, les ordinaux sont bien ordonnés. »)

e) Démontrer que toute famille d'ordinaux possède une borne supérieure.

f) Démontrer que $\varnothing$ est un ordinal. Quels sont les ordinaux finis ? Quel est le plus petit ordinal infini ?

g) Soit S un ensemble bien ordonné. Démontrer qu'il existe une unique ordinal qui est isomorphe à S.

Exercice **(1.5.7)**. — Soit $(\mathrm{A}, \cdot)$ un monoïde.

a) Démontrer que la loi de composition donnée par $a * b = ba$ fait de A un monoïde; on l'appelle le monoïde opposé et on le note A^{o}.

b) Si A est un groupe, démontrer que A^{o} est un groupe et que l'application $a \mapsto a^{-1}$ est un isomorphisme du groupe A sur le groupe opposé A^{o}.

c) Donner un exemple de monoïde qui n'est pas isomorphe au monoïde opposé.

d'extensions $g : \mathrm{K}(a) \to \mathrm{F}'$ tel que $g|_{\mathrm{K}} = f$ et $g(a) = b$. Alors, $(\mathrm{K}, f) \prec (\mathrm{K}(a), g)$ et $\mathrm{K} \neq \mathrm{K}(a)$, ce qui contredit le caractère maximal de (K, f).

On a ainsi démontré qu'il existe un homomorphisme d'extensions $f : \mathrm{F} \to \mathrm{F}'$. Il reste à vérifier que f est surjectif. Soit $b \in \mathrm{F}'$ et soit $\mathrm{P} \in \mathrm{E}[\mathrm{T}]$ son polynôme minimal. Soit $n = \deg(\mathrm{P})$ et soit $\mathrm{P} = \prod_{i=1}^{n}(\mathrm{T} - a_i)$ la factorisation de P dans $\mathrm{F}[\mathrm{T}]$. On a donc $\mathrm{P} = \prod_{i=1}^{n}(\mathrm{T} - f(a_i))$ dans $\mathrm{F}'[\mathrm{T}]$. Puisque $\mathrm{P}(b) = 0$, il existe $i \in \{1, \ldots, n\}$ tel que $f(a_i) = b$; en particulier, b appartient à l'image de f. Cela démontre que f est surjective. □

4.4. Corps finis

Un *corps fini* est un corps de cardinal fini.

4.4.1. — Soit F un corps et soit E un sous-corps de E. Supposons que E soit commutatif et fini. Soit $d = \dim_{\mathrm{E}}(\mathrm{F})$ et soit $(a_1, \ldots, a_d)$ une base de F sur E. Tout élément de F s'écrit de manière unique $\sum_{i=1}^{d} x_i a_i$, avec $(x_i) \in \mathrm{E}^{(d)}$. Ainsi, d est fini si et seulement si F est un corps fini et l'on a $\mathrm{Card}(\mathrm{F}) = \mathrm{Card}(\mathrm{E})^{[\mathrm{F}:\mathrm{E}]}$.

4.4.2. — Soit E un corps fini. L'image de l'homomorphisme canonique de $\mathbf{Z}$ dans E étant finie, cet homomorphisme n'est pas injectif et son noyau est un idéal non nul (p) de $\mathbf{Z}$. Comme E est intègre, p est un nombre premier : *la caractéristique d'un corps fini est un nombre premier p, et le sous-corps premier de* E *est isomorphe à* $\mathbf{Z}/p\mathbf{Z}$.

4.4.3. — Pour tout entier d, notons Φ_d le d-ième *polynôme cyclotomique,* c'est-à-dire le polynôme unitaire de $\mathbf{C}[\mathrm{T}]$ dont les racines sont les racines primitives d-ièmes de l'unité, chacune avec multiplicité 1. Autrement dit, on a

$$\Phi_d = \prod_{\substack{a\in\mathbf{C}^\times \\ a \text{ est d'ordre } d}} (\mathrm{T} - a).$$

Ces racines sont les nombres complexes $\exp(2ik\pi/n)$, où $k \in \{1, \ldots, n\}$ est un entier premier à n. Par suite, on a $\deg(\Phi_d) = \varphi(d)$, l'indicateur d'Euler. On a par exemple $\Phi_1 = \mathrm{T} - 1$, $\Phi_2 = \mathrm{T} + 1$, $\Phi_3 = \mathrm{T}^2 + \mathrm{T} + 1$, etc.

Si $a \in \mathbf{C}$ vérifie $a^n = 1$, l'ordre d de a divise n et a est une racine primitive d-ième de l'unité. Par suite,

$$\mathrm{T}^n - 1 = \prod_{d|n} \Phi_d.$$

Ainsi, $I \neq A$. Soit M un idéal maximal de A qui contient I et soit Ω le corps A/M. C'est une extension de E dans laquelle tout polynôme irréductible de $E[T]$ est scindé.

D'après le lemme précédent, l'ensemble F des éléments de Ω qui sont algébriques sur E est une clôture algébrique de E.

Soit F et F′ des clôtures algébriques de E ; notons $j : E \to F$ et $j' : E \to F'$ les homomorphismes canoniques. Soit $\mathscr{E}$ l'ensemble des couples (K, f) où K est une sous-extension de F et $f : K \to F'$ est un homomorphisme de corps. La relation $(K, f) \prec (K', f')$ définie par « $K \subset K'$ et $f'|_K = f$ » est une relation d'ordre dans $\mathscr{E}$.

L'ensemble $\mathscr{E}$ contient le couple $(j(E), i)$, où soit $i : j(E) \to F'$ est l'unique application donnée par $j' \circ j^{-1}$.

Soit $\mathscr{A}$ une partie totalement ordonnée de $\mathscr{E}$; démontrons que $\mathscr{A}$ est majorée. C'est le cas si $\mathscr{A}$ est vide, car $\mathscr{E}$ n'est pas vide. Supposons maintenant que $\mathscr{A}$ ne soit pas vide. Soit L la réunion des corps K, pour $(K, f) \in \mathscr{A}$. Soit $a \in L$. Soit (K, f) et (K', f') deux couples de $\mathscr{A}$ tels que $a \in K$ et $a \in K'$. Par hypothèse, on a $K \subset K'$ et $f'|_K = f$, ou $K' \subset K$ et $f|_{K'} = f'$. Cela entraîne que $f(a) = f'(a)$. Il existe donc une unique application $g : L \to F'$ telle que $g(a) = f(a)$ pour tout $a \in L$ et tout couple (K, f) tel que $a \in K$.

Démontrons que L est une sous-extension de F et que g est un homomorphisme d'extensions. Par construction, L contient $j(E)$, et en particulier, il contient 0, 1. Pour tout $a \in j(E)$, on a $g(a) = i(a)$, donc $g \circ j = j'$. En particulier, $g(0) = 0$ et $g(1) = 1$. D'autre part, si $a, b \in L$, il existe deux couples (K, f) et (K', f') dans $\mathscr{A}$ tels que $a \in K$ et $b \in K'$. Puisque $\mathscr{A}$ est totalement ordonné, on a $K \prec K'$ ou $K' \prec K$. Supposons, pour fixer les idées, que $K' \prec K$. Alors, $a, b \in K$ et $f|_{K'} = f'$. Par suite, ab, $a + b$, $-a$ appartiennent à K, et donc à L, de même que $1/a$ si $a \neq 0$. Cela entraîne que que L est une sous-extension de F. De plus, $g(a + b) = f(a + b) = f(a) + f(b) = g(a) + g(b)$, et $g(ab) = f(ab) = f(a)f(b) = g(a)g(b)$ L'application g est donc un homomorphisme de corps. Puisque $g \circ j = j'$, c'est un morphisme d'extensions.

D'après le théorème de Zorn, l'ensemble $\mathscr{E}$ possède un élément maximal, disons (K, f). Supposons par l'absurde que $K \neq F$ et soit $a \in F - K$. Comme a est algébrique sur E, il est aussi algébrique sur K ; soit $P \in K[T]$ son polynôme minimal. Via le morphisme f, considérons F′ comme une extension de K. Par hypothèse, il existe $b \in F'$ tel que $P(b) = 0$. Il existe alors un homomorphisme

Exercice **(1.5.8)**. — Soit M un monoïde.

Démontrer que le produit de deux éléments inversibles à droite (*resp.* à gauche) est inversible à droite (*resp.* à gauche) et donner une formule pour un tel inverse.

Exercice **(1.5.9)**. — Dans chacun des monoïdes suivants, identifier l'ensemble des éléments inversibles à droite (*resp.* à gauche).

a) Le monoïde des applications d'un ensemble A dans lui-même.

b) Le monoïde des applications linéaires d'un **R**-espace vectoriel E dans lui-même. Cas de la dimension finie ?

c) Le monoïde des applications polynomiales de **R** dans **R**.

d) Le monoïde multiplicatif d'une K-algèbre associative de dimension finie, K étant un corps fixé (K = **R** ou **C**, si l'on veut).

Exercice **(1.5.10)**. — Soit M un monoïde commutatif ; on note + sa loi de composition et 0 son élément neutre.

a) Soit $\sim$ la relation dans $M \times M$ donnée par $(a, b) \sim (c, d)$ s'il existe $u \in M$ tel que $a + d + u = b + c + u$. Démontrer que c'est une relation d'équivalence.

b) On note A l'ensemble quotient et $[a, b]$ la classe d'un couple (a, b). Démontrer qu'il existe une unique loi de composition de A telle que $[a, b] + [c, d] = [a + c, b + d]$ pour $a, b, c, d \in M$. Démontrer que A est un groupe abélien et que l'application $j : M \to A$ donnée par $a \mapsto [a, 0]$ est un homomorphisme de monoïdes. Démontrer aussi que tout élément de A est la différence de deux éléments de $j(M)$.

c) Soit B un groupe et soit $f : M \to B$ un homomorphisme de monoïdes. Démontrer qu'il existe un unique homomorphisme de groupes $\varphi : A \to B$ tel que $\varphi \circ j = f$.

Exercice **(1.5.11)**. — Soit M un monoïde (non nécessairement commutatif).

a) Soit A un groupe et soit $j : M \to A$ un morphisme de monoïdes tel que $j(M)$ engendre A. Démontrer que $\mathrm{Card}(A) \leqslant \sup(\mathrm{Card}(\mathbf{N}), \mathrm{Card}(M))$.

b) Démontrer qu'il existe un ensemble Φ dont les éléments sont des couples (j, A), où A est un groupe et $j : M \to A$ un morphisme de monoïdes tel que $j(M)$ engendre A, qui vérifie la propriété suivante : Pour tout couple (f, B), où B est un groupe et $f : M \to B$ est un morphisme de monoïdes, il existe un couple $(j, A) \in \Phi$ et un morphisme $\varphi : A \to B$ tel que $\varphi \circ j = f$.

c) Démontrer qu'il existe un groupe A et un homomorphisme de monoïdes $j : M \to A$ vérifiant la propriété universelle : Pour tout groupe B et tout morphisme de monoïdes $f : M \to B$, il existe un unique morphisme de groupes $\varphi : A \to B$ tel que $\varphi \circ j = f$.

sur E. Soit $Q \in E[T]$ son polynôme minimal. C'est un multiple de P dans $F[T]$. Par hypothèse, le polynôme Q est scindé dans Ω ; en particulier, le polynôme P est scindé dans Ω. Soit $b \in \Omega$ une racine de P. Il existe un unique homomorphisme de F-algèbres $f : F' \to \Omega$ tel que $f(a) = b$. L'élément b est algébrique sur F, donc sur E; donc $b \in F$. Ainsi, $\deg(P) = 1$. □

Théorème **(4.3.6)** (Steinitz). — *Soit* E *un corps commutatif.*

a) *Le corps* E *possède une clôture algébrique.*
b) *Deux clôtures algébriques de* E *sont isomorphes.*

Démonstration. — Soit $\mathscr{P}$ l'ensemble des polynômes irréductibles unitaires de $E[T]$. Introduisons l'anneau A des polynômes en des indéterminées $T_{f,i}$, où $f \in \mathscr{P}$ et $1 \leqslant i \leqslant \deg(f)$. Pour tout $f \in \mathscr{P}$, on écrit

$$f - \prod_{i=1}^{\deg(f)} (T - T_{f,i}) = \sum_{i=1}^{\deg(f)} c_{f,i} T^{i-1}$$

dans l'anneau $A[T]$ des polynômes à coefficients dans A en l'indéterminée T. Soit I l'idéal de A engendré par ces éléments $c_{f,1}, \ldots, c_{f,\deg(f)}$, pour f parcourant $\mathscr{P}$.

Démontrons par l'absurde que $I \neq A$. Dans le cas contraire, il existe une famille presque nulle $(b_{f,i})$ d'éléments de A telle que $1 = \sum b_{f,i} c_{f,i}$. L'ensemble $\mathscr{P}_1$ des polynômes $g \in \mathscr{P}$ tels qu'il existe $j \in \{1, \ldots, \deg(g)\}$, $f \in \mathscr{P}$ et $i \in \{1, \ldots, \deg(f)\}$ tels que l'indéterminée $T_{g,j}$ apparaisse dans $c_{f,i}$ ou dans $b_{f,i}$ est fini ; soit P leur produit. Soit A_1 le sous-anneau de A des polynômes en les indéterminées $T_{g,j}$, pour $g \in \mathscr{P}_1$ et $1 \leqslant j \leqslant \deg(g)\}$, et soit I_1 l'idéal de A_1 engendré par les éléments $c_{g,1}, \ldots, c_{g,\deg(g)}$, pour g parcourant $\mathscr{P}_1$. Par construction, les éléments $b_{f,i}$ appartiennent à A_1, de même que les éléments $c_{f,i}$ tels que $b_{f,i} \neq 0$; ainsi, la relation $1 = \sum b_{f,i} c_{f,i}$ entraîne que $I_1 = A_1$.

Soit F une extension de décomposition du polynôme P. Par définition, le polynôme P est scindé dans F; en particulier, chaque polynôme g de $\mathscr{P}_1$ est scindé dans F. Pour tout $g \in \mathscr{P}_1$ et tout $j \in \{1, \ldots, \deg(g)\}$, il existe des éléments $a_{g,j} \in F$ tels que

$$g = \prod_{j=1}^{\deg(g)} (T - a_{g,j})$$

dans $F[T]$. Soit $\varphi : A_1 \to F$ l'unique homomorphisme de E-algèbres qui applique $T_{g,j}$ sur $a_{g,j}$, pour $g \in \mathscr{P}_1$ et $1 \leqslant j \leqslant \deg(g)$. On a donc $\varphi(c_{g,j}) = 0$ pour tous (g, j), d'où $I_1 \subset \mathrm{Ker}(\varphi)$, puis la contradiction $0 = \varphi(1) = 1$.

et de rayon R est compact et que la fonction $z \mapsto |P(z)|$ est continue sur $\mathbf{C}$, il existe $a \in \mathbf{C}$ tel que $|a| \leqslant R$ et

$$\inf_{\substack{z\in\mathbf{C}\\ |z|\leqslant R}} |P(z)| = |P(a)|.$$

En particulier, on a $|P(a)| \leqslant |P(0)| < |P(z)|$ pour tout $z \in \mathbf{C}$ tel que $|z| \geqslant R$. Cela entraîne que $|a| < R$.

Remarquons qu'il existe $b_0, \dots, b_n \in \mathbf{C}$ tels que

$$P = b_0 + b_1(T - a) + \cdots + b_n(T - a)^n.$$

On définit en effet b_n comme le quotient de la division euclidienne de P par $(T - a)^n$; comme $\deg(P) \leqslant n$, b_n est constant et le reste est un polynôme P_1 de degré $\leqslant n - 1$. On définit alors b_{n-1} comme le quotient de la division euclidienne de P par $(T - a)^{n-1}$, etc. Observons aussi que $b_n = c_n$.

Supposons par l'absurde que $P(a) \neq 0$. Alors, $b_0 = P(a) \neq 0$. Comme $b_n \neq 0$, il existe un plus petit entier $m \geqslant 1$ tel que $b_m \neq 0$, de sorte que $b_1 = \cdots = b_{m-1} = 0$. Soit θ_0 et θ_m des arguments de b_0 et b_m, de sorte que $b_0 = |b_0|e^{i\theta_0}$ et $b_m = |b_m|e^{i\theta_m}$. Définissons θ par la relation $\theta_0 + \pi = \theta_m + m\theta$. Lorsque $r \in \mathbf{R}_+$ tend vers 0, on a $|a + re^{i\theta}| < R$ et

$$P(a + re^{i\theta}) = b_0 + b_m e^{im\theta} r^m + o(r^m) = |b_0|(1 - \frac{b_m}{b_0} r^m + o(r^m),$$

donc $|P(a + re^{i\theta})| < |P(a)|$. Ceci contredit la définition de a. □

Définition **(4.3.4)**. — *Soit* E *un corps commutatif. On dit qu'une extension* F *de* E *est une* clôture algébrique *de* E *si c'est une extension algébrique et si le corps* F *est algébriquement clos.*

Proposition **(4.3.5)**. — *Soit* E *un corps commutatif, soit* Ω *une extension de* E *dans laquelle tout polynôme irréductible de* E[T] *est scindé (par exemple, une extension algébriquement close de* E*). Alors, l'ensemble* F *des éléments de* Ω *qui sont algébriques sur* E *est une clôture algébrique de* E.

Démonstration. — L'ensemble F est un sous-corps de Ω dont tout élément est algébrique sur E ; c'est donc une extension algébrique de E.

Considérons alors un polynôme irréductible $P \in F[T]$ et démontrons que $\deg(P) = 1$. Soit F′ une extension de rupture de P et $a \in F'$ tel que $P(a) = 0$. L'élément a est algébrique sur F, et F est algébrique sur E, donc a est algébrique

CHAPITRE 2

GROUPES

2.1. Définitions

Définition **(2.1.1)**. — *Un monoïde est un magma associatif et unifère. Un groupe est un monoïde dont tout élément est inversible. On dit qu'un monoïde (*resp. *un groupe) est commutatif, ou abélien, si sa loi de composition est commutative.*

La notation la plus courante pour la loi de composition d'un monoïde est le symbole ·, d'ailleurs le plus souvent omis ; dans ce cas, l'élément neutre est souvent noté e ou 1, et l'inverse d'un élément a est noté a^{-1}.

Dans le cas de monoïdes ou de groupes abéliens, on note aussi la loi + et l'élément neutre 0 ; l'inverse d'un élément a est alors appelé opposé et noté $-a$.

2.1.2. — Soit A un monoïde, d'élément neutre e. Pour tout entier naturel n et toute suite $(a_1, \dots, a_n)$ d'éléments de A, on définit le produit $\prod_{i=1}^n a_i = a_1 \dots a_n$ par récurrence de la façon suivante :

(2.1.2.1)
$$\prod_{i=1}^{n} a_i = \begin{cases} e & \text{si } n = 0 ; \\ a_1 \prod_{i=2}^{n} a_i & \text{si } n \geqslant 1. \end{cases}$$

Pour tout entier m tel que $0 \leqslant i \leqslant m$, on vérifie par récurrence sur m la formule

(2.1.2.2)
$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{m} a_i \prod_{i=m+1}^{n} a_i.$$

Lorsque le monoïde est commutatif et que sa loi est notée +, ce produit est appelé somme et noté $\sum_{i=1}^n a_i$. On a alors la formule supplémentaire

(2.1.2.3)
$$\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i,$$

pour $n \in \mathbf{N}$ et $a_1, \dots, a_n, b_1, \dots, b_n \in \mathrm{A}$.

2.1.3. — Soit A un monoïde et soit a un élément de A. Pour tout entier naturel n, on note a^n le produit de la suite $(a, \dots, a)$ (n termes). Si a est inversible, on définit a^n pour tout entier relatif n en posant $a^n = (a^{-1})^{-n}$ si $n < 0$.

On vérifie par récurrence que l'on a $a^{m+n} = a^m \cdot a^n$ et $(a^m)^n = a^{mn}$ pour tout couple (m, n) d'entiers naturels (*resp.* pour tout couple d'entiers relatifs si a est inversible).

2.1.4. — Soit A un monoïde. On dit que des éléments a, b de A *commutent* si l'on a $ab = ba$. On a alors $(ab)^n = a^n \cdot b^n$ pour tout entier naturel n et, lorsque A est un groupe, pour tout entier relatif n.

Lorsque A est un groupe, on appelle *commutateur* du couple (a, b) l'élément $[a, b] = a^{-1}b^{-1}ab$; il est égal à l'élément neutre si et seulement si les éléments a et b commutent.[(1)]

2.1.5. — Soit A un groupe et soit a un élément de A. On dit que a est d'ordre infini s'il n'existe pas d'entier naturel $n > 0$ tel que $a^n = e$; sinon, on appelle *ordre* de a le plus entier naturel $n > 0$ tel que $a^n = e$. Un élément d'ordre fini est aussi appelé élément de torsion ; on dit que A est sans torsion si son élément neutre est le seul élément de torsion.

Lemme **(2.1.6)**. — *Soit* A *un groupe.*

a) *Soit a un élément d'ordre fini de* A *et soit n son ordre. Si $m \in \mathbf{Z}$, alors $a^m = e$ si et seulement si m est multiple de n.*

b) *Supposons que* A *soit commutatif. Soit a et b des éléments de* A*, d'ordres m et n respectivement. Alors, ab est d'ordre fini, et cet ordre divise* $\mathrm{ppcm}(m, n)$ *; si m et n sont premiers entre eux, alors ab est d'ordre mn.*

Démonstration. — a) Soit $m = nq + r$ la division euclidienne de m par n, de sorte que $0 \leqslant r < n$. On a $e = a^m = a^{nq}a^r = (a^n)^q a^r = e^q a^r = a^r$. Par définition de l'ordre de a, l'entier n est le plus petit entier strictement positif tel que $a^n = e$. On a donc $r = 0$, ce qui prouve que m est multiple de n.

(1) Ni la notation, ni la définition ne sont très strictes ; les crochets sont parfois remplacés par des parenthèses ; d'autres auteurs le définissent par $aba^{-1}b^{-1}$.

de D. Comme P et P′ sont multiples de P, on a $\mathrm{P}(a) = \mathrm{P}'(a) = 0$. Si l'on écrit $\mathrm{P} = \sum_{m=0}^{n} c_n(\mathrm{T}-a)^n$, on a $\mathrm{P}(a) = c_0$ et $\mathrm{P}'(a) = c_1$; ainsi, P est multiple de $(\mathrm{T}-a)^2$, donc a est racine multiple de P. Cela entraîne que D n'a pas de racine dans F, donc $\mathrm{D} = 1$. □

4.3. Clôture algébrique

Définition **(4.3.1)**. — *Soit* E *un corps commutatif. On dit que* E *est* algébriquement clos *si tout polynôme irréductible de* $\mathrm{E}[\mathrm{T}]$ *possède une racine dans* E.

Lemme **(4.3.2)**. — *Soit* E *un corps commutatif. Les conditions suivantes sont équivalentes :*

(i) *Le corps* E *est algébriquement clos ;*
(ii) *Les polynômes irréductibles de* $\mathrm{E}[\mathrm{T}]$ *sont les polynômes de degré* 1 *;*
(iii) *Tout polynôme de* $\mathrm{E}[\mathrm{T}]$ *est scindé dans* E.

Démonstration. — (i)⇒(ii). Soit P un polynôme irréductible de $\mathrm{E}[\mathrm{T}]$. Comme P n'est pas inversible, on a $\deg(\mathrm{P}) \geqslant 1$. Par hypothèse, P possède une racine a dans E. Alors, $\mathrm{T} - a$ divise P, de sorte qu'il existe un polynôme $\mathrm{Q} \in \mathrm{E}[\mathrm{T}]$ tel que $\mathrm{P} = (\mathrm{T} - a)\mathrm{Q}$. Puisque P est irréductible et que $\mathrm{T} - a$ n'est pas inversible, Q est inversible, donc $\deg(\mathrm{Q}) = 0$, puis $\deg(\mathrm{P}) = 1$.

(ii)⇒(iii). Soit $\mathrm{P} \in \mathrm{E}[\mathrm{T}]$. Il n'y a rien à démontrer si $\mathrm{P} = 0$. Sinon, on peut décomposer P en produit de polynômes irréductibles, $\mathrm{P} = \mathrm{P}_1 \dots \mathrm{P}_n$. Par hypothèse, $\deg(\mathrm{P}_i) = 1$ pour tout i. Ainsi, P est scindé.

(iii)⇒(i). Soit P un polynôme irréductible de $\mathrm{E}[\mathrm{T}]$. Puisque P est scindé dans E, P est produit de facteurs de degré 1. Puisque $\deg(\mathrm{P}) \geqslant 1$, il possède au moins un facteur de degré 1 et donc une racine. □

Théorème **(4.3.3)** (« Théorème de d'Alembert–Gauß »)
Le corps $\mathbf{C}$ *des nombres complexes est algébriquement clos.*

Démonstration. — Il suffit de démontrer que tout polynôme non constant de $\mathbf{C}[\mathrm{T}]$ possède une racine dans $\mathbf{C}$. Soit P un tel polynôme, soit n son degré ; écrivons-le $\mathrm{P} = \sum_{m=0}^{n} c_m \mathrm{T}^m$, de sorte que $n \geqslant 1$ et $c_n \neq 0$. Pour $z \in \mathbf{C}$, on a $|\mathrm{P}(z)| \to +\infty$ lorsque $|z| \to +\infty$. Par suite, il existe un nombre réel $\mathrm{R} > 0$ tel que $|\mathrm{P}(z)| \geqslant 1 + |\mathrm{P}(0)|$ pour tout $z \in \mathbf{C}$ tel que $|z| \geqslant \mathrm{R}$. Puisque le disque de centre 0

Sinon, soit P_1 un facteur irréductible de P de degré $\geqslant 2$ et soit a une racine de P_1 dans F. Posons $E' = E(a)$; c'est une extension de E, isomorphe à $E[T]/(P_1)$. Soit b une racine de P_1 dans Ω ; il existe donc un unique homomorphisme d'extensions $f' : E' \to \Omega$ tel que $f'(a) = b$. Alors, l'homomorphisme f' permet de considérer le corps Ω comme une extension de E'. De même, E' est un sous-corps de F, donc on peut considérer F comme une extension de E'. On a $[E' : E] = \deg(P_1) \geqslant 2$, donc $[F : E'] < [F : E]$. Par récurrence, il existe un homomorphisme $f : F \to \Omega$ d'extensions de E' ; c'est un homomorphisme d'extensions de E. □

Corollaire **(4.2.7)**. — *Soit* E *un corps commutatif et soit* $P \in E[T]$ *un polynôme non constant. Deux extensions de* E *qui sont extensions de décomposition de* P *sont isomorphes.*

Démonstration. — Soit F et F' deux extensions de E qui sont extensions de décomposition de P. D'après la proposition 4.2.6, appliquée avec $\Omega = F'$, il existe un homomorphisme d'extensions $f : F \to F'$. Soit $n = \deg(P)$ et considérons une factorisation $P = c\prod_{i=1}^{n}(T - a_i)$ de P dans F. On a donc $P = f(c)\prod_{i=1}^{n}(T - f(a_i))$ dans $F'[T]$, ce qui prouve que l'ensemble $\{f(a_i)\}$ est l'ensemble des racines de P dans F'. Puisque F' est une extension de décomposition de P, $F' = E(f(a_1), \ldots, f(a_n))$, si bien que f est surjectif. On a ainsi prouvé que F et F' sont isomorphes. □

Définition **(4.2.8)**. — *Soit* E *un corps commutatif. Soit* $P \in E[T]$ *et soit* F *une extension de décomposition de* P. *On dit que le polynôme* P *est* séparable *si ses racines dans* F *sont toutes simples.*

Cela ne dépend pas du choix de l'extension de décomposition.

Proposition **(4.2.9)**. — *Soit* E *un corps commutatif. Pour qu'un polynôme* $P \in E[T]$ *soit séparable, il faut et il suffit que l'on ait* $\operatorname{pgcd}(P, P') = 1$.

Démonstration. — Soit F une extension de décomposition de P. Supposons que $\operatorname{pgcd}(P, P') = 1$ et soit $U, V \in E[T]$ des polynômes tels que $UP + VP' = 1$. Soit $a \in F$ une racine de P et soit m sa multiplicité ; supposons par l'absurde que $m \geqslant 2$. Alors $(T - a)^m$ divise P, donc $(T - a)^{m-1}$ divise P' et a est racine commune à P et P'. On a ainsi $1 = U(a)P(a) + V(a)P'(a) = 0$; contradiction ! Cela démontre que toutes les racines de P sont simples.

Supposons maintenant que toutes les racines de P soient simples. Soit $D = \operatorname{pgcd}(P, P')$; comme c'est un diviseur de P, il est scindé dans F. Soit a une racine

b) Soit $p = \operatorname{ppcm}(m, n)$; comme m divise p, on a $a^p = e$; comme n divise p, on a $b^p = e$. Comme A est commutatif, on a $(ab)^p = a^p b^p = e$, ce qui prouve que ab est d'ordre fini divisant p. Supposons maintenant que m et n soient premiers entre eux, de sorte que $p = mn$. Soit N un entier tel que $(ab)^N = e$. On a $e = (ab)^{Nm} = a^{Nm}b^{Nm} = b^{Nm}$, donc Nm est multiple de n ; comme m et n sont premiers entre eux, N est multiple de n. De même, N est multiple de m. Utilisant de nouveau que m et n sont premiers entre eux, on obtient que N est multiple de mn. Par suite, l'ordre de ab est égal à mn. □

2.2. Exemples

2.2.1. — Les ensembles des entiers relatifs, des nombres rationnels, des nombres réels, des nombres complexes sont des groupes pour l'addition.

L'ensemble des entiers naturels est un monoïde pour l'addition, de même que l'ensemble $\{0, 2, 3, \ldots\}$.

2.2.2. — Les ensembles des nombres entiers naturels, des nombres entiers relatifs, des nombres rationnels, des nombres réels, des nombres réels positifs ou nuls, des nombres complexes sont des monoïdes pour la multiplication, mais ne sont pas des groupes.

Plus généralement, un anneau est un monoïde pour la multiplication.

Les ensembles des nombres rationnels non nuls, des nombres réels non nuls, des nombres réels strictement positifs, des nombres complexes non nuls, des nombres complexes de modules 1 sont des groupes pour la multiplication.

Soit n un entier naturel non nul. L'ensemble des nombres complexes tels que $z^n = 1$ est un groupe pour la multiplication.

Rappelons qu'on dit qu'un nombre complexe z est une racine de l'unité s'il existe un entier naturel $n \geqslant 1$ tel que $z^n = 1$. L'ensemble des racines de l'unité, muni de la multiplication, est un groupe.

2.2.3. — Soit M un monoïde. L'ensemble des éléments inversibles de M est noté $M^\times$; c'est un groupe pour la loi de composition de M.

2.2.4. — Soit A un anneau commutatif (on peut prendre, par exemple, $A = \mathbf{Z}$, $A = \mathbf{R}$, $A = \mathbf{C}$) et soit n un entier naturel. L'ensemble $M_n(A)$ des matrices $n \times n$ à coefficients dans A est un monoïde pour la multiplication des matrices.

Une matrice $M \in M_n(A)$ est inversible si et seulement si son déterminant est inversible dans A. L'ensemble $GL_n(A)$ des matrices inversibles est donc un groupe pour la multiplication des matrices ; l'ensemble $SL_n(A)$ des matrices de déterminant 1 en est un sous-groupe.

2.2.5. — L'ensemble des éléments inversible du monoïde multiplicatif $\mathbf{Z}$ est égal à $\{\pm 1\}$.

Soit n un entier $\geqslant 1$ et soit $M = \mathbf{Z}/n\mathbf{Z}$, muni de sa multiplication. Si l'on veut, on peut sans grand dommage considérer que M est l'ensemble $\{0, \dots, n-1\}$, la multiplication étant donnée par le reste de la division euclidienne par n du produit usuel.

Démontrons qu'un entier $m \in M$ est inversible si et seulement si m et n sont premiers entre eux. Supposons en effet que m est inversible et soit $a \in M$ tel que $a \cdot m = 1$; cela signifie qu'il existe $q \in \mathbf{Z}$ tel que $am = 1 + nq$. Alors, tout diviseur commun à m et n divise $am - nq = 1$, donc $\operatorname{pgcd}(m, n) = 1$. Inversement, supposons que m et n soient premiers entre eux ; d'après le théorème de Bézout, il existe des entiers u et v tels que $um + vn = 1$; on a donc $u \cdot m = 1$ dans M, ce qui prouve que m est inversible.

Rappelons aussi qu'on note $\varphi(n)$ le cardinal de l'ensemble des entiers $m \in \{1, \dots, n\}$ tels que $\operatorname{pgcd}(m, n) = 1$ (*indicateur d'Euler*).

2.2.6. — Soit E un ensemble. L'ensemble des applications de E dans lui-même est un monoïde pour la composition ; son élément neutre est l'application identique.

L'ensemble des éléments inversibles de ce monoïde est l'ensemble $\mathfrak{S}(E)$ des bijections dans E dans E, qu'on appelle aussi *permutations* de E. C'est un groupe pour la composition des applications.

Lorsque E est l'ensemble fini $\{1, \dots, n\}$, le groupe $\mathfrak{S}(E)$ est aussi noté $\mathfrak{S}_n$.

2.2.7. — Soit Q l'ensemble à 8 éléments, $\{1, -1, i, -i, j, -j, k, -k\}$ (groupe quaternionique d'ordre 8). Il existe une unique loi de groupe sur Q, d'élément neutre 1, pour laquelle $(-1)^2 = 1$, $a(-1) = (-1)a = -a$ si $a \in \{i, j, k\}$, $i^2 = j^2 = k^2 = -1$ et $ij = k$.

On a aussi $jk = i$, $ki = j$, $ji = -k$, $ik = -j$ et $kj = -i$. Le centre de Q est le sous-groupe $\{-1, 1\}$.

Corollaire **(4.2.3)**. — *Soit* E *un corps commutatif et soit* $P \in E[T]$ *un polynôme. Il existe une extension* F *de* E *dans laquelle le polynôme* P *est scindé.*

Démonstration. — Si $P = 0$, on pose $F = E$. Supposons maintenant $P \neq 0$.

Notons P_0 le produit des facteurs irréductibles de P qui sont de degré $\geqslant 2$ et raisonnons par récurrence sur $\deg(P_0)$. Si $\deg(P_0) = 0$, alors P_0 est constant, on peut poser $F = E$. Soit P_1 un facteur irréductible de P_0 ; par hypothèse, $\deg(P_1) \geqslant 2$. Soit F' une extension de rupture du polynôme P_1 sur E. Notons Q le polynôme P considéré comme élément de $F'[T]$. Soit $Q_0 \in F'[T]$ le produit des facteurs irréductibles de Q qui sont de degré $\geqslant 2$; c'est un diviseur de P_0. Puisque le polynôme P_1 possède une racine dans F', l'image du polynôme P_0 possède une racine dans F', de sorte que l'on a $\deg(Q_0) < \deg(P_0)$. Par récurrence, il existe une extension F de F' dans laquelle le polynôme Q est scindé. Ainsi, F est une extension de E dans laquelle le polynôme P est scindé. □

Corollaire **(4.2.4)**. — *Soit* E *un corps commutatif et soit* $P \in E[T]$ *un polynôme non nul. Soit* F *une extension de* E. *Pour que* P *soit scindé dans* F, *il faut et il suffit que pour toute extension* G *de* F, *toute racine a de* P *dans* G *appartienne à* F.

Démonstration. — Supposons que P est scindé dans F et écrivons $P = c(T - a_1) \dots (T - a_n)$, avec $c, a_1, \dots, a_n \in F$. Soit G une extension de F et soit b une racine de P dans G. On a donc $P(b) = c(b - a_1) \dots (b - a_n) = 0$. Comme $P \neq 0$, on a $c \neq 0$; il existe donc $j \in \{1, \dots, n\}$ tel que $b = a_j$, d'où $b \in F$.

Inversement, supposons que P ne soit pas scindé dans F. En particulier, $P \neq 0$ et il existe un facteur irréductible $P_1 \in F[T]$ tel que $\deg(P_1) \geqslant 2$. Soit $G = F[T]/(P_1)$ et soit a l'image de T dans G ; puisque $\deg(P_1) \geqslant 2$, on a $a \notin F$. Ainsi, G est une extension de F dans laquelle P possède une racine qui n'appartient pas à F. □

Définition **(4.2.5)**. — *Soit* E *un corps commutatif et soit* $P \in E[T]$. *On dit qu'une extension* F *de* E *est une* extension de décomposition *de* P *si le polynôme* P *est scindé dans* F *et si l'ensemble des racines de* P *dans* F *engendre* F *sur* E.

Proposition **(4.2.6)**. — *Soit* E *un corps commutatif, soit* $P \in E[T]$ *un polynôme non constant et soit* Ω *une extension de* E *dans laquelle* P *est scindé. Soit* F *une extension de* E *qui est engendrée par l'ensemble des racines de* P *dans* F. *Il existe un homomorphisme d'extensions de* F *dans* Ω.

Démonstration. — On démontre l'assertion par récurrence sur $[F : E]$. Si $[F : E] = 1$, alors $\operatorname{Hom}_E(F, \Omega)$ est réduit à l'homomorphisme canonique de E dans Ω.

Démonstration. — Soit $P \in F[T]$ le polynôme minimal de a. On l'écrit $P = T^n + c_{n_1}T^{n-1} + \cdots + c_0$. Les éléments $c_0, \ldots, c_{n-1}$ sont algébriques sur E. D'après le corollaire 4.1.12, la E-algèbre $F_1 = E[c_0, \ldots, c_{n-1}]$ est une extension finie de E. Par construction, a est algébrique sur F_1, de sorte que la F_1-algèbre $F_1[a]$ est une extension finie de F_1. D'après la proposition 4.1.3, l'extension $F_1[a]$ de E est finie. Par suite, chacun de ses éléments est algébrique sur E. En particulier, a est algébrique sur E. □

4.2. Extensions de rupture, extensions de décomposition

Lemme **(4.2.1)**. — *Soit* E *un corps commutatif et soit* $P \in E[T]$ *un polynôme* irréductible. *Soit* $F = E[T]/(P)$ *et soit* $a \in F$ *l'image de* T *par l'homomorphisme canonique de* E[T] *dans* F. *Alors,* F *est une extension de* E *et a est une racine de* P *dans* F.

De plus, pour toute extension G *de* E *et toute racine b de* P *dans* G, *il existe un unique homomorphisme d'extensions* $f : F \to G$ *tel que* $f(a) = b$.

Démonstration. — Il s'agit de redire des propriétés déjà vues. Comme P est irréductible et comme l'anneau E[T] est principal, l'idéal (P) est maximal, de sorte que F est une extension de E. Soit $c : E[T] \to F$ l'homomorphisme canonique de E[T] dans F ; c'est un homomorphisme de E-algèbres. Comme $c(T) = a$, on a $c(f) = f(a)$ pour tout polynôme $f \in E[T]$; par définition de c, on a $c(P) = 0$, donc $P(a) = 0$.

Soit G une extension de E et soit b une racine de P dans G. Soit $g : E[T] \to G$ l'unique homomorphisme de E-algèbres qui applique T sur b. On a $g(P) = P(b) = 0$. Par suite, $\mathrm{Ker}(g)$ contient (P) et il existe un homomorphisme $f : F \to G$ de E-algèbres tel que $f \circ c = g$. En particulier, $f(a) = f(c(T)) = g(T) = b$. Soit $f' : F \to G$ un homomorphisme d'extensions de E tel que $f'(a) = b$. Les homomorphismes de E-algèbres f et f' coïncident sur a ; comme $F = E[a]$, ils sont égaux. □

Définition **(4.2.2)**. — *Avec les notations du lemme 4.2.1, on dit que l'extension* F *de* E *est une* extension de rupture *du polynôme irréductible* P.[1]

[1] On trouve plus souvent la terminologie *corps de rupture* ; cette terminologie est hélas assez impropre car elle néglige la structure de E-algèbre sur F.

2.3. Sous-groupes

2.3.1. — Soit A un monoïde. On dit qu'une partie B de A est un sous-monoïde si elle contient l'élément neutre de A et si le produit de deux éléments quelconques de B appartient à B. La loi de composition de A induit alors, par restriction, une loi de composition sur B qui en fait un monoïde.

Si A est un groupe, on dit qu'une partie B de A est un sous-groupe si elle contient l'élément neutre de A, si le produit de deux éléments quelconques de B appartient à B, et si l'inverse d'un élément quelconque de B appartient à B. Loi de composition de A induit alors, par restriction, une loi de composition sur B qui en fait un groupe.

Exemple **(2.3.2)**. — Soit A un monoïde.

a) Le *centralisateur* d'un élément $a \in A$ est l'ensemble $Z_a(A)$ des éléments de A qui commutent avec a ; c'est un sous-monoïde de A. Si A est un groupe, c'est un sous-groupe de A.

En effet, si $b, c \in Z_a(A)$, on a $ab = ba$ et $ac = ca$, donc $abc = bac = bca$ si bien que $bc \in Z_a(A)$. De plus, $e \in Z_a(A)$. Cela prouve que $Z_a(A)$ est un sous-monoïde de A.

Enfin, si $b \in Z_a(A)$ et est inversible dans A, alors $a = abb^{-1} = bab^{-1}$, donc $b^{-1}a = ab^{-1}$ et $b^{-1} \in Z_a$. En particulier, Z_a est un sous-groupe de A si A est un groupe.

b) Le *centre* de A est l'ensemble Z(A) des éléments de A qui commutent avec tout élément de A ; c'est un sous-monoïde de A. Si A est un groupe, c'est un sous-groupe de A.

En effet, Z(A) est l'intersection de la famille $(Z_a(A))_{a \in A}$ des centralisateurs des éléments de A. L'assertion résulte donc du lemme 2.3.5.

c) Supposons que A soit un groupe. Soit B un sous-groupe de A. On appelle *normalisateur* de B dans A l'ensemble $N_A(B)$ des éléments $a \in A$ tels que $\mathrm{Int}(a)(B) = aBa^{-1} = B$. C'est un sous-groupe de A qui contient B.[2] En effet, on a $\mathrm{Int}(e)(B) = B$. Soit ensuite $a, a' \in N_A(B)$; alors $\mathrm{Int}(aa')(B) = \mathrm{Int}(a)(\mathrm{Int}(a')(B)) = \mathrm{Int}(a)(B) = B$, donc $aa' \in N_A(B)$. Enfin, si $a \in N_A(B)$, on a $\mathrm{Int}(a^{-1})(B) = \mathrm{Int}(a^{-1})(\mathrm{Int}(a)(B)) = \mathrm{Int}(a^{-1}a)(B) = \mathrm{Int}(e)(B) = B$, donc $a^{-1} \in N_A(B)$. Cela prouve que $N_A(B)$ est un sous-groupe de A.

[2] La définition initialement donnée est incorrecte, voir l'exercice 2.12.38.

Exemple **(2.3.3)** (Sous-groupes de $\mathbf{Z}$). — Soit $a \in \mathbf{Z}$. Si $a = 0$, l'ensemble $a\mathbf{Z} = 0$ est un sous-groupe de A. Si $a \neq 0$, on remarque que $a\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$ dont $|a|$ est le plus petit élément strictement positif.

Inversement, soit A un sous-groupe de $\mathbf{Z}$ et démontrons qu'il existe un unique entier $a \geqslant 0$ tel que $A = a\mathbf{Z}$. Si $A = \{0\}$, on pose $a = 0$. Sinon, A possède un élément non nul, donc aussi un élément strictement positif quitte à considérer l'opposé du précédent. Notons alors a le plus petit élément strictement positif de A. On démontre par récurrence sur q que l'on a $qa \in A$ pour tout entier $q \geqslant 0$, puis pour tout entier $q \leqslant 0$ puisqu'alors $qa = -(-q)a$. Ainsi, $a\mathbf{Z} \subset A$. Inversement, soit $b \in A$ et soit $b = aq + r$ la division euclidienne de b par a ; on a $0 \leqslant r < a$ et $r = b - qa$ appartient à A, donc $r = 0$ par minimalité de a ; cela démontre que $b = qa$ appartient à $a\mathbf{Z}$, d'où l'inclusion $A \subset a\mathbf{Z}$. On a donc $A = a\mathbf{Z}$.

Lemme **(2.3.4)**. — *Soit* A *un groupe abélien, dont la loi de composition est notée multiplicativement.*

a) *Pour tout entier $n \geqslant 1$, l'ensemble des éléments $a \in A$ tels que $a^n = e$ est un sous-groupe de* A.

b) *L'ensemble des éléments d'ordre fini de* A *est un sous-groupe de* A.

Le sous-groupe de A des éléments a tels que $a^n = e$ est appelé sous-groupe de n-torsion de A ; celui des éléments d'ordre fini est appelé sous-groupe de torsion de A. On dit aussi qu'un groupe est sans torsion si son élément neutre est le seul élément d'ordre fini.

Démonstration. — a) On a $e^n = e$; si $a^n = e$, alors $(a^{-1})^n = (a^n)^{-1} = e$; si $a^n = b^n = e$, alors $(ab)^n = a^n b^n$ car A est commutatif, donc $(ab)^n = e$. Cela prouve que l'ensemble indiqué est un sous-groupe de A.

b) Soit T cet ensemble. On a $e^1 = e$, donc $e \in T$. Soit $a, b \in T$; soit m, n des entiers $\geqslant 1$ tels que $a^m = b^n = e$; on a donc $a^{mn} = b^{mn} = e$, donc $(ab)^{mn} = e$ d'après la première assertion. Cette assertion montre aussi que a^{-1} est d'ordre fini si a est d'ordre fini. Cela démontre que T est un sous-groupe de A. □

Lemme **(2.3.5)**. — . *Soit* A *un monoïde et soit $(B_i)_{i\in I}$ une famille de sous-monoïdes de* A ; *posons $B = \bigcap_{i\in I} B_i$. Alors,* B *est un sous-monoïde de* A *et $B^\times = B \cap A^\times$. En particulier, si* A *est un groupe et si les B_i sont des sous-groupes de* A, *alors* B *est un sous-groupe de* A.

Corollaire **(4.1.12)**. — *Soit* E *un corps commutatif, soit* F *une extension de* E *et soit* A *une partie finie de* F *formée d'éléments algébriques sur* E. *Alors la sous-*E*-algèbre* $E[A]$ *de* F *engendrée par* F *est une extension finie de* E.

Démonstration. — On note $A = \{a_1, \dots, a_n\}$ et on raisonne par récurrence sur n. Il n'y a rien à démontrer si $n = 0$. Supposons $n \geqslant 1$ et posons $F' = E[a_1, \dots, a_{n-1}]$; observons que $E[A] = F'[a_n]$. Par récurrence, F′ est une extension finie de E. D'autre part, comme a_n est algébrique sur E, il est *a fortiori* algébrique sur F′. Par suite, $F'[a_n]$ est une extension finie de F′. D'après la proposition 4.1.3, la F′-algèbre $F'[a_n]$ est une extension finie de E, ce qu'il fallait démontrer. □

Corollaire **(4.1.13)**. — *Soit* E *un corps commutatif et soit* F *une extension de* E. *L'ensemble des éléments de* F *qui sont algébriques sur* E *est un sous-corps de* F.

Démonstration. — Soit $j : E \to F$ l'homomorphisme de corps qui définit l'extension F. Pour tout $a \in E$, l'élément $j(a)$ est racine du polynôme $T - a$, donc est algébrique sur E.

Soit a, b des éléments de F qui sont algébriques sur E. D'apprès le corollaire précédent, $E[a, b]$ est une extension finie de E. En particulier, ab et $a + b$ sont algébriques sur E. Cela démontre que l'ensemble des éléments de F qui sont algébriques sur E est un sous-anneau de F.

De plus, si a est un élément de F qui est algébrique sur E, on a vu que $E[a]$ est un sous-corps de E dont tous les éléments de E sont algébriques. Si $a \neq 0$, ce sous-corps contient $1/a$. Ainsi, l'ensemble des éléments de F qui sont algébriques sur E est un sous-corps de F. □

Remarque **(4.1.14)**. — Soit E un corps commutatif, soit F une extension finie de E et soit a un élément de F. Alors $E(a)$ est une sous-extension de F, de degré égal au degré de a, et l'on a $[F : E] = [F : E(a)]\,[E(a) : E]$. En particulier, le degré de a divise le degré $[F : E]$ de l'extension F.

Corollaire **(4.1.15)**. — *Soit* E *un corps commutatif, soit* F *une extension algébrique de* E *et soit* G *une extension de* F.

Soit a un élément de G *qui est algébrique sur* F. *Alors a est algébrique sur* E.

En particulier, si G *est une extension algébrique de* F, *c'est une extension algébrique de* E.

l'ensemble des nombres complexes qui sont algébriques sur $\mathbf{Q}$ est dénombrable. Comme l'ensemble des nombres complexes n'est pas dénombrable, l'ensemble des nombres transcendants n'est pas dénombrable (Cantor, 1874).

Proposition **(4.1.9)**. — *Soit* E *un corps commutatif, soit* F *une extension de* E *et soit a un élément de* F. *Soit* $\varphi : \mathrm{E}[\mathrm{T}] \to \mathrm{F}$ *l'homomorphisme de* E*-algèbres donné par* $\varphi(\mathrm{P}) = \mathrm{P}(a)$.

a) *Si a est transcendant sur* E, *l'homomorphisme φ est injectif et* $\mathrm{E}[a]$ *est un espace vectoriel de dimension infinie sur* E.

b) *Si a est algébrique sur* E, *il existe un unique polynôme unitaire de degré minimal tel que* $\varphi(\mathrm{P}) = 0$. *De plus,* P *est irréductible, engendre* $\mathrm{Ker}(\varphi)$, *et l'on a* $\dim_{\mathrm{E}}(\mathrm{E}[a]) = \deg(\mathrm{P})$. *Enfin,* $\mathrm{E}[a]$ *est un sous-corps de* F.

Définition **(4.1.10)**. — *Soit* E *un corps commutatif, soit* F *une extension de* E *et soit $a \in \mathrm{F}$ un élément algébrique sur* E. *L'unique polynôme unitaire de degré minimal tel que* $\mathrm{P}(a) = 0$ *est appelé le* polynôme minimal *de a et son degré est appelé degré de a sur* E*; ses racines sont les* conjugués *de a dans* F.

Démonstration. — a) Supposons a transcendant. Alors $\mathrm{P}(a) \neq 0$ pour tout polynôme non nul $\mathrm{P} \in \mathrm{E}[\mathrm{T}]$, de sorte que φ est injectif et définit un isomorphisme de $\mathrm{E}[\mathrm{T}]$ sur $\mathrm{E}[a]$. Comme $\mathrm{E}[\mathrm{T}]$ est un E-espace vectoriel de dimension infinie sur E, on a $\dim_{\mathrm{E}}(\mathrm{E}[\mathrm{T}]) = \infty$, d'où $\dim_{\mathrm{E}}(\mathrm{E}[a]) = \infty$.

b) Supposons a algébrique. Alors $\mathrm{Ker}(\varphi) \neq (0)$; soit P l'unique polynôme unitaire de degré minimal appartenant à $\mathrm{Ker}(\varphi)$. On a donc $\mathrm{Ker}(\varphi) = (\mathrm{P})$ et φ induit un homomorphisme injectif d'anneaux de $\mathrm{E}[\mathrm{T}]/(\mathrm{P})$ dans F, d'image $\mathrm{E}[a]$. Comme F est un corps, l'idéal (P) est premier et P est irréductible. Par suite, l'idéal (P) est maximal et $\mathrm{E}[a]$ est un corps.

Soit $n = \deg(\mathrm{P})$. Par division euclidienne, tout élément de $\mathrm{E}[\mathrm{T}]$ est congru à un unique polynôme de degré $< n$ modulo (P). Ainsi, $\dim_{\mathrm{E}}(\mathrm{E}[\mathrm{T}]/(\mathrm{P})) = n$. □

Corollaire **(4.1.11)**. — *Soit* E *un corps commutatif et soit* F *une extension finie de* E. *Alors* F *est une extension algébrique de* E.

Démonstration. — Soit $a \in \mathrm{F}$. Comme $\mathrm{E}[a]$ est un sous-espace vectoriel de F, il est de dimension finie, et a est donc algébrique sur E. □

Corollaire **(2.3.6)**. — *Soit* A *un monoïde (*resp. *un groupe) et soit* S *une partie de* A. *Il existe un plus petit sous-monoïde de* A *(*resp. *un plus petit-sous groupe de* A*) qui contient* S.

C'est l'intersection de la famille des sous-monoïdes (*resp.* des sous-groupes) de A qui contiennent S ; on l'appelle le sous-monoïde (*resp.* le sous-groupe) de A engendré par S et on le note $\langle \mathrm{S} \rangle$.

Exemple **(2.3.7)**. — Soit n un entier ; soit m un entier tel que $1 \leqslant m \leqslant n$ et soit $(a_1, \ldots, a_m)$ une suite d'éléments de $\{1, \ldots, n\}$, deux à deux distincts. On note $(a_1\ a_2\ \ldots\ a_m)$ l'élément du groupe symétrique $\mathfrak{S}_n$ qui applique a_1 sur a_2, a_2 sur a_3, etc., a_{m-1} sur a_m et a_m sur a_1, et qui fixe tout autre élément de $\{1, \ldots, n\}$.

Les ensembles suivants engendrent $\mathfrak{S}_n$:

a) L'ensemble $\mathrm{S} = \{(i\ j)\,;\, 1 \leqslant i < j \leqslant n\}$;
b) L'ensemble $\mathrm{S}' = \{(i\ i+1)\,;\, 1 \leqslant i < n\}$;
c) L'ensemble $\mathrm{S}'' = \{(1\ i)\,;\, 2 \leqslant i \leqslant n\}$;
d) L'ensemble $\mathrm{T} = \{(1\ 2), (1\ 2\ \ldots\ n)\}$.

Exemple **(2.3.8)**. — Dans le groupe $\mathrm{SL}_2(\mathbf{Z})$, on considère les deux matrices suivantes :

$$\mathrm{S} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad \mathrm{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Démontrons que l'ensemble $\{\mathrm{S}, \mathrm{T}\}$ engendre le groupe $\mathrm{SL}_2(\mathbf{Z})$.

Par l'absurde, considérons une matrice $\mathrm{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $\mathrm{SL}_2(\mathbf{Z})$ qui n'appartienne pas au groupe engendré par S et T et telle que la somme $|a| + |c|$ soit minimale.

On observe d'abord que pour toute matrice $\mathrm{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $\mathrm{SL}_2(\mathbf{Z})$ et tout entier $q \in \mathbf{Z}$, on a

$$\mathrm{S}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \quad \text{et} \quad \mathrm{T}^q \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mathrm{S} = \begin{pmatrix} a + qc & b + qd \\ c & d \end{pmatrix}.$$

Quitte à remplacer A par SA, on peut donc supposer que $|c| \leqslant |a|$. Supposons que $c \neq 0$ et soit $a = cq + r$ la division euclidienne de a par c, de sorte que $0 \leqslant r < |c|$. On a alors $\mathrm{T}^{-q}\mathrm{A} = \left(\begin{smallmatrix} r & \\ b-qd & \\ c & d \end{smallmatrix}\right)$ et l'inégalité $|r| + |c| < |c| + |c| \leqslant |a| + |c|$ contredit le choix de A. Par suite, $c = 0$; comme $ad - bc = 1$, on a $a = \pm 1$.

Supposons $a = 1$; alors $d = 1$ de sorte que $\mathrm{A} = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \mathrm{T}^b$. De même, si $a = -1$, on a $d = -1$ et $\mathrm{A} = \left(\begin{smallmatrix} -1 & b \\ 0 & -1 \end{smallmatrix}\right) = -\left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right) = \mathrm{S}^2\mathrm{T}^{-b}$. Dans les deux cas, on obtient que

A appartient au sous-groupe $\langle S, T\rangle$, et cette contradiction conclut la preuve que $\langle S, T\rangle = SL_2(\mathbf{Z})$.

2.4. Morphismes

2.4.1. — Soit A et B des monoïdes. On dit qu'une application $f : A \to B$ est un morphisme de monoïdes si l'on a $f(e_A) = e_B$ et si $f(ab) = f(a)f(b)$ pour tout couple (a, b) d'éléments de A.

Si A et B sont des groupes, on dit aussi que f est un morphisme de groupes. Remarquons qu'alors, on a $f(a^{-1}) = f(a)^{-1}$ pour tout $a \in A$. On a par suite

$$f([a, b]) = f(a^{-1}b^{-1}ab) = f(a)^{-1}f(b)^{-1}f(a)f(b) = [f(a), f(b)]$$

pour tout couple (a, b) d'éléments de A.

L'application identique id_A d'un monoïde (*resp.* d'un groupe) est un morphisme de monoïdes (*resp.* de groupes).

Si A et B sont des monoïdes (*resp.* des groupes), l'application de A dans B constante de valeur e est un morphisme de monoïdes (*resp.* de groupes), parfois qualifié de trivial.

Si $f : A \to B$ et $g : B \to C$ sont des morphismes de monoïdes (*resp.* de groupes), leur composée $g \circ f$ est un morphisme de monoïdes (*resp.* de groupes).

On dit qu'un morphisme $f : A \to B$ de monoïdes (*resp.* de groupes) est un *isomorphisme* s'il existe un morphisme de monoïdes (*resp.* de groupes) $g : B \to A$ tel que $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$. Pour que f soit un isomorphisme, il faut et il suffit qu'il soit bijectif; son application réciproque est en effet automatiquement un morphisme.

Ainsi, les monoïdes et leurs morphismes forment une catégorie, de même que les groupes et leurs morphismes.

Un morphisme $f : A \to A$ est appelé *endomorphisme* de A, et *automorphisme* de A si c'est un isomorphisme.

Remarque **(2.4.2)**. — Soit A un monoïde (*resp.* un groupe). L'ensemble $\mathrm{End}(A)$ des endomorphismes de A est un sous-monoïde du monoïde des applications de A dans lui-même (pour la composition des applications). L'ensemble $\mathrm{Aut}(A)$ des automorphismes de A est l'ensemble de ses éléments inversibles; c'est un sous-groupe du groupe des permutations de A (pour la composition des applications).

Démonstration. — Pour tout $a \in F$, $(T - a)^{m_a(P)}$ divise P. Lorsque a parcourt F, les polynômes $T - a$ sont premiers entre eux deux à deux; par suite, $\prod_{a\in F}(T - a)^{m_a(P)}$ divise P. En particulier, le degré du membre de gauche, égal à $\sum_{a\in F} m_a(P)$, est inférieur ou égal à $\deg(P)$. On a $m_a(P) \geqslant 1$ si et seulement si a est une racine de P. Par conséquent, $\sum_{a\in F} m_a(P)$ est supérieur ou égal au cardinal de l'ensemble des racines de P dans F. □

Définition **(4.1.6)**. — *Soit* F *un corps commutatif et soit* $P \in F[T]$. *On dit que* P *est* scindé *dans* F *s'il existe* $c \in F$ *et une suite* $(a_1, \ldots, a_n)$ *d'éléments de* F *tels que* $P = c(T - a_1)\ldots(T - a_n)$ *dans* $F[T]$.

On constante que les polynômes constants sont scindés, de même que les polynômes de degré 1.

Plus généralement, si E est un corps commutatif, $P \in E[T]$ et si F est une extension de E, on peut considérer le polynôme P comme un élément de $F[T]$. On parlera ainsi des racines de P dans F, de leurs multiplicités, ou on dira éventuellement que P est scindé dans F.

Définition **(4.1.7)**. — *Soit* E *un corps commutatif et soit* F *une extension de* E.

Soit a *un élément de* F. *On dit que* a *est* algébrique *sur* E *s'il existe un polynôme unitaire* $P \in E[T]$ *tel que* $P(a) = 0$*; dans le cas contraire, on dit que* a *est* transcendant *sur* E.

On dit que l'extension F *est algébrique sur* E *si tout élément de* F *est algébrique sur* E.

Plus généralement, on dit que des éléments $a_1, \ldots, a_n$ de F sont *algébriquement dépendants* sur E s'il existe un polynôme non nul $P \in E[T_1, \ldots, T_n]$ tel que $P(a_1, \ldots, a_n) = 0$; une telle relation est appelée *relation de dépendance algébrique* non triviale.

Exemple **(4.1.8)**. — a) Les nombre réel $\sqrt{2}$, les nombres complexes i, $1 + i\sqrt[3]{5} - \sqrt[7]{11}$ sont algébriques sur $\mathbf{Q}$. Si $\alpha \in \mathbf{Q}$, le nombre complexe $e^{2i\pi\alpha}$ est algébrique sur $\mathbf{Q}$, de même que les nombres réels $\cos(2\pi\alpha)$ et $\sin(2\pi\alpha)$.

b) Le nombre réel $\sum_{n=0}^{\infty} 10^{-n!}$ est transcendant sur $\mathbf{Q}$ (Liouville, 1844), de même que le nombre réel $\sum_{n=0}^{\infty} 10^{-n^3}$ (Roth, 1955).

c) Les nombres réels e et π sont transcendants (Hermite, Lindemann).

d) L'ensemble des polynômes à coefficients rationnels est dénombrable; comme un polynôme non nul a moins de racines complexes que son degré,

presque nulle $(x_{i,j})_{i\in I}$ d'éléments de E tels que $x_j = \sum_{i\in I} x_{i,j}a_i$. Si $x_j = 0$, alors $x_{i,j} = 0$ pour tout i ; par suite, la famille $(x_{i,j})_{i,j}$ est presque nulle et l'on a

$$x = \sum_{j\in J} x_j b_j = \sum_{j\in J}\sum_{i\in I} x_{i,j}a_i b_j$$

ce qui prouve que la famille $(a_i b_j)_{\substack{i\in I\\ j\in J}}$ engendre le E-espace vectoriel G.

Démontrons que cette famille est libre. Soit $(x_{i,j})$ une famille presque nulle d'éléments de E telle que $\sum_{i,j} x_{i,j}a_i b_j = 0$. Écrivons

$$0 = \sum_{j\in J}\left(\sum_{i\in I} x_{i,j}a_i\right) b_j.$$

Comme (b_j) est une base de G sur F, on a $\sum_{i\in I} x_{i,j}a_i = 0$ pour tout $j \in J$. Fixons $j \in J$; comme la famille (a_i) est une base de F sur E, on a $x_{i,j} = 0$ pour tout i. Cela démontre que la famille $(x_{i,j})$ est nulle.

Par suite,

$$[G : E] = \mathrm{Card}(I \times J) = \mathrm{Card}(I)\,\mathrm{Card}(J) = [F : E]\,[G : F].$$

Cela démontre la proposition. □

4.1.4. — Soit F un corps commutatif. Rappelons que pour tout élément $a \in F$, il existe un unique homomorphisme de F-algèbres $\varphi : E[T] \to F$ tel que $\varphi(T) = a$; on note $P(a) = \varphi(P)$.

Soit $P \in F[T]$ un polynôme en une indéterminée T. On dit qu'un élément $a \in F$ est une *racine* de P si l'on a $P(a) = 0$. Si a est une racine de P, alors $T - a$ divise P. Si $P \neq 0$, il existe un plus grand entier n tel que $(T - a)^n$ divise P ; on l'appelle la *multiplicité* de la racine a. C'est aussi la valuation $(T - a)$-adique de P. On dit qu'une racine est *simple* si sa multiplicité est égale à 1 ; sinon, on dit que c'est une racine multiple.

Proposition **(4.1.5)**. — *Soit* F *un corps commutatif et soit* $P \in F[T]$ *un polynôme non nul. Pour* $a \in F$, *notons* $m_a(P)$ *la multiplicité de* a *comme racine de* P. *On a*

$$\sum_{a\in F} m_a(P) \leqslant \deg(P).$$

En particulier, l'ensemble des racines de P *dans* F *est un ensemble fini de cardinal* $\leqslant \deg(P)$.

Exemple **(2.4.3)**. — Soit A un monoïde (*resp.* un groupe) et soit a un élément inversible de A. L'application $\mathrm{Int}(a) : A \to A$ donnée par $x \mapsto axa^{-1}$ est un endomorphisme de monoïdes (*resp.* de groupes) ; en effet, pour $x, y \in A$, on a

$$\mathrm{Int}(a)(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \mathrm{Int}(a)(x)\,\mathrm{Int}(a)(y).$$

On a $\mathrm{Int}(a) = \mathrm{id}_A$ si et seulement si $ax = xa$ pour tout $x \in A$, c'est-à-dire si se seulement si a appartient au centre de A.

En outre, si b est un autre élément inversible de A, on a

$$\mathrm{Int}(a) \circ \mathrm{Int}(b) = \mathrm{Int}(ab)$$

puisque

$$\begin{aligned}\mathrm{Int}(a)(\mathrm{Int}(b)(x)) &= a(bxb^{-1})a^{-1} = (ab)x(b^{-1}a^{-1})\\ &= (ab)x(ab)^{-1} = \mathrm{Int}(ab)(x)\end{aligned}$$

pour tout $x \in A$.

Il s'ensuit que $\mathrm{Int}(a)$ est un automorphisme de A et que son automorphisme réciproque est l'automorphisme $\mathrm{Int}(a^{-1})$. On dit que c'est l'*automorphisme intérieur* de A associé à a.

Soit $A^\times$ le groupe des éléments inversibles de A ; ce qui précède démontre que l'application $\mathrm{Int} : A^\times \to \mathrm{Aut}(A)$ est un homomorphisme de groupes. Son noyau est $A^\times \cap Z(A)$.

Lemme **(2.4.4)**. — *Soit* $f : A \to B$ *un morphisme de monoïdes (*resp. *de groupes)*

a) *L'image* $f(A)$ *est un sous-monoïde (*resp. *un sous-groupe) de* B.

b) *Soit* B' *un sous-monoïde (*resp. *un sous-groupe) de* B*; l'image réciproque* $f^{-1}(B')$ *est un sous-monoïde (*resp. *un sous-groupe) de* A.

c) *Soit* $g : A \to B$ *un second morphisme de monoïdes (*resp. *de groupes). L'ensemble* $\mathrm{Ker}(f, g)$ *des* $a \in A$ *tels que* $f(a) = g(a)$ *est un sous-monoïde (*resp. *un sous-groupe) de* A.

Démonstration. — a) On a $e_B = f(e_A) \in f(A)$. Soit $a, b \in f(A)$ et soit $x, y \in A$ tels que $a = f(x)$ et $b = f(y)$; alors, $ab = f(x)f(y) = f(xy) \in f(A)$. Cela démontre que $f(A)$ est un sous-monoïde de B. Supposons que A et B soient des groupes et soit $x \in f(A)$; soit $a \in A$ tel que $x = f(a)$; on a alors $x^{-1} = f(a^{-1}) \in f(A)$. Ainsi, $f(A)$ est un sous-groupe de B.

b) On a $f(e_A) = e_B \in B'$, donc $e_A \in f^{-1}(B')$. Soit $a, b \in f^{-1}(B')$; on a $f(a), f(b) \in B'$, donc $f(ab) = f(a)f(b) \in B'$ si bien que $ab \in f^{-1}(B')$. Cela prouve que $f^{-1}(B')$ est un sous-monoïde de A. Supposons que A et B soient des groupes et que B' soit un sous-groupe de B ; si $a \in f^{-1}(B')$, on a $f(a) \in B'$ donc $f(a^{-1}) = f(a)^{-1} \in B'$. Cela prouve que $f^{-1}(B')$ est un sous-groupe de A.

c) Comme $f(e_A) = g(e_A) = e_B$, on a $e_A \in \mathrm{Ker}(f, g)$. Soit $a, b \in \mathrm{Ker}(f, g)$, de sorte que $f(a) = f(b)$ et $g(a) = g(b)$; on a alors $f(ab) = f(a)f(b) = g(a)g(b) = g(ab)$ donc $ab \in \mathrm{Ker}(f, g)$. Cela prouve que $\mathrm{Ker}(f, g)$ est un sous-monoïde de A. Supposons maintenant que A soit un groupe et soit $a \in \mathrm{Ker}(f, g)$; on a $f(a^{-1}) = f(a)^{-1} = g(a)^{-1} = g(a^{-1})$, donc $a^{-1} \in \mathrm{Ker}(f, g)$. Cela démontre que $\mathrm{Ker}(f, g)$ est un sous-groupe de A. □

Définition **(2.4.5)**. — *Soit* $f : A \to B$ *un morphisme de groupes. On appelle noyau de* f *le sous-groupe* $f^{-1}(\{e_B\})$ *de* A*; on le note* $\mathrm{Ker}(f)$.

Proposition **(2.4.6)**. — *Pour qu'un morphisme de groupes* $f : A \to B$ *soit injectif, il faut et il suffit que l'on ait* $\mathrm{Ker}(f) = \{e_A\}$.

Démonstration. — Supposons que f soit injectif. Comme $f(e_A) = e_B$, l'élément e_A est alors le seul antécédent de e_B par f, c'est-à-dire $f^{-1}(\{e_B\}) = \{e_A\}$.

Supposons inversement que $\mathrm{Ker}(f) = \{e_A\}$ et démontrons que f est injectif. Soit a, b des élements de A tels que $f(a) = f(b)$. Alors, $f(ab^{-1}) = f(a)f(b)^{-1} = e_B$, donc $ab^{-1} = e_A$ et $a = b$. Cela prouve que f est injectif. □

2.5. Produit d'une famille de groupes

2.5.1. — Soit $(A_i)_{i\in I}$ une famille de monoïdes ; pour tout i, notons e_i l'élément neutre de A_i. Soit A le produit de cette famille ; un élément de A est une famille $(a_i)_{i\in I}$, où $a_i \in A_i$ pour tout $i \in I$.

On définit une loi de composition dans A en posant $(a_i)_{i\in I} \cdot (b_i)_{i\in I} = (a_i b_i)_{i\in I}$. Elle fait de A un monoïde dont l'élément neutre est la famille $(e_i)_{i\in I}$.

Pour tout $j \in I$, on note $p_j : A \to A_j$ la projection d'indice j ; elle applique la famille $(a_i)_{i\in I}$ sur l'élément a_j de A_j. C'est un morphisme de monoïdes.

Si les A_i sont des groupes, alors A est un groupe, et les projections p_j sont des morphismes de groupes.

CHAPITRE 4

CORPS

4.1. Extensions de corps

Définition **(4.1.1)**. — *Soit* E *un corps commutatif. On appelle* extension *de* E *une* E*-algèbre commutative qui est un corps.*

Une *sous-extension* d'une extension F de E est une sous-E-algèbre qui est corps. Si F et F′ sont des extensions de E, un morphisme de E-algèbres de F dans F′ est aussi appelé *morphisme d'extensions.*

Une extension d'un corps E revient à la donnée d'un corps F et d'un homomorphisme de corps $j : E \to F$. Remarquons qu'un tel homomorphisme j est injectif : en effet, son noyau est un idéal de E qui ne contient pas 1, donc est égal à $\{0\}$. Quitte à remplacer E par son image dans F, on peut ainsi faire comme si j est l'inclusion d'un sous-corps E de F.

Définition **(4.1.2)**. — *Soit* E *un corps commutatif et soit* F *une extension de* E.

On appelle degré *de* F *sur* E*, et on note* $[F : E]$*, la dimension de* F *comme* E*-espace vectoriel. On dit que* F *est une extension* finie *de* E *si* $[F : E]$ *est fini.*

Proposition **(4.1.3)**. — *Soit* E *un corps commutatif, soit* F *une extension de* E *et soit* G *une extension de* F*. Alors,* G *est une extension de* E *et l'on a*

$$[G : E] = [G : F]\,[F : E].$$

En particulier, si F *est une extension finie de* E *et* G *est une extension finie de* F*, alors* G *est une extension finie de* E.

Démonstration. — Soit $(a_i)_{i\in I}$ une base de F sur E et soit $(b_j)_{j\in J}$ une base de G sur F. Soit x un élément de G ; il existe une famille presque nulle $(x_j)_{j\in J}$ d'éléments de F telle que $x = \sum_{j\in J} x_j b_j$. Pour tout $j \in J$, il existe une famille

c) Soit ε la classe de T dans l'anneau quotient $A[T]/(T^2)$. Démontrer que l'application $f : A \to A[T]/(T^2)$ définie par $f(a) = a + D(a)\varepsilon$ est un homomorphisme de A-algèbres.

d) Soit K un anneau commutatif; on suppose que $A = K[T]$. Démontrer qu'il existe une unique dérivation D sur A qui applique T sur 1 et tout polynôme constant sur 0.

Exercice **(3.13.36)**. — Soit A un anneau et soit $f \in A[T]$.

a) Soit I un idéal de A tel que $I^2 = 0$, soit $a \in A$ et $b \in I$. Démontrer que $f(a+b) = f(a) + bf'(a)$. On suppose que $f(a) \in I$ et que $f'(a)$ est inversible modulo I. Démontrer qu'il existe un unique élément $a' \in A$ tel que $a' \equiv a \pmod{I}$ et $f(a') = 0$.

b) Soit I un idéal de A. On suppose qu'il existe un entier $m \geqslant 1$ tel que $I^m = 0$. Soit $a \in A$ tel que $f(a) \in I$ et tel que $f'(a)$ soit inversible modulo I. Démontrer qu'il existe un unique élément $a' \in A$ tel que $a' \equiv a \pmod{I}$ et $f(a') = 0$.

c) Trouver tous les éléments $a \in \mathbf{Z}/125\mathbf{Z}$ tels que $a^2 = -1$.

Exercice **(3.13.37)**. — Soit $A = \mathbf{Z}[i\sqrt{5}]$ le sous-anneau de $\mathbf{C}$ engendré par $i\sqrt{5}$.

a) Démontrer que tout élément de A s'écrit de manière unique sous la forme $a + ib\sqrt{5}$, pour $a, b \in \mathbf{Z}$.

b) Démontrer que $A^\times = \{\pm 1\}$.

c) Démontrer que $2, 3, 1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles dans A.

d) Démontrer que A n'est pas un anneau factoriel.

Proposition **(2.5.2)** (Propriété universelle du produit d'une famille de groupes)

Soit $(A_i)_{i\in I}$ *une famille de monoïdes (*resp. *de groupes), soit* A *son produit; pour tout* $i \in I$, *soit* $p_i : A \to A_i$ *la projection d'indice* i.

Soit B *un monoïde (*resp. *un groupe) et soit* $(f_i)_{i\in I}$ *une famille où, pour tout* i, f_i *est un morphisme de monoïdes (*resp. *de groupes) de* B *dans* A_i. *Il existe un unique morphisme de monoïdes (*resp. *de groupes)* $f : B \to A$ *tel que* $f_i = p_i \circ f$ *pour tout* $i \in I$.

Démonstration. — Définissons une application $f : B \to A$ par la formule $f(b) = (f_i(b))_{i\in I}$, pour $b \in B$. C'est un morphisme de monoïdes (*resp.* de groupes) et l'on a $f_i(b) = p_i(f(b))$ pour tout $b \in B$, c'est-à-dire $f_i = p_i \circ f$. Inversement, soit $f' : B \to A$ une application telle que $p_i \circ f' = f_i$ pour tout $i \in I$; pour $b \in B$, on a $f'(b) = (p_i \circ f'(b))_{i\in I} = (f_i(b)) = f(b)$, ce qui démontre que $f = f'$. □

2.5.3. — Soit A un groupe et soit B et C des sous-groupes de A tels que $B \cap C = \{e\}$ et $B \cdot C = A$. Remarquons que l'application f de $B \times C$ dans A donnée par $(b, c) \mapsto bc$ est une bijection : elle est surjective par hypothèse; de plus, si $(b, c), (b', c') \in B \times C$ sont tels que $bc = b'c'$, on a $c(c')^{-1} = b^{-1}b'$; cet élément appartenant à la fois à C et à B, il est égal à e ce qui montre $b = b'$ et $c = c'$.

a) Supposons que l'on a $bc = cb$ pour tout $b \in B$ et tout $c \in C$. Alors, l'application f est un morphisme de groupes; comme elle est bijective, c'est un isomorphisme. On dit que A est le *produit direct* de ses deux sous-groupes B et C et l'on note (abusivement) $A = B \times C$.

b) Supposons maintenant que pour tout $b \in B$ et tout $c \in C$, on ait $cbc^{-1} \in B$.[3] On dit alors que A est un *produit semi-direct* de B par C et l'on note (abusivement) $A = B \rtimes C$. Remarquons que pour $c \in C$, l'application $b \mapsto cbc^{-1}$ est un automorphisme $\varphi(c)$ de B, et l'application $\varphi : C \to \mathrm{Aut}(B)$ est un morphisme de groupes. Pour $b, b' \in B$ et $c, c' \in C$, on a $(bc)(b'c') = (bcb'c^{-1})cc' = (b\varphi(c)(b'))cc'$.

Nous allons maintenant construire une autre structure de groupe sur l'ensemble $B \times C$ de sorte que l'application $f : B \times C \to A$ donnée par $(b, c) \mapsto bc$ soit un morphisme de groupes.

Cette construction est valable dans une plus grande généralité : on se donne deux groupes B et C, ainsi qu'un morphisme de groupes de C dans le

[3] Si $cBc^{-1} \subset B$ pour tout $c \in C$, on a aussi $B = c^{-1}cBc^{-1}c \subset c^{-1}Bc \subset B$, donc $B = cBc^{-1}$. Cette propriété signifie ainsi que le normalisateur de B dans A contient C; comme il contient B et que l'on a $A = BC$, elle équivaut donc au fait que B soit un sous-groupe distingué de A.

groupe $\mathrm{Aut}(\mathrm{B})$ des automorphismes de B. On munit alors l'ensemble $\mathrm{B} \times \mathrm{C}$ de la loi de composition $*$ donnée par $(b,c)*(b',c') = (b\varphi(c)(b'), cc')$. Elle est associative car

$$\begin{aligned}\big((b,c)*(b',c')\big)*(b'',c'') &= (b\varphi(c)(b'), cc')*(b'',c'')\\ &= (b\varphi(c)(b')\varphi(cc')(b''), cc'c''),\\ (b,c)*\big((b',c')*(b'',c'')\big) &= (b,c)*(b'\varphi(c')(b''), c'c'')\\ &= (b\varphi(c)(b'\varphi(c')(b'')), cc'c'',\end{aligned}$$

et

$$b\varphi(c)(b'\varphi(c')(b'')) = b\varphi(c)(b')\varphi(c)(\varphi(c')(b'')) = b\varphi(c)(b')\varphi(cc')(b'').$$

Le couple (e,e) est un élément neutre, car on a $(b,c)*(e,e) = (b\varphi(c)(e),c) = (b,c)$ et $(e,e)*(b,c) = (\varphi(e)(b),c) = (b,c)$. De plus, pour $b, b' \in \mathrm{B}$ et $c, c' \in \mathrm{C}$, la relation $(b,c)*(b',c') = (e,e)$ équivaut à $b\varphi(c)(b') = e$ et $cc' = e$, ce qui prouve que $(\varphi(c)^{-1}(b), c^{-1})$ est l'unique inverse à droite de (b',c'), tandis que $(\varphi((c')^{-1})(b'), (c')^{-1})$ est l'unique inverse à gauche de (b,c). Par suite, tout élément est inversible pour cette loi de composition.

On note $\mathrm{B} \rtimes_\varphi \mathrm{C}$ l'ensemble $\mathrm{B} \times \mathrm{C}$ muni de cette loi de groupe ; on dit que c'est le *produit semi-direct* des groupes B et C *relativement à l'homomorphisme* φ.

Revenant maintenant au contexte de ce paragraphe, on voit donc que l'application canonique $(b,c) \mapsto bc$ du groupe $\mathrm{B} \rtimes_\varphi \mathrm{C}$ dans A est un isomorphisme de groupes.

Exemple **(2.5.4)**. — Soit K un corps et soit V un K-espace vectoriel. Le groupe $\mathrm{GA}(\mathrm{V})$ des automorphismes affines de V est le groupe des transformations de V de la forme $x \mapsto a(x) + b$, où $a \in \mathrm{GL}(\mathrm{V})$ et $b \in \mathrm{V}$. Il contient le sous-groupe $\mathrm{GL}(\mathrm{V})$ (formé des automorphismes affines qui fixent l'origine, lorsque $b = 0$) et le sous-groupe, noté T_V, des translations (données par $\tau_b : x \mapsto x+b$, lorsque $a = \mathrm{id}_\mathrm{V}$). Pour $a \in \mathrm{GL}(\mathrm{V})$ et $b \in \mathrm{V}$, on a $a \circ \tau_b \circ a^{-1} = \tau_{a(b)}$ puisque $a \circ \tau_b \circ a^{-1}(x) a(a^{-1}(x) + b) = x + a(b)$ pour tout $x \in \mathrm{V}$. Cela démontre que $\mathrm{GA}(\mathrm{V})$ le produit semi-direct de ses sous-groupes $\mathrm{GL}(\mathrm{V})$ et de T_V.

2.6. Opérations d'un groupe dans un ensemble

2.6.1. — Soit A un monoïde (*resp.* un groupe) et soit X un ensemble.

Exercice **(3.13.33)**. — Pour tout entier $n \geqslant 1$, soit $\Phi_n \in \mathbf{C}[\mathrm{T}]$ le polynôme unitaire dont les racines sont simples, égales aux racines primitives n-ième de l'unité (« polynôme cyclotomique »).

a) Démontrer que pour tout entier $n \geqslant 1$, on a $\prod_{d|n} \Phi_d = \mathrm{T}^n - 1$.

b) Calculer Φ_1. Calculer Φ_p si p est un nombre premier.

c) Démontrer par récurrence sur n que $\Phi_n \in \mathbf{Z}[\mathrm{T}]$ pour tout entier $n \geqslant 1$.

Exercice **(3.13.34)**. — Soit n un entier $\geqslant 1$. Le but de l'exercice est de démontrer que le polynôme cyclotomique Φ_n est irréductible dans $\mathbf{Q}[\mathrm{T}]$.

a) Soit a une racine primitive n-ième de l'unité et soit $\mathrm{P} \in \mathbf{Q}[\mathrm{T}]$ un polynôme unitaire de degré minimal tel que $\mathrm{P}(a) = 0$. Démontrer que $\mathrm{P} \in \mathbf{Z}[\mathrm{T}]$ et que P divise Φ_n dans $\mathbf{Z}[\mathrm{T}]$.

b) Soit p un nombre premier qui ne divise pas n. Démontrer que a^p est une racine primitive p-ième de l'unité.

c) Démontrer que le polynôme $\mathrm{P}(\mathrm{T}^p) - \mathrm{P}(\mathrm{T})^p$ appartient à $p\mathbf{Z}[\mathrm{T}]$. En déduire qu'il existe $b \in \mathbf{Z}[a]$ tel que $\mathrm{P}(a^p) = pb$.

d) On suppose que $b \neq 0$. Démontrer qu'il existe un polynôme $\mathrm{Q} \in \mathbf{Z}[\mathrm{T}]$ tel que $\mathrm{T}^n - 1 = \mathrm{PQ}$ et $\mathrm{Q}(a^p) = 0$. En dérivant $\mathrm{T}^n - 1$, démontrer que $n \in \mathbf{Z}[a]$ puis en déduire une contradiction.

e) Démontrer que $\mathrm{P}(z) = 0$ pour toute racine primitive n-ième de l'unité et en déduire que $\mathrm{P} = \Phi_n$.

f) Démontrer que pour tout entier $n \geqslant 1$, le polynôme Φ_n est irréductible dans $\mathbf{Q}[\mathrm{T}]$.

Exercice **(3.13.35)**. — Soit A un anneau commutatif. On dit qu'une application $\mathrm{D} : \mathrm{A} \to \mathrm{A}$ est une dérivation sur A si c'est un morphisme de groupes additifs et si, pour tout $a, b \in \mathrm{A}$, on a $\mathrm{D}(ab) = a\mathrm{D}(b) + b\mathrm{D}(a)$.

Soit D une dérivation sur A.

a) Démontrer que pour tout $a \in \mathrm{A}$ et tout $n \in \mathbf{N}$, on a $\mathrm{D}(a^n) = na^{n-1}\mathrm{D}(a)$. Si a est inversible, démontrer cette relation pour $n \in \mathbf{Z}$.

b) Soit B l'ensemble des éléments $a \in \mathrm{A}$ tels que $\mathrm{D}(a) = 0$. Démontrer que B est un sous-anneau de A.

e) Soit p un nombre premier tel que $p \equiv 1 \pmod 4$. Démontrer qu'il existe $u, v \in \mathbf{Z}$ tels que $u^2 + v^2 = p$ (théorème de Fermat sur les sommes de deux carrés).

Exercice **(3.13.30)**. — Soit F un corps commutatif et soit E un sous-corps de F. Soit P, Q deux polynômes de E[T].

a) On suppose que P et Q sont premiers entre eux. Démontrer que P et Q restent premiers entre eux lorsqu'on les considère comme polynômes à coefficients dans E[T].

b) Plus généralement, démontrer que le pgcd de P et Q est le même, qu'on les considère comme polynômes à coefficients dans E ou dans F.

Exercice **(3.13.31)**. — Soit p un nombre premier.

a) Soit d un entier $\geqslant 1$. Démontrer qu'il existe un élément d'ordre multiplicatif d dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si d divise $p-1$.

b) Démontrer que -1 est un carré dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si $p \equiv 1 \pmod 4$ ou $p = 2$.

c) Démontrer que l'équivalence des propriétés suivantes : (i) Le polynôme $T^2 + T + 1$ est réductible dans $(\mathbf{Z}/p\mathbf{Z})[T]$; (ii) -3 est un carré dans $\mathbf{Z}/p\mathbf{Z}$; (iii) $p \equiv 1 \pmod 3$.

Exercice **(3.13.32)**. — Soit A un anneau intègre et soit K son corps des fractions. Soit $f = a_n T^n + \cdots + a_0$ un polynôme à coefficients dans A en une indéterminée T.

a) Soit P un idéal premier de A tel que $a_0, \ldots, a_{n-1} \in P$, $a_n \notin P$ et $a_0 \notin P^2$. Démontrer qu'il n'existe pas de polynômes non constants $g, h \in A[T]$ tels que $f = gh$.

On suppose dans la suite que A est un anneau factoriel qu'il existe un un élément irréductible p de A tel que p divise $a_0, \ldots, a_{n-1}$, et p^2 ne divise pas a_0.

b) On suppose de plus que f est de contenu 1. Démontrer que le polynôme f est irréductible dans A[T].

c) Démontrer que le polynôme f est irréductible dans K[T]. (« Critère d'Eisenstein ».)

d) Démontrer que pour tout nombre premier p, le polynôme $T^{p-1} + \cdots + T + 1$ est irréductible dans $\mathbf{Q}[T]$. (Faire d'abord une substitution $T = U + 1$.)

e) Soit K un corps. Démontrer que pour tout polynôme $f \in K[X]$ qui n'est pas un carré, le polynôme $Y^2 - f(X)$ est irréductible dans K[X, Y].

Une *opération* (à gauche) de A dans X est un morphisme de A dans le monoïde des applications de X dans lui-même. Explicitement, c'est une application $f : A \to \mathfrak{F}(X; X)$ telle que $f(e) = \mathrm{id}_X$ et $f(ab)(x) = f(a)(f(b)(x))$ pour tous $a, b \in A$ et tout $x \in X$.

Si a est un élément inversible de A, alors $f(a)$ est un élément inversible de $\mathfrak{F}(X; X)$, c'est-à-dire une permutation de X. En particulier, si A est un groupe, une opération (à gauche) de A dans X est un morphisme de groupes de A dans le groupe $\mathfrak{S}(X)$ des permutations de X.

Se donner une telle opération f revient à se donner une application $\varphi : A \times X \to X$ telle que $\varphi(e, x) = x$ et $\varphi(a, \varphi(b, x)) = \varphi(ab, x)$ pour tous $a, b \in A$ et tout $x \in X$.

Le lien entre les deux points de vue consiste à poser $\varphi(a, x) = f(a)(x)$ pour $a \in A$ et $x \in X$.

Si B est une partie de A et Y une partie de X, on note parfois $B \cdot Y$ la partie $\{b \cdot y \,;\, b \in B,\ y \in Y\}$ de X.

2.6.2. — Soit A un monoïde (*resp.* un groupe) et soit X un ensemble. On définit de façon analogue les opérations à droite de A dans X. C'est un morphisme de A dans le monoïde opposé au monoïde des applications de X dans lui-même, c'est-à-dire une application $g : A \to \mathfrak{F}(X; X)$ telle que $g(e) = \mathrm{id}_X$ et $g(ab)(x) = g(b)(g(a)(x))$, pour tous $a, b \in A$ et tout $x \in X$.

Se donner une opération à droite g revient aussi à se donner une application $\psi : X \times A \to X$ telle que $\psi(x, e) = x$ et $\psi(\psi(x, a), b) = \varphi(x, ab)$ pour tous $a, b \in A$ et tout $x \in X$.

Lorsque A est un groupe, on passe d'une opération à droite g à une opération à gauche f en posant $f(a)(x) = g(a^{-1})(x)$ et $\varphi(a, x) = \psi(x, a^{-1})$ pour $a \in A$ et $x \in X$.

Exemple **(2.6.3)**. — Soit X un ensemble. Le monoïde $\mathfrak{F}(X; X)$, le groupe $\mathfrak{S}(X)$ des permutations de X agissent dans X de façon tautologique (via le morphisme identique). Cela revient aussi poser $f \cdot x = f(x)$ pour $f \in \mathfrak{F}(X; X)$ et $x \in X$.

Exemple **(2.6.4)**. — Soit K un corps (disons $K = \mathbf{R}$ ou $\mathbf{C}$) et soit V un K-espace vectoriel. Le monoïde $\mathrm{End}(V)$ des endomorphismes de V et le groupe $\mathrm{GL}(V)$ des automorphismes de V agissent de façon tautologique dans V, par la formule $f \cdot v = f(v)$ si $f \in \mathrm{End}(V)$ et $v \in V$.

Soit G un groupe. On appelle *représentation linéaire* de G dans V tout morphisme de groupes du groupe G dans le groupe $\mathrm{GL}(\mathrm{V})$ des automorphismes linéaires de V. Cela fournit en particulier une opération de G dans V.

Exemple **(2.6.5)**. — Soit A un monoïde (*resp.* un groupe) opérant dans un ensemble X. Par restriction, tout sous-monoïde (*resp.* sous-groupe) de A opère dans X. Plus généralement, soit B un monoïde et soit $u : \mathrm{B} \to \mathrm{A}$ un morphisme de monoïdes. Alors B opère dans X par la formule $b \cdot x = u(b) \cdot x$ pour $b \in \mathrm{B}$ et $x \in \mathrm{X}$.

On dit qu'une partie Y de X est *stable* pour l'opération de A si l'on a $a \cdot y \in \mathrm{Y}$ pour tout $y \in \mathrm{Y}$ et tout $a \in \mathrm{A}$. Dans ce cas, l'opération de A dans X se restreint en une opération de A dans Y.

Exemple **(2.6.6)**. — Soit A un monoïde. Le loi de composition de A, $\mathrm{A} \times \mathrm{A} \to \mathrm{A}$, induit une opération à gauche et une opération à droite de A dans lui-même, respectivement données par $a \cdot x = ax$ et $x \cdot a = xa$ pour $a, x \in \mathrm{A}$. On les appelle les opérations par translation à gauche et à droite. Cela fournit en particulier une injection du monoïde A dans le monoïde des applications de A dans lui-même et, si A est un groupe, un homomorphisme injectif de A dans le groupe $\mathfrak{S}(\mathrm{A})$ (« *plongement de Cayley* »).

L'homomorphisme de groupes $\mathrm{Int} : \mathrm{A}^\times \to \mathrm{Aut}(\mathrm{A})$ qui applique un élément inversible $a \in \mathrm{A}^\times$ sur l'automorphisme intérieur de A donné par $x \mapsto axa^{-1}$ est une opération de $\mathrm{A}^\times$ sur A, dite par conjugaison.

Ces opérations sont extrêmement importantes, notamment lorsque A est un groupe.

2.6.7. — Soit A un monoïde opérant dans un ensemble X.

Soit $x \in \mathrm{X}$; notons A_x l'ensemble des éléments $a \in \mathrm{A}$ tels que $a \cdot x = x$. On a $e \in \mathrm{A}_x$; si $a, b \in \mathrm{A}_x$, on a $ab \cdot x = a \cdot (b \cdot x) = a \cdot x = x$, donc $ab \in \mathrm{A}_x$. Ainsi, A_x est un sous-monoïde de A, qu'on appelle le *fixateur* de x.

Soit a un élément inversible de A appartenant à A_x; on a $a^{-1} \cdot x = a^{-1} \cdot (a \cdot x) = (a^{-1}a) \cdot x = e \cdot x = x$, donc $a^{-1} \in \mathrm{A}_x$. En particulier, si A est un groupe, alors les fixateurs des éléments de X sont des sous-groupes de A.

Plus généralement, si Y est une partie de X, on appelle fixateur de Y l'intersection des fixateurs des éléments de Y. C'est un sous-monoïde de A; si A est un groupe, c'est un sous-groupe de A. On appelle aussi *stabilisateur* de Y

Exercice **(3.13.26)**. — *a*) Soit A l'anneau $\mathscr{C}(\mathbf{R}; \mathbf{R})$ des fonctions continues de $\mathbf{R}$ dans $\mathbf{R}$. Démontrer que l'ensemble des fonctions à support compact est un idéal de A qui n'est pas contenu dans un idéal de la forme $\mathrm{M}_x = \{f\,;\, f(x) = 0\}$, pour $x \in \mathrm{X}$.

b) Soit $f_1, \dots, f_n \in \mathrm{M}_0$; démontrer que $\inf(|f_1|, \dots, |f_n|)^{1/2}$ n'appartient pas à l'idéal engendré par les f_i. En déduire que dans l'anneau A, l'idéal M_0 n'est pas de type fini.

c) Soit B l'anneau des fonctions continues sur le disque unité de $\mathbf{C}$ dont la restriction au disque ouvert est holomorphe. Soit I un idéal de B; démontrer qu'il existe un polynôme $\mathrm{P} \in \mathbf{C}[\mathrm{T}]$ dont toutes les racines sont de module $\leqslant 1$ tel que $\mathrm{I} = (\mathrm{P})$. En déduire que les idéaux maximaux de B sont les idéaux $(z - a)$, pour $a \in \mathbf{C}$ de module $\leqslant 1$.

Exercice **(3.13.27)**. — Soit A un anneau commutatif intègre et soit $j : \mathrm{A} - \{0\} \to \mathbf{N}$ une application. On suppose que pour tous $a, b \in \mathrm{A}$ tels que $b \neq 0$, il existe $q, r \in \mathrm{A}$ tels que $a = bq + r$ et $r = 0$ ou $j(r) < j(b)$.

Soit $j' : \mathrm{A} - \{0\} \to \mathbf{N}$ l'application définie par $j'(a) = \inf\{j(ax)\,;\, x \in \mathrm{A} - \{0\}\}$. Démontrer que j' est un stathme euclidien sur A.

Exercice **(3.13.28)**. — Soit A un anneau commutatif intègre et soit j un stathme euclidien sur A.

a) Soit $a \in \mathrm{A} - \{0\}$ un élément non nul, non inversible, pour lequel $j(a)$ soit minimal. Démontrer que pour tout élément $b \in \mathrm{A} - (a)$, il existe un élément inversible $u \in \mathrm{A}^\times$ et $v \in \mathrm{A}$ tel que $1 = ub + va$.

b) On suppose que $\mathrm{A}^\times$ est fini. Démontrer qu'il existe un idéal maximal M de A tel que $\mathrm{Card}(\mathrm{A}/\mathrm{M}) \leqslant \mathrm{Card}(\mathrm{A}^\times) + 1$.

Exercice **(3.13.29)**. — Soit A le sous-anneau de $\mathbf{C}$ engendré par i (anneau des entiers de Gauß).

a) Pour tout $z \in \mathbf{C}$, démontrer qu'il existe $a \in \mathrm{A}$ tel que $|a - z|^2 \leqslant 1/2$.

b) Démontrer que l'application $\mathrm{N} : z \mapsto |z|^2$ est un stathme euclidien sur A.

c) Soit $a \in \mathrm{A}$ tel que $\mathrm{N}(a)$ soit un nombre premier; démontrer que a est irréductible.

d) Pour tout nombre premier p, démontrer que l'anneau $\mathrm{A}/(p)$ est isomorphe à l'anneau $(\mathbf{Z}/p\mathbf{Z})[\mathrm{T}]/(\mathrm{T}^2 + 1)$. En déduire que p est irréductible dans A si et seulement si $p \equiv 3 \pmod 4$.

b) On suppose inversement que $M = A - A^\times$ est un sous-groupe du groupe additif de A. Démontrer que M est un idéal bilatère de A, et est l'unique idéal à gauche maximal de A.

Exercice **(3.13.23)**. — Soit A un anneau commutatif, soit S un partie multiplicative de A et soit $j : A \to A_S$ l'homomorphisme canonique de A dans l'anneau des fractions de A à dénominateurs dans S.

a) Soit P un idéal premier de A tel que $P \cap S = \varnothing$. Démontrer que P_S est un idéal premier de A_S.

b) Soit Q un idéal premier de A_S. Démontrer que $P = j^{-1}(Q)$ est l'unique idéal premier de A tel que $P_S = Q$.

c) On suppose que $S = A - P$, où P est un idéal premier de A. Démontrer que tout idéal de A_P qui est distinct de A_P est contenu dans P_P. En déduire que l'anneau A_P possède un unique idéal maximal.

Exercice **(3.13.24)**. — Soit A un anneau commutatif possédant un seul idéal maximal. Soit I et J des idéaux de A et soit *a* un élément simplifiable de A tels que $IJ = (a)$.

a) Démontrer qu'il existe $x \in I$ et $y \in J$ tels que $xy = a$.

b) Démontrer que *x* et *y* sont simplifiables.

c) Démontrer que $I = (x)$ et $J = (y)$.

Exercice **(3.13.25)**. — Soit A un anneau. On dit qu'un idéal à gauche I de A est maximal si $I \neq A$ et si pour tout idéal à gauche J de A tel que $I \subset J$, on a $J = I$ ou $J = A$.

a) Démontrer que tout idéal à gauche I de A qui est distinct de A est contenu dans un idéal à gauche maximal.

b) Soit R l'intersection de la famille des idéaux à gauche maximaux de A (« radical de Jacobson » de A). Démontrer qu'un élément *a* de A appartient à R si et seulement si $1 - xa$ est inversible à gauche, pour tout $x \in A$.

c) Démontrer que R est un idéal bilatère de A.

d) Soit *a* un élément de A. On suppose que l'image de *a* dans A/R est inversible; démontrer que *a* est inversible.

e) Soit J un idéal à gauche de A tel que $1 + x$ est inversible, pour tout $x \in J$. Démontrer que $J \subset R$.

l'ensemble des éléments $a \in A$ tels que $a \cdot Y = Y$. C'est un sous-monoïde de A, et un sous-groupe de A si A est un groupe.

2.6.8. — Soit A un groupe opérant (à gauche) dans un ensemble X. Soit *x* un élément de X. L'application de A dans X $a \mapsto a \cdot x$ est appelée application orbitale définie par *x*, et son image, égale à $A \cdot x$ est appelée l'orbite de *x*.

Observons que la relation dans X définie par « *x* appartient à l'orbite de *y* » est une relation d'équivalence dans X. La relation $x = e \cdot x$ montre en effet qu'elle est réflexive; si $x = a \cdot y$, on a $a^{-1} \cdot x = y$, donc cette relation est symétrique; enfin, si $x = a \cdot y$ et $y = b \cdot z$, on a $x = ab \cdot z$, donc cette relation est transitive.

L'ensemble des orbites de X est l'ensemble quotient de X par cette relation d'équivalence; on le note X/A ou A\X.[4]

2.6.9. — On dit que l'opération est *transitive* si elle a exactement une orbite. Cela revient à dire que X n'est pas vide (sinon, il y aurait zéro orbite) *et* que pour tout couple (x, y) d'éléments de X, il existe $a \in A$ tel que $y = a \cdot x$.

On dit qu'elle est *libre* si le fixateur de tout élément $x \in X$ est réduit à $\{e\}$. (C'est une propriété un peu exceptionnelle.)

On dit qu'elle est *fidèle* si $a = e$ est le seul élément de A tel que $a \cdot x = x$ pour tout $x \in X$. Cela revient à dire que l'homomorphisme de A dans $\mathfrak{S}(X)$ est injectif. En pratique, on peut toujours se ramener à une action fidèle, quitte à remplacer A par le quotient de A par le sous-groupe (distingué) noyau de l'homomorphisme précédent.

Exemple **(2.6.10)**. — Soit A un groupe et soit B un sous-groupe de A. Lorsqu'on fait opérer B par translation à gauche (*resp.* à droite) sur A, l'orbite B*a* (*resp.* *a*B) d'un élément de *a* est appelée[5] sa *classe à gauche* (*resp.* sa *classe à droite*) modulo B.

On note B\A et A/B les ensembles des classes à droite à gauche modulo B.

On remarque que l'action de A sur lui-même par translations à droite induit une action à droite de A sur B\A; explicitement : $Bx \cdot a = Bxa$. De même, l'action de A par translations à gauche induit une action à gauche sur A/B, donnée explicitement par $a \cdot xB = axB$.

[4] La notation la plus courante est X/A, mais lorsque l'on manipule à la fois des actions à droite et à gauche, il est commode de placer le groupe du côté où il agit.

[5] Les meilleurs auteurs préfèrent inverser cette terminologie et appeler B*a* la classe à droite de *a*, parce que *a* y figure à droite...

2.6.11. — Soit A un groupe opérant à gauche dans un ensemble X ; soit x un élément de X et soit A_x son fixateur. L'application orbitale de x, $A \to X$, passe au quotient pour la relation d'équivalence à droite modulo A_x et définit une application de A/A_x dans X, donnée par la formule $aA_x \mapsto a \cdot x$ pour $a \in A$.

Cette application est injective et son image est l'orbite de x.

2.6.12. — Soit A un groupe et soit B un sous-groupe de A. Les ensembles A/B et B\A des classes à droite et à gauche sont distincts en général. Cependant, l'application $aB \mapsto Ba^{-1}$ est une bijection de A/B sur B\A. Lorsque A/B (ou B\A) est fini, son cardinal est appelé *indice* de B dans A et noté $(A : B)$.

Proposition **(2.6.13)**. — *Soit* A *un groupe fini opérant dans un ensemble fini* X. *Pour toute orbite* $O \in X/A$, *choisissons un élément* x_O *de cette orbite et soit* A_O *son fixateur. On a la relation :*

$$\mathrm{Card}(X) = \sum_{O \in X/A} \mathrm{Card}(O) = \sum_{O \in X/A} (A : A_O).$$

Démonstration. — Comme les orbites de A dans X sont les classes d'équivalence d'une relation d'équivalence, elles définissent une partition de X, ce qui démontre la première égalité. D'autre part, l'application de A/A_O dans X donnée par $aA_O \mapsto a \cdot x_O$ est une injection d'image O, donc $\mathrm{Card}(O) = \mathrm{Card}(A/A_O) = (A : A_O)$. La deuxième égalité en découle. □

Corollaire **(2.6.14)**. — *Soit* G *un groupe fini et soit* H *un sous-groupe de* G. *On a*

$$\mathrm{Card}(G) = (G : H)\,\mathrm{Card}(H).$$

Démonstration. — Faisons agir H par translations à gauche dans G. Les orbites sont les classes à gauche Hg ; elles ont toutes pour cardinal $\mathrm{Card}(H)$ et sont au nombre de $(G : H)$. Le corollaire s'ensuit. □

Corollaire **(2.6.15)** (Lagrange). — *Soit* G *un groupe fini et soit* g *un élément de* G. *L'ordre de* g *divise le cardinal de* G.

Corollaire **(2.6.16)** (Équation aux classes). — *Soit* G *un groupe fini et soit* Z *son centre. Pour chaque classe de conjugaison* $C \in \mathscr{C}(G)$ *non réduite à un singleton, choisissons un élément* $x_C \in C$ *et notons* Z_C *le centralisateur de* x_C. *On a alors*

$$\mathrm{Card}(G) = \mathrm{Card}(Z) + \sum_{C \in \mathscr{C}(G)} (G : Z_C).$$

Exercice **(3.13.19)**. — Soit $f : A \to B$ un homomorphisme d'anneaux commutatifs, soit S une partie multiplicative de A et soit T une partie multiplicative de B telle que $f(S) \subset T$. Démontrer qu'il existe un unique homomorphisme d'anneaux $\varphi : A_S \to B_T$ qui applique $a/1$ sur $f(a)/1$ pour tout $a \in A$.

Exercice **(3.13.20)**. — Soit A un anneau commutatif, soit s un élément de A et soit $S = \{1, s, s^2, \ldots\}$ l'ensemble des puissances de s. Soit A_s l'anneau des fractions de A à dénominateurs dans S ; on le considère comme une A-algèbre au moyen de l'homomorphisme canonique $j : A \to A_s$.

a) Démontrer qu'il existe un unique homomorphisme de A-algèbres $f : A[T] \to A_s$ qui applique T sur $1/s$.

b) Démontrer que f est surjectif et que son noyau contient $1 - sT$.

c) Démontrer que l'image de s dans l'anneau quotient $A[T]/(1 - sT)$ est inversible.

d) Soit $\varphi : A[T]/(1 - sT) \to A_s$ l'homomorphisme déduit de f par passage au quotient. Démontrer que φ est un isomorphisme.

Exercice **(3.13.21)**. — Soit A un anneau commutatif, soit S une partie multiplicative de A et soit $j : A \to A_S$ l'homomorphisme canonique de A dans l'anneau des fractions de A à dénominateurs dans S.

a) Soit I un idéal de A ; on note I_S l'idéal de A_S engendré par $j(I)$. Démontrer que I_S est l'ensemble des fractions a/s, pour $a \in I$ et $s \in S$.

b) Démontrer que $I_S = A_S$ si et seulement si $S \cap I \neq \varnothing$.

c) Soit J un idéal de A_S et soit $I = j^{-1}(J)$. Démontrer que l'on a $I_S = J$.

d) Soit $f : A \to A/I$ l'homomorphisme canonique, soit $T = f(S)$ et soit $k : A/I \to (A/I)_T$ l'homomorphisme canonique de A/I dans l'anneau des fractions de A/I à dénominateurs dans T. Démontrer qu'il existe un unique homomorphisme d'anneaux $\varphi : (A/I)_T \to A_S/I_S$ qui applique $f(a)/1$ sur la classe de $a/1$ modulo I_S. Démontrer que φ est un isomorphisme.

Exercice **(3.13.22)**. — Soit A un anneau non nul.

a) On suppose que A possède un seul idéal à gauche maximal M. Démontrer que $A - M$ est l'ensemble $A^\times$ des éléments inversibles de A.

Exercice **(3.13.14)**. — Soit A un anneau et soit I un idéal à droite de A.

a) Démontrer que l'idéal à gauche engendré par I est un idéal bilatère.

b) Soit J l'ensemble des éléments $a \in A$ tels que $xa = 0$ pour tout $x \in I$. Démontrer que J est un idéal bilatère de A.

Exercice **(3.13.15)**. — Soit A un anneau commutatif, soit I et J des idéaux tels que $I + J = A$. Démontrer que $I^n + J^n = A$ pour tout entier $n \geqslant 1$.

Exercice **(3.13.16)**. — Soit A un anneau.

a) Soit (P_i) une famille totalement ordonnée d'idéaux premiers de A. Démontrer que son intersection $P = \bigcap_i P_i$ est un idéal premier de A.

b) Démontrer que tout idéal premier de A contient un idéal premier minimal.

Exercice **(3.13.17)**. — Soit A un anneau et soit I l'idéal bilatère de A engendré par les éléments de la forme $xy - yx$, pour $x, y \in A$.

a) Démontrer que l'anneau A/I est commutatif.

b) Soit J un idéal bilatère de A tel que l'anneau A/J soit commutatif. Démontrer que $I \subset J$.

Exercice **(3.13.18)**. — Soit A un anneau commutatif et soit S une partie multiplicative de A. Soit A_S l'anneau des fractions de A à dénominateurs dans S et soit $j : A \to A_S$ l'homomorphisme canonique.

a) Démontrer que le noyau de j est l'ensemble des éléments $a \in A$ tels qu'il existe $s \in S$ tel que $as = 0$.

b) En déduire que j est injectif si et seulement si tout élément de S est simplifiable.

c) Soit $a \in A$. Démontrer que $j(a)$ est inversible dans A_S si et seulement s'il existe $b \in A$ tel que $ab \in S$.

d) Soit S′ l'ensemble des éléments $a \in A$ tels qu'il existe $b \in A$ de sorte que $ab \in S$. Démontrer que S′ est l'ensemble des éléments $a \in A$ tels que $j(a)$ soit inversible dans A_S.

e) Démontrer qu'il existe un unique homomorphisme d'anneaux de A_S dans $A_{S'}$ qui applique $a/1$ sur $a/1$, pour tout $a \in A$. Démontrer que cet homomorphisme est un isomorphisme.

Démonstration. — On considère l'action de G sur lui-même par automorphismes intérieurs. Ses orbites sont les classes de conjugaison; pour tout point $x \in G$, le fixateur de x est le centralisateur de x. Enfin, l'orbite d'un élément x est réduite à un élément si et seulement si x appartient au centre de G. La formule en résulte. □

2.7. Sous-groupes distingués et groupes quotients

Définition **(2.7.1)**. — *Soit* A *un groupe. On dit qu'un sous-groupe* B *de* A *est* distingué *si pour tout* $a \in A$ *et tout* $b \in B$, *on a* $aba^{-1} \in B$.

Ainsi, un sous-groupe de A est distingué s'il est stable par tout automorphisme intérieur de A. Observons tout de suite que si A est abélien, alors tout sous-groupe de A est distingué.

Plus généralement, on appelle sous-groupe *caractéristique* d'un groupe A tout sous-groupe B tel que pour tout automorphisme f de A, on ait $f(B) \subset B$. En particulier, un sous-groupe caractéristique est distingué. Le sous-groupe $\{e\}$ et le sous-groupe A sont des sous-groupes caractéristiques de A.

Exemple **(2.7.2)**. — Le centre Z d'un groupe A est un sous-groupe caractéristique (et donc distingué).

Soit en effet $f \in \mathrm{Aut}(A)$ et $a \in Z$; démontrons que $f(a) \in Z$. Soit $b \in A$ et soit $b' \in A$ tel que $f(b') = b$; On a alors

$$f(a)b = f(a)f(b') = f(ab') = f(b'a) = f(b')f(a) = bf(a),$$

si bien que $f(a) \in Z$.

Exemple **(2.7.3)**. — Soit $f : A \to C$ un homomorphisme de groupes. Pour $a \in A$ et $b \in \mathrm{Ker}(f)$, on a $f(aba^{-1}) = f(a)f(b)f(a)^{-1} = f(a)f(a)^{-1} = e$, donc $aba^{-1} \in \mathrm{Ker}(f)$. En particuier, le noyau d'un homomorphisme de groupes est donc un sous-groupe distingué.

Plus généralement, démontrons l'image réciproque $f^{-1}(B)$ d'un sous-groupe distingué B de C est un sous-groupe distingué de A. Soit en effet $a \in A$ et $b \in f^{-1}(B)$; on a $f(aba^{-1}) = f(a)f(b)f(a)^{-1} \in B$ puisque $f(b)$ est un sous-groupe distingué de C; donc $aba^{-1} \in f^{-1}(B)$, ce qui démontre que $f^{-1}(B)$ est un sous-groupe distingué de B.

Exemple **(2.7.4)**. — Soit A un groupe et soit B un sous-groupe de A. Le normalisateur $N_B(A)$ est le plus grand sous-groupe de A dont B soit un sous-groupe distingué.

Lemme **(2.7.5)**. — *Soit* A *un groupe. L'intersection* $\bigcap_{i\in I} B_i$ *d'une famille* $(B_i)_{i\in I}$ *de sous-groupes distingués de* A *est un sous-groupe distingué de* A.

Démonstration. — Notons B cette intersection; c'est un sous-groupe de A d'après le lemme 2.3.5. Soit $a \in A$ et soit $b \in B$. Pour tout $i \in I$, on a $b \in B_i$, donc $aba^{-1} \in B_i$, car B_i est un sous-groupe distingué de A; par suite, $b \in B$. Cela démontre que B est un sous-groupe distingué de A. □

Corollaire **(2.7.6)**. — *Soit* A *un groupe et soit* S *une partie de* A. *Il existe un plus petit sous-groupe distingué de* A *qui contient* S.

C'est l'intersection de la famille de tous les sous-groupes distingués de A qui contiennent S.

On dit que c'est le sous-groupe distingué de A engendré par S.

2.7.7. — Soit A un groupe. Rappelons qu'on dit qu'une relation d'équivalence $\sim$ dans A est compatible avec la loi de groupe de A si les relations $a \sim b$ et $a' \sim b'$ entraînent $aa' \sim bb'$.

Supposons que ce soit le cas et soit a, b des éléments de A tels que $a \sim b$; comme $a^{-1} \sim a^{-1}$, il vient alors $e = a^{-1}a \sim a^{-1}b$, puis $b^{-1} = eb^{-1} \sim a^{-1}bb^{-1} = a^{-1}$ car $b^{-1} \sim b^{-1}$; comme la relation $\sim$ est symétrique, on a donc $a^{-1} \sim b^{-1}$.

Soit C l'ensemble quotient $A/\sim$ de A par la relation d'équivalence $\sim$ et soit $c : A \to C$ la surjection canonique (qui associe à un élément $a \in A$ sa classe d'équivalence. La loi de groupe de A passe au quotient et définit une unique loi de composition dans C telle que que $c(ab) = c(a)c(b)$ pour tous $a, b \in A$. Cette loi est associative, l'élément $c(e)$ est un élément neutre, et tout élément de C est inversible. Pour cette loi, C est donc un groupe, qu'on appelle le groupe quotient de A par la relation d'équivalence $\sim$, et l'application c est un homomorphisme de groupes dont le noyau est la classe de e.

Lemme **(2.7.8)**. — *Soit* A *un groupe et soit* B *une partie de* A. *Les quatre propriétés suivantes sont équivalentes :*

(i) *L'ensemble* B *est un sous-groupe distingué de* A *;*

Exercice **(3.13.11)**. — Soit n un entier naturel. Soit K un corps commutatif. Soit A l'anneau $K[T_1, \dots, T_n]$ et soit P l'anneau des fonctions de K^n dans K.

a) Pour tout $f \in A$, on note $\varphi(f)$ la fonction de K^n dans K donnée par $a \mapsto f(a)$. Démontrer que l'application $\varphi : A \to P$ est un homomorphisme d'anneaux.

b) On suppose que K est un corps infini. Démontrer que l'homomorphisme φ est injectif mais pas surjectif.

c) On suppose que K est un corps fini. Démontrer que l'homomorphisme φ est surjectif mais pas injectif.

Exercice **(3.13.12)**. — *a*) Soit M un monoïde commutatif vérifiant la propriété $(*)$: pour tout $m \in M$, l'ensemble des couples $(p, q) \in M \times M$ tels que $p + q = m$ est fini. Soit A un anneau commutatif.

Montrer que le produit de convolution définit encore une loi commutative et associative sur A^M. Vérifier qu'alors $(A^M, +, *)$ est une A-algèbre commutative et associative dont $A^{(M)}$ est une sous-algèbre. (« Algèbre large du monoïde M ».)

b) Soit n un entier naturel. Démontrer que le monoïde $M = \mathbf{N}^n$ vérifie la propriété $(*)$.

c) Démontrer qu'une fonction $f \in A^M$ est inversible pour le produit de convolution si et seulement $f(0) \in A^\times$.

d) On suppose que A est un anneau noethérien et que $M = \mathbf{N}$. Démontrer que $(A^{\mathbf{N}}, +, *)$ est un anneau noethérien.

Exercice **(3.13.13)**. — Soit K un corps, soit V un K-espace vectoriel de dimension finie et soit A l'anneau $\mathrm{End}_K(V)$ des endomorphismes de V.

a) Soit W un sous-espace vectoriel de V. Démontrer que $N_W = \{u \in A ; W \subset \mathrm{Ker}(u)\}$ est un idéal à gauche de A.

b) Inversement, si I est un idéal à gauche de A, démontrer qu'il existe un unique sous-espace vectoriel W de V tel que $I = N_W$.

c) Soit W un sous-espace vectoriel de V. Démontrer que $I_W = \{u \in A ; \mathfrak{I}(u) \subset W$ est un idéal à droite de A.

d) Inversement, si J est un idéal à droite de A, démontrer qu'il existe un unique sous-espace vectoriel W de V tel que $J = I_W$.

e) Soit I un idéal bilatère de A. Démontrer que $I = \{0\}$ ou $I = A$.

b) Démontrer que l'endomorphisme identique est l'unique endomorphisme de A.

Exercice **(3.13.8)**. — *a*) Soit A le sous-anneau de **C** engendré par i (où $i^2 = -1$) (« entiers de Gauß »).

b) Démontrer que pour tout élément a de A, il existe un unique couple (u, v) d'entiers relatifs tels que $a = u + iv$.

c) Démontrer que le monoïde des endomorphismes de A possède deux éléments, l'identité et la conjugaison complexe.

d) Pour $a = u + iv \in \mathrm{A}$, on pose $\mathrm{N}(a) = u^2 + v^2 = |a|^2$. Démontrer que $\mathrm{N} : \mathrm{A} \to \mathbf{N}$ est un homomorphisme de monoïdes multiplicatifs.

e) Démontrer que a est inversible dans A si et seulement si $a \in \{\pm 1, \pm i\}$. En déduire que le groupe $\mathrm{A}^\times$ est isomorphe à $\mathbf{Z}/4\mathbf{Z}$.

Exercice **(3.13.9)**. — Soit A un anneau commutatif. Soit $f = a_0 + a_1\mathrm{T} + \cdots + a_n\mathrm{T}^n \in \mathrm{A}[\mathrm{T}]$.

a) Démontrer que f est nilpotent dans l'anneau $\mathrm{A}[\mathrm{T}]$ si et seulement si, pour tout i, a_i est nilpotent dans A.

b) On suppose que a_0 est inversible et que $a_1, \ldots, a_n$ sont nilpotents dans A ; démontrer que f est inversible dans A.

c) Inversement, on suppose que f est inversible dans $\mathrm{A}[\mathrm{T}]$ et soit $g = b_0 + \cdots + b_m\mathrm{T}^m$ son inverse ; démontrer par récurrence sur k que $a_n^{k+1} b_{m-k} = 0$. En déduire que a_0 est inversible et que $a_1, \ldots, a_n$ sont nilpotents.

d) On suppose que f n'est pas simplifiable. Soit $g \in \mathrm{A}[\mathrm{T}]$ un polynôme non nul de degré minimal tel que $fg = 0$; démontrer que $a_k g = 0$ pour tout entier k. En déduire qu'il existe un élément non nul $a \in \mathrm{A}$ tel que $af = 0$.

Exercice **(3.13.10)**. — Soit A un anneau.

a) Soit $a \in \mathrm{A}^\times$ et $b \in \mathrm{B}$; démontrer qu'il existe un automorphisme φ de la A-algèbre $\mathrm{A}[\mathrm{T}]$, et un seul, tel que $\varphi(\mathrm{T}) = a\mathrm{T} + b$.

b) Soit φ un automorphisme de la A-algèbre $\mathrm{A}[\mathrm{T}]$. Démontrer qu'il existe un unique couple (a, b), où $a \in \mathrm{A}^\times$ et $b \in \mathrm{A}$, tels que $f = \varphi(\mathrm{T}) - a\mathrm{T} - b$ soit divisible par T^2.

c) Soit $f \in \mathrm{A}$ tel que $f - \mathrm{T}$ soit nilpotent. Démontrer qu'il existe un automorphisme φ de $\mathrm{A}[\mathrm{T}]$, et un seul, tel que $\varphi(\mathrm{T}) = f$.

(ii) *La relation $a \sim b$ définie par $a^{-1}b \in \mathrm{B}$ est une relation d'équivalence dans* A *qui est compatible avec sa loi de groupe ;*

(iii) *Il existe une relation d'équivalence dans* A *qui est compatible avec sa loi de groupe telle que* B *soit la classe de e ;*

(iv) *Il existe un groupe* C *et un homomorphisme de groupes surjectif $f : \mathrm{A} \to \mathrm{C}$ de noyau* B.

Démonstration. — (i)⇒(ii). Pour $a \in \mathrm{A}$, on a $a^{-1}a = e \in \mathrm{B}$; ainsi, cette relation est réflexive. Pour $a, b \in \mathrm{A}$ tels que $a \sim b$, l'élément $b^{-1}a = (a^{-1}b)^{-1}$ appartient à B, car c'est l'inverse d'un élément de B ; cette relation est donc symétrique. Soit $a, b, c \in \mathrm{A}$ tels que $a \sim b$ et $b \sim c$; l'élément $a^{-1}c = (a^{-1}b)(b^{-1}c)$ est le produit de deux éléments de B, donc appartient à B ; cette relation est donc transitive. Cela démontre que la relation indiquée est une relation d'équivalence. Démontrons maintenant qu'elle est compatible avec sa loi de groupe. Soit a, b, a', b' des éléments de A tels que $a \sim a'$ et $b \sim b'$; alors

$$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = (b^{-1}b')(b')^{-1}(a^{-1}a')b' ;$$

l'élément $b^{-1}b'$ appartient à B par hypothèse, de même que l'élément $a^{-1}a'$; comme B est un sous-groupe distingué de A, on a donc $(b')^{-1}(a^{-1}a')b' \in \mathrm{B}$; par suite, $(ab)^{-1}(a'b')$ appartient à B et $ab \sim a'b'$. Cela démontre (ii).

L'implication (ii)⇒(iii) est évidente.

Démontrons que (iii) implique (iv). Soit C le groupe quotient de A par la relation d'équivalence $\sim$ et soit $c : \mathrm{A} \to \mathrm{C}$ l'homomorphisme de groupes canonique. Il est surjectif et son noyau est le sous-groupe B.

L'implication (iv)⇒(i) résulte de ce que le noyau d'un homomorphisme de groupes est un sous-groupe distingué. □

2.7.9. — Soit A un groupe et soit B un sous-groupe distingué de A. Le groupe quotient de A par la relation d'équivalence associée au sous-groupe distingué B est noté A/B ; on dit que c'est le quotient de A par B.

Proposition **(2.7.10)** (Propriété universelle du groupe quotient)

Soit A *un groupe, soit* B *un sous-groupe distingué de* A*, soit $p : \mathrm{A} \to \mathrm{A}/\mathrm{B}$ la surjection canonique. Soit* C *un groupe et soit $f : \mathrm{A} \to \mathrm{C}$ un morphisme de groupes tel que $f(\mathrm{B}) = \{e\}$. Il existe un unique morphisme de groupes $\bar{f} : \mathrm{A}/\mathrm{B} \to \mathrm{C}$ tel que $f = \bar{f} \circ p$.*

De plus, $\bar{f}$ est injectif si et seulement si $\mathrm{Ker}(f) = \mathrm{B}$*; $\bar{f}$ est surjectif si et seulement si* $\mathrm{Im}(f) = \mathrm{C}$.

Démonstration. — Notons $\sim$ la relation d'équivalence dans A associée au sous-groupe distingué B. Soit a et b des éléments de A tels que $a \sim b$; on a $f(a)^{-1}f(b) = f(a^{-1}b) = e$ car $a^{-1}b \in \mathrm{B}$ et $\mathrm{B} \subset \mathrm{Ker}(f)$; ainsi, $f(a) = f(b)$. D'après la propriété universelle du magma quotient, il existe donc un unique morphisme de magmas $\bar{f} : \mathrm{A/B} \to \mathrm{C}$ telle que $\bar{f}(p(a)) = f(a)$ pour tout $a \in \mathrm{A}$; de plus, $\bar{f}(e) = \bar{f}(p(e)) = f(e) = e$. Ainsi, $\bar{f}$ est un morphisme de groupes.

Supposons que $\mathrm{Ker}(f) = \mathrm{B}$ et soit $x \in \mathrm{A/B}$ tel que $\bar{f}(x) = e$; soit $a \in \mathrm{A}$ tel que $x = p(a)$; on a donc $f(a) = \bar{f}(x) = e$, d'où $a \in \mathrm{B}$, si bien que $x = e$. Cela démontre que $\bar{f}$ est injectif.

Inversement, supposons que $\bar{f}$ soit injectif et soit $a \in \mathrm{Ker}(f)$; on a $e = f(a) = \bar{f}(p(a))$, donc $p(a) = e$ puisque $\mathrm{Ker}(\bar{f}) = \{e\}$; par suite, $a \in \mathrm{B}$. □

Corollaire **(2.7.11)**. — *Soit* A *un groupe et soit* B *un sous-groupe distingué de* A*, soit* $p : \mathrm{A} \to \mathrm{A/B}$ *la surjection canonique.*

a) *Soit* C *un sous-groupe de* A *contenant* B*. Alors* B *est un sous-groupe distingué de* C *et l'application* $p|_{\mathrm{C}}$ *induit par passage au quotient un isomorphisme de* C/B *sur son image dans* A/B.

b) *L'application* $\mathrm{C} \mapsto p(\mathrm{C})$ *induit une bijection de l'ensemble des sous-groupes de* A *qui contiennent* B *sur l'ensemble des sous-groupes de* A/B*. Sa bijection réciproque est donnée par* $\mathrm{D} \mapsto p^{-1}(\mathrm{D})$.

c) *Pour qu'un sous-groupe* C *de* A *qui contient* B *soit distingué dans* A*, il faut et il suffit que* $p(\mathrm{C})$ *soit un sous-groupe distingué de* A/B*. Alors, l'homomorphisme composé des surjections canoniques de* A *sur* A/B *et de* A/B *sur* $(\mathrm{A/B})/p(\mathrm{C})$ *induit, par passage au quotient, un isomorphisme de* A/C *sur* $(\mathrm{A/B})/p(\mathrm{C})$.

En raison de ce corollaire, on identifiera souvent C/B au sous-groupe $p(\mathrm{C})$ de A/B lorsque C est un sous-groupe de A qui contient B.

Démonstration. — a) L'application $p|_{\mathrm{C}} : \mathrm{C} \to \mathrm{A/B}$ est un homomorphisme de groupes, son noyau est $\mathrm{Ker}(p) \cap \mathrm{C} = \mathrm{B}$ (qui est donc un sous-groupe distingué de C) et son image est $p(\mathrm{C})$. Elle induit donc un isomorphisme de C/B sur $p(\mathrm{C})$.

b) Si C est un sous-groupe de A qui contient B, son image $p(\mathrm{C})$ est un sous-groupe de A/B. Si D est un sous-groupe de A/B, son image réciproque $p^{-1}(\mathrm{D})$ est un sous-groupe de A qui contient B. Pour tout sous-groupe D de A/B, on

c) Si A est commutatif, démontrer que cet homomorphisme est un isomorphisme.

Exercice **(3.13.4)**. — Soit A un anneau.

a) Soit $a \in \mathrm{A}$ un élément nilpotent. Démontrer que $1 + a$ est inversible dans A et calculer son inverse.

b) Soit a, b des éléments de A; on suppose que a est inversible, b nilpotent, et que $ab = ba$. Démontrer que $a + b$ est inversible.

c) Soit a, b des éléments nilpotents de A qui commutent. Démontrer que $a + b$ est nilpotent.

d) Donner des exemples qui montrent que dans les deux questions précédentes, on ne peut pas omettre l'hypothèse que a et b commutent.

Exercice **(3.13.5)**. — Soit A un anneau, soit a et b des éléments de A.

a) On suppose que ab est nilpotent. Démontrer que ba est nilpotent. En déduire une formule reliant les inverses de $1 - ab$ et de $1 - ba$.

b) On suppose que $1 - ab$ est inversible dans A. Démontrer que $1 - ba$ est inversible.

Exercice **(3.13.6)**. — Soit A le sous-anneau de $\mathbf{C}$ engendré par $\sqrt{2}$.

a) Démontrer que pour tout élément a de A, il existe un unique couple (u, v) d'entiers relatifs tels que $a = u + v\sqrt{2}$.

b) Démontrer que le monoïde des endomorphismes de A possède deux éléments, l'identité et l'application donnée par $u + v\sqrt{2} \mapsto u - v\sqrt{2}$.

c) Pour $a = u + v\sqrt{2}$, on pose $\mathrm{N}(a) = u^2 - 2v^2$. Démontrer que $\mathrm{N} : \mathrm{A} \to \mathbf{Z}$ est un homomorphisme de monoïdes multiplicatifs.

d) Démontrer que a est inversible dans A si et seulement si $\mathrm{N}(a) \in \{\pm 1\}$.

e) Soit a un élément inversible de A. On suppose que $1 < a < 3$; démontrer alors que $a = 1 + \sqrt{2}$. Dans le cas général, démontrer qu'il existe un unique entier $n \in \mathbf{Z}$ tel que $|a| = (1 + \sqrt{2})^n$. En déduire que le groupe $\mathrm{A}^\times$ est isomorphe à $\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})$.

Exercice **(3.13.7)**. — Soit A le sous-anneau de $\mathbf{C}$ engendré par $\sqrt[3]{2}$.

a) Démontrer que pour tout $a \in \mathrm{A}$, il existe un unique triple $(u, v, w) \in \mathbf{Z}^3$ tel que $a = u + v\sqrt[3]{2} + w\sqrt[3]{4}$.

l'homomorphisme composé de l'injection de $A[T]$ dans $K[T]$ et de la surjection canonique de $K[T]$ sur $K[T]/(f)_K$. Le noyau de φ contient l'idéal (f) engendré par f dans $A[T]$. Inversement, soit $g \in A[T]$ tel que $\varphi(g) = 0$ et démontrons que $g \in (f)$; soit a le contenu de g et soit $g_1 \in A[T]$ tel que $g = ag_1$. Par hypothèse, il existe alors un polynôme $h \in K[T]$ tel que $g = fh$; soit b, c des éléments non nuls de A et soit $h_1 \in A[T]$ un polynôme primitif tel que $bh_1 = ch$. Alors, $acg_1 = cg = cfh = bh_1$. Par suite, $b = \mathrm{ct}(bh_1)$ divise le contenu de ag qui est égal à ac. □

Corollaire **(3.12.5)**. — *Soit* A *un anneau factoriel. Pour tout entier* $n \in \mathbf{N}$, *l'anneau* $A[T_1, \dots, T_n]$ *est un anneau factoriel.*

Corollaire **(3.12.6)**. — *Soit* K *un corps. Pour tout entier* $n \in \mathbf{N}$, *l'anneau* $K[T_1, \dots, T_n]$ *est un anneau factoriel.*

3.13. Exercices

Exercice **(3.13.1)**. — Soit A un anneau et soit S une partie de A.

a) Démontrer que le centralisateur $Z_S(A)$ de S dans A (pour la structure de monoïde multiplicatif) est un sous-anneau de A.

b) En déduire que le centre de A est un sous-anneau de A.

Exercice **(3.13.2)**. — Soit K un corps, soit V un K-espace vectoriel de dimension n, soit $A = \mathrm{End}_K(V)$ l'anneau des endomorphismes de V et soit $u \in A$.

a) Déterminer $Z_u(A)$ lorsque u est diagonalisable.

b) déterminer $Z_u(A)$ lorsque le polynôme minimal de u est égal à T^n.

c) Démontrer que le centre de A est l'ensemble des endomorphismes de la forme $v \mapsto \lambda v$, pour $\lambda \in K$.

Exercice **(3.13.3)**. — Soit A un anneau. Soit a un élément de a tel que $a^2 = a$ (on dit que a est idempotent).

a) On pose $A_a = aAa$; Démontrer que l'addition et la multiplication de A font de A_a un anneau. Est-ce un sous-anneau de A ?

b) Démontrer que $1 - a$ est idempotent et démontrer que l'addition induit un homomorphisme injectif de l'anneau produit $A_a \times A_{1-a}$ dans A.

a $p(p^{-1}(D)) = D \cap \mathrm{Im}(p) = D$ car p est surjective. De plus, si C est un sous-groupe de A, alors $p^{-1}(p(C))$ est un sous-groupe de A qui contient C. Si de plus C contient B et $a \in p^{-1}(p(C))$, $p(a) \in p(C)$, donc il existe $c \in C$ tel que $p(a) = p(c)$; posons $b = ac^{-1}$; on a $p(b) = p(a)p(c)^{-1} = e$, donc $b \in B$, donc $b \in C$ et $a = bc \in C$, si bien que $p^{-1}(p(C)) = C$.

c) Supposons que C soit un sous-groupe distingué de A et démontrons que $p(C)$ est un sous-groupe distingué de A/B. Soit $x \in A/B$ et $y \in p(C)$; soit $a \in A$ tel que $x = p(a)$ et soit $c \in C$ tel que $y = p(c)$; on a $xyx^{-1} = p(aca^{-1})$; comme C est distingué dans A, on a $aca^{-1} \in C$, donc $xyx^{-1} \in p(C)$, ce qu'il fallait démontrer.

Inversement, supposons que $p(C)$ soit un sous-groupe distingué de A/B et soit $q : (A/B)/p(C)$ la surjection canonique. Le noyau de l'homomorphisme $q \circ p : A \to (A/B)/p(C)$ est égal à $p^{-1}(p(C)) = C$. Cela prouve que C est un sous-groupe distingué de A.

En outre, l'homomorphisme $q \circ p$ induit, par passage au quotient, un isomorphisme de A/C sur $(A/B)/p(C)$. □

Corollaire **(2.7.12)**. — *Soit* A *un groupe, soit* B *et* C *des sous-groupes de* A*; supposons que* B *soit distingué dans* A *et notons* p *la surjection canonique de* A *sur* A/B. *Alors* BC *est un sous-groupe de* A *dont* B *est un sous-groupe distingué,* $B \cap C$ *est un sous-groupe distingué de* C *et l'injection de* C *dans* A *induit, par passage aux quotients, un isomorphisme de* $C/(B \cap C)$ *sur* BC/B.

Démonstration. — L'application $p|_C$ est un homomorphisme de groupes d'image $p(C)$ et de noyau $B \cap C$; cela prouve que $B \cap C$ est un sous-groupe distingué de C et que $p|_C$ induit un isomorphisme de $C/(B \cap C)$ sur $p(C)$. Par ailleurs, on a $p^{-1}(C) = BC$: l'inclusion $BC \subset p^{-1}(C)$ est évidente ; inversement, si $a \in p^{-1}(C)$, soit $c \in C$ tel que $p(a) = p(c)$ et posons $b = ac^{-1}$; alors $p(b) = e$, donc $b \in B$, ce qui prouve que $a \in BC$. En particulier, BC est un sous-groupe de A qui contient B. Ainsi, $p|_{BC}$ induit un isomorphisme de BC/B sur $p(C)$. Cela entraîne le corollaire. □

Corollaire **(2.7.13)**. — *Soit* $(A_i)_{i \in I}$ *une famille de groupes, pour tout* $i \in I$, *soit* B_i *un sous-groupe distingué de* A_i *et soit* $f_i : A_i \to A_i/B_i$ *la surjection canonique. L'application* f *de* $\prod_{i \in I} A_i$ *dans* $\prod_{i \in I}(A_i/B_i)$ *donnée par* $f((a_i)) = (f_i(a_i))$ *est un homomorphisme de groupes, surjectif, et son noyau est égal à* $\prod_{i \in I} B_i$. *Par*

passage au quotient, l'homomorphisme f induit un isomorphisme de groupes de $(\prod_{i\in I} A_i)/(\prod_{i\in I} B_i)$ sur $\prod_{i\in I}(A_i/B_i)$.

Démonstration. — Pour tout $i \in I$, notons e_i l'élément neutre de A_i ; l'élément neutre de $\prod_{i\in I} A_i$ est la famille (e_i) et son image par f est l'élément neutre de $\prod_{i\in I}(A_i/B_i)$. Soit $a = (a_i)$ et $b = (b_i)$ des éléments de $\prod_{i\in I} A_i$; on a

$$f(ab) = f((a_i)(b_i)) = f((a_ib_i)) = (f_i(a_ib_i)) = (f_i(a_i))(f_i(b_i)) = f(a)f(b),$$

si bien que f est un homomorphisme de groupes. Pour qu'un élément $a = (a_i)$ appartienne au noyau de f, il faut et il suffit que, pour tout $i \in I$, on ait $f_i(a_i) = e$, c'est-à-dire $a_i \in B_i$. Par suite, $\mathrm{Ker}(f) = \prod_{i\in I} B_i$. □

2.7.14. — Le *groupe dérivé* $D(A)$ de A est le sous-groupe de A engendré par les commutateurs d'éléments de A.

Démontrons que c'est un sous-groupe *caractéristique* de A. Notons S l'ensemble des commutateurs d'éléments de A. Soit u, v des éléments de A et f un automorphisme de A ; on a

$$\begin{aligned} f([u,v]) &= f(u^{-1}v^{-1}uv) \\ &= f(u)^{-1}f(v)^{-1}f(u)f(v) \\ &= [f(u), f(v)], \end{aligned}$$

ce qui prouve que $f(S) \subset S$. Appliquons ce raisonnement à l'automorphisme f^{-1}. On a donc $f^{-1}(S) \subset S$, d'où, appliquant f, l'inclusion $S \subset f(S)$. Par suite, $S = f(S)$. Comme $f(D(A))$ est le sous-groupe de A engendré par $f(S)$, on a $f(D(A)) = D(A)$.

En particulier, $D(A)$ est un sous-groupe distingué de A.

Notons $p : A \to A/D(A)$ l'homomorphisme surjectif canonique. Pour tout couple (a, b) d'éléments de A, on a $[p(a), p(b)] = p([a, b]) = p(e) = e$. Par suite, le groupe $A/D(A)$ est commutatif.

Proposition **(2.7.15)** (Propriété universelle du quotient par le groupe dérivé)

Soit A *un groupe. Pour tout groupe abélien* B *et tout morphisme de groupes $f : A \to B$, il existe un unique homomorphisme de groupes $\varphi : A/D(A) \to B$ tel que $f = \varphi \circ p$.*

Définition **(2.7.16)**. — *On dit qu'un groupe* A *est* simple *s'il n'est pas réduit à l'élément neutre et si ses seuls sous-groupes distingués sont $\{e\}$ et* A.

si bien que h est un polynôme constant, de valeur $a \in A$. Puisque a et $\mathrm{ct}(h)$ sont associés, a n'est pas irréductible. De même toute factorisation non triviale $a = bc$ dans A est une factorisation non triviale dans $A[T]$. Cela démontre donc que est irréductible. □

Théorème **(3.12.4)** (Gauß). — *Si* A *est un anneau factoriel, l'anneau* $A[T]$ *est un anneau factoriel.*

Démonstration. — On note K le corps des fractions de A. Si f est un élément de $A[T]$, on note $(f)_K$ l'idéal principal de $K[T]$ engendré par f.

Soit (f_n) une suite d'éléments de $A[T]$ tels que la suite d'idéaux principaux $((f_n))$ soit croissante.

La suite des idéaux $((\mathrm{ct}(f_n)))$ engendrés par les contenus des f_n est croissante ; comme l'anneau A est factoriel, cette suite est stationnaire. Soit m un entier tel que $(\mathrm{ct}(f_n)) = (\mathrm{ct}(f_m))$ pour tout entier $n \geqslant m$. Soit $c = \mathrm{ct}(f_m)$; pour tout $n \geqslant m$, définissons un polynôme $g_n \in A[T]$ par la formule $f_n = cg_n$. La suite d'idéaux $((g_n))_{n\geqslant m}$ est encore croissante.

Comme $K[T]$ est un anneau principal, c'est un anneau factoriel et la suite correspondante $((g_n)_K)$ d'idéaux principaux de $K[T]$ est stationnaire. Il existe donc un entier $p \geqslant m$ tel que, pour tout entier $n \geqslant p$, g_n et g_p soient associés dans $K[T]$.

Soit n un entier $\geqslant p$. Soit $\lambda \in K$ tel que $g_n = \lambda g_p$; soit $a, b \in A$ tels que $\lambda = a/b$. L'égalité $ag_p = bf_n$ dans $A[T]$ entraîne l'égalité de leurs contenus. Comme g_n et g_p sont primitifs, le membre de gauche est de contenu a, et celui de droite de contenu b. Il s'ensuit que les éléments a et b sont associés dans A, d'où $\lambda \in A^\times$. Par suite, g_n et g_p sont associés dans $A[T]$.

Pour $n \geqslant p$, on a ainsi $(f_n) = (cg_n) = c(g_n) = c(g_p) = (f_p)$, ce qui démontre que la suite d'idéaux principaux (f_n) de $A[T]$ est stationnaire.

Soit maintenant f un élément irréductible de $A[T]$; démontrons que l'idéal (f) est premier.

Si f est un élément irréductible a de A, alors $A[T]/(f)$ est isomorphe à $(A/(a))[T]$. L'anneau A étant factoriel, l'idéal (a) est premier et $A/(a)$ est un anneau intègre ; par suite, $(A/(a))[T]$ est un anneau intègre et (f) est un idéal premier de $A[T]$.

Dans l'autre cas, f est un polynôme primitif qui est irréductible dans $K[T]$. Notons $(f)_K$ l'idéal de $K[T]$ engendré par f et $\varphi : A[T] \to K[T]/(f)_K$

Proposition **(3.12.3)**. — *Soit* A *un anneau factoriel et soit* K *son corps des fractions. Les éléments irréductibles de* A *sont les polynômes constants, de valeur un élément irréductible de* A*, et les polynômes primitifs de* A[T] *qui sont irréductibles dans* K[T].

Démonstration. — Démontrons d'abord que les éléments indiqués sont irréductibles.

Soit p un élément irréductible de A. Tout d'abord, p n'est pas inversible car pour tout polynôme $f \in A[T]$, le terme constant de pf est multiple de p, donc n'est pas inversible. Soit ensuite $f, g \in A[T]$ des polynômes tels que $fg = p$; on a donc $\deg(f) + \deg(f) = 0$, donc $\deg(f) = \deg(g) = 0$ si bien que f et g sont constants. Comme A est factoriel, f ou g est un élément inversible de A, donc un élément inversible de A[T].

Soit $h \in A[T]$ un polynôme primitif qui est irréductible dans K[T]. En particulier, h n'est pas inversible dans K[T], donc h n'est pas inversible dans A[T]. Soit ensuite f, g des éléments de A[T] tels que $h = fg$. Vue dans K[T], cette égalité entraîne que f ou g est inversible dans K[T], donc est de degré 0. Supposons que ce soit f; alors f est un élément de A qui divise le contenu de h, donc est inversible puisque $\mathrm{ct}(h) = 1$ par hypothèse.

Soit maintenant h un élément irréductible de A[T]. Démontrons que h est de l'une des deux formes indiquées. Soit h_1 un polynôme de A[T] tel que $h = \mathrm{ct}(h)h_1$. Puisque h est irréductible, ou bien $\mathrm{ct}(h)$, ou bien h_1 est inversible.

Supposons que $\mathrm{ct}(h)$ soit inversible et démontrons que h est irréductible dans K[T]. Si l'on avait $\deg(h) = 0$, alors h serait un polynôme constant de terme constant inversible, donc serait inversible. Par suite, $\deg(h) > 0$ et h n'est pas inversible dans K[T]. Soit $f, g \in K[T]$ tels que $h = fg$. Soit a' un élément non nul tel que $af \in A[T]$; soit $a'' = \mathrm{ct}(a'f)$ et soit $f_1 \in A[T]$ tel que $a'f = a''f_1$; on a donc $\mathrm{ct}(f_1) = 1$ et $f = (a''/a')f_1$. De même, il existe un polynôme primitif $g_1 \in A[T]$ et des élément $b', b'' \in A - \{0\}$ tels que $g = (b'/b'')g_1$. L'égalité $h = fg$ entraîne l'égalité $a''b''h = a'b'f_1g_1$. Comparons les contenus des deux membres, $a'b'$ et $a''b''$ sont associés, si bien qu'il existe un élément inversible $u \in A^\times$ tel que $a'b' = ua''b''$, d'où $h = uf_1g_1$. Comme h est irréductible dans A[T], f_1 ou g_1 est inversible dans A[T], donc de degré 0. Par suite, f ou g est non nul et de degré 0, donc inversible dans K[T].

Supposons maintenant que $\mathrm{ct}(h)$ ne soit pas inversible. Dans ce cas, l'égalité $h = \mathrm{ct}(h)h_1$ et l'irréductibilité de h entraîne que h_1 est inversible dans A[T],

2.8. Groupes et monoïdes libres, coproduits

2.8.1. — Soit S un ensemble. On note M(S) l'ensemble des suites finies (éventuellement vide) d'élements de S; un élément $(m_1, \dots, m_n)$ de M(S) est appelé *mot* sur l'ensemble S; l'entier n est appelé sa *longueur*. On munit l'ensemble M(S) de la loi de composition donnée par

$$(s_1, \dots, s_m)(t_1, \dots, t_n) = (s_1, \dots, s_m, t_1, \dots, t_n)$$

si $m, n \in \mathbf{N}$ et $s_1, \dots, s_m, t_1, \dots, t_n$ sont des éléments de S. Cette loi est associative et possède la suite vide $\varepsilon = ()$ pour élément neutre. Ainsi, M(S) est un monoïde, qu'on appelle le *monoïde libre* sur l'ensemble S.

On note j l'application de S dans M(S) donnée par $j(s) = (s)$. Elle est injective et son image $j(S)$ engendre M(S).

Proposition **(2.8.2)** (Propriété universelle du monoïde libre)

Soit S *un ensemble, soit* A *un monoïde et soit* $f : S \to A$ *une application. Il existe un unique morphisme de monoïdes* $\varphi : M(S) \to A$ *tel que* $\varphi \circ j = f$.

Démonstration. — Définissons une application $\varphi : M(S) \to A$ en posant $\varphi(x) = f(s_1) \dots f(s_n)$ pour $x = (s_1, \dots, s_n) \in M(S)$. On a $\varphi(\varepsilon) = e$; si $x = (s_1, \dots, s_m)$ et $y = (t_1, \dots, t_n)$ sont des éléments de M(S), on a $xy = (s_1, \dots, s_m, t_1, \dots, t_n)$, d'où

$$\begin{aligned}\varphi(xy) &= \varphi\big((s_1, \dots, s_m, t_1, \dots, t_n)\big)\\ &= f(s_1) \dots f(s_m) f(t_1) \dots f(t_n)\\ &= \varphi(x)\varphi(y).\end{aligned}$$

Cela prouve que φ est un morphisme de monoïdes. Pour $s \in S$, on a évidemment $\varphi(j(s)) = \varphi\big((s)\big) = f(s)$, donc $\varphi \circ j = f$.

Enfin, si $\varphi' : M(S) \to A$ est un morphisme de monoïdes tel que $\varphi \circ j = \varphi' \circ j$, φ et φ' coïncident sur l'image $j(S)$ de S. Comme cette image engendre M(S) et que $\mathrm{Ker}(\varphi, \varphi')$ est un sous-monoïde de M(S), on a $\varphi = \varphi'$. □

2.8.3. — Soit S un ensemble et soit S′ une autre copie (disjointe) de l'ensemble S; pour $s \in S$, l'élément correspondant de S est noté s'. Soit M′(S) le monoïde libre sur l'ensemble $S \cup S'$ et soit $j' : S \cup S' \to M'(S)$ l'injection canonique. Soit $\sim$ la plus petite relation d'équivalence dans M′(S) qui est compatible avec sa structure de monoïde pour laquelle $ss' \sim e$ et $s's \sim e$ pour tout $s \in S$ et soit F(S) le

monoïde quotient. On note $j : S \to F(S)$ l'application qui, à $s \in S$, associe la classe dans $F(S)$ de l'élément s de $M'(S)$.

Soit p la surjection canonique de $M'(S)$ sur $F(S)$. Par construction, on a $p(s)p(s') = p(s')p(s) = e$, pour tout $s \in S$, donc les éléments $p(s)$ et $p(s')$ de $F(S)$ sont inversibles. Par récurrence sur la longueur d'un élément m de $M'(S)$, son image $p(m)$ dans $F(S)$ est inversible, ce qui prouve que $F(S)$ est un groupe.

En outre, le groupe $F(S)$ est engendré (comme groupe) par $j(S)$.

Proposition **(2.8.4)** (Propriété universelle du groupe libre)
Pour tout groupe A *et toute application* $f : S \to A$, *il existe un unique morphisme de groupes* $\varphi : F(S) \to A$ *tel que* $\varphi \circ j = f$.

Démonstration. — Soit $f : S \to A$ une application. Soit $f' : S \cup S' \to A$ l'application telle que $f'(s) = f(s)$ et $f'(s') = f(s)^{-1}$ pour tout $s \in S$. Il existe un unique morphisme de monoïdes $\varphi' : M'(S) \to A$ tel que $\varphi' \circ j' = f'$. La relation d'équivalence définie par φ' (pour laquelle $m \equiv m'$ si et seulement si $\varphi'(m) = \varphi'(m')$) est compatible avec la structure de monoïde de $M'(S)$; comme $\varphi'(ss') = f'(s)f'(s') = f(s)f(s)^{-1} = e$ et $\varphi'(s's) = f'(s')f'(s) = f(s)^{-1}f(s) = e$, on a $ss' \equiv e$ et $s's \equiv e$. Par suite, cette relation d'équivalence est moins fine que la relation $\sim$ et il existe une application $\varphi : F(S) \to A$ telle que $\varphi(p(m)) = \varphi'(m)$ pour tout $m \in M'(S)$. L'application φ est un morphisme de magmas et vérifie $\varphi(e) = e$; c'est donc un morphisme de groupes.

Comme $j(S)$ engendre le groupe $F(S)$, deux morphismes de groupes de $F(S)$ dans A qui coïncident sur S sont égaux, si bien que tout morphisme de groupes $\psi : F(S) \to A$ tel que $\psi \circ j = f$ est égal à φ. □

2.8.5. — Pour mieux appréhender le groupe $F(S)$, il est important de comprendre à quelle condition deux mots de $M'(S)$ ont même image dans $F(S)$. On dit pour cela qu'un mot $m = (m_1, \dots, m_n) \in M'(S)$ est *réduit* s'il n'existe pas d'entier $i \in \{1, \dots, n-1\}$ et d'élément $s \in S$ tel que $(m_i, m_{i+1}) = (s, s')$ ou $(m_i, m_{i+1}) = (s', s)$.

Observons que $j'(m_i)j'(m_{i+1}) = p(s)p(s)^{-1} = e$ ou $j'(m_i)j'(m_{i+1}) = p(s)^{-1}p(s) = e$, si bien que le mot $m' = (m_1, \dots, m_{i-1}, m_{i+2}, \dots, m_n)$ a même image que m dans $F(S)$.

Proposition **(2.8.6)**. — *Tout élément de* $F(S)$ *est l'image d'un* unique *mot réduit par p.*

on a $v_p(a) \leqslant v_p(c)$ et $v_p(b) \leqslant v_p(c)$. Comme p ne divise pas simultanément a et b, on a $v_p(a) = 0$ ou $v_p(b) = 0$. Par suite, $v_p(ab) = v_p(a) + v_p(b) \leqslant v_p(c)$. Comme p est arbitraire, cela entraîne que ab divise c.

b) Supposons $b = 0$. Comme a est un pgcd de a et 0, l'hypothèse que a et b sont premiers entre eux entraîne que a est inversible ; l'assertion est alors évidente. On suppose dans la suite que $b \neq 0$.

Par hypothèse, a divise bc, et b divise bc ; d'après la première assertion, ab divise bc. Soit $q \in A$ tel que $bc = qab$. Puisque $b \neq 0$, on a donc $c = qa$, donc a divise c. □

3.12. Caractère factoriel des anneaux de polynômes

Définition **(3.12.1)**. — *Soit* A *un anneau factoriel. Pour tout polynôme* $f \in A[T]$, *on appelle* contenu *de* f *un plus grand diviseur commun de ses coefficients ; on le note* $\mathrm{ct}(f)$. *On dit qu'un polynôme de* $A[T]$ *est* primitif *si son contenu est inversible.*

Si f est un polynôme non nul de $A[T]$, son contenu n'est pas nul et on peut écrire $f = \mathrm{ct}(f)f_1$, où $f_1 \in A[T]$ est un polynôme primitif.

Proposition **(3.12.2)**. — *Soit* A *un anneau factoriel. Soit* f, g *des éléments de* $A[T]$. *Alors* $\mathrm{ct}(fg)$ *et* $\mathrm{ct}(f)\,\mathrm{ct}(g)$ *sont associés. En particulier, si* f *et* g *sont primitifs, alors* fg *est primitif.*

Démonstration. — Supposons d'abord que f et g sont primitifs et démontrons que fg est primitif. Soit p un élément irréductible de A et soit $\varphi : A \to A/(p)$ l'homomorphisme canonique de A dans l'anneau quotient $A/(p)$. Notons encore φ l'homomorphisme de $A[T]$ dans $A/(p)[T]$ qui applique un polynôme $\sum a_n T^n$ sur $\sum \varphi(a_n)T^n$. Par hypothèse, $\varphi(f) \neq 0$ et $\varphi(g) \neq 0$; comme A est un anneau factoriel, l'idéal (p) est un premier et l'anneau $(A/(p))$ est intègre ; par suite, $(A/(p))[T]$ est un anneau intègre, donc $\varphi(fg) = \varphi(f)\varphi(g) \neq 0$. Cela entraîne que p ne divise pas tous les coefficients de fg, donc que p ne divise pas $\mathrm{ct}(fg)$. Puisque ceci vaut pour tout élément irréductible p de A, le polynôme fg est primitif.

Traitons maintenant le cas général. Soit f_1 et g_1 des polynômes tels que $f = \mathrm{ct}(f)f_1$ et $g = \mathrm{ct}(g)g_1$. On a alors $\mathrm{ct}(f_1) = 1$, $\mathrm{ct}(g_1) = 1$ et $fg = \mathrm{ct}(f)\,\mathrm{ct}(g)f_1g_1$, donc $\mathrm{ct}(fg) = \mathrm{ct}(f)\,\mathrm{ct}(g)\,\mathrm{ct}(f_1g_1) = \mathrm{ct}(f)\,\mathrm{ct}(g)$. □

n'en dépend qu'à multiplication par un élément inversible près. Autrement dit, l'idéal principal (d) est le plus petit idéal principal qui contient l'idéal $((a_i))$ engendré par les a_i.

De même, l'élément m vérifie la propriété suivante : *pour qu'un élément a de* A *soit multiple de chacun des a_i, il faut et il suffit qu'il soit multiple de m.* En effet, chacune des assertions équivaut à la suivante :

a) Pour tout i, a est multiple de a_i ;
b) Pour tout p et pour tout i, on a $v_p(a) \leqslant v_p(a_i)$;
c) Pour tout p, on a $v_p(a) \leqslant m_p$;
d) L'élément a est multiple de m.

On dit que m est un *plus petit multiple commun* de la famille (a_i) et on note (par abus) $m = \mathrm{ppcm}((a_i))$. Il dépend des choix faits pour l'ensemble $\mathscr{P}$, mais n'en dépend qu'à multiplication par un élément inversible près. Autrement dit, l'idéal principal (m) est l'intersection $\bigcap_i (a_i)$ des idéaux (a_i).

On déduit de ces définitions des propriétés d'associativité pour le plus grand diviseur commun et le plus petit multiple commun, comme $\mathrm{pgcd}(\mathrm{pgcd}(a,b),c) = \mathrm{pgcd}(a,b,c)$. De même, on a $\mathrm{pgcd}(a(a_i)) = a\,\mathrm{pgcd}(a_i)$ et $\mathrm{ppcm}(a(a_i)) = a\,\mathrm{ppcm}(a_i)$.

On dit que les a_i sont *premiers entre eux* si leur plus grand diviseur commun est inversible. Si d est un plus grand diviseur commun de la famille (a_i), non nul, alors les a_i/d sont premiers entre eux.

Remarque **(3.11.15)**. — Soit A un anneau principal. Soit $(a_i)_{i\in I}$ une famille d'éléments de A et soit a un générateur de l'idéal engendré par les a_i. Alors, a est un plus grand diviseur commun de la famille (a_i). En particulier, il existe une famille $(u_i)_{i\in I}$ presque nulle telle que $a = \sum u_i a_i$.

Lorsque A est un anneau euclidien, l'algorithme d'Euclide fournit donc un moyen algorithmique de calcul du plus grand diviseur commun.

Proposition **(3.11.16)**. — *Soit* A *un anneau factoriel, soit a, b, c des éléments de* A. *On suppose que a et b sont premiers entre eux.*

a) *Si a et b divisent c, alors ab divise c.*
b) *Si a divise bc, alors a divise c.*

Démonstration. — a) L'assertion est évidente si $c = 0$. On peut donc supposer que a, b, c ne sont pas nuls. Soit p un élément irréductible de A. Par hypothèse,

Démonstration (van der Waerden). — Soit $\mathrm{M}'(\mathrm{S})_0$ l'ensemble des mots réduits de $\mathrm{M}'(\mathrm{S})$. On va faire opérer S dans $\mathrm{M}'(\mathrm{S})_0$ de la façon suivante. Soit $s \in \mathrm{S}$ et soit $m = (m_1, \dots, m_n) \in \mathrm{M}'(\mathrm{S})_0$;

– Si $m_1 = s'$, on pose $s \cdot m = (m_2, \dots, m_n)$;
– Si $m_1 \neq s'$, on pose $s \cdot m = (s, m_1, \dots, m_n)$.

On remarque d'abord que $s \cdot m \in \mathrm{M}'(\mathrm{S})_0$ pour tout $s \in \mathrm{S}$ et tout $m \in \mathrm{M}'(\mathrm{S})_0$. Fixons alors $s \in \mathrm{S}$ et vérifions que l'application $m \mapsto s \cdot m$ est une permutation de $\mathrm{M}'(\mathrm{S})_0$. Soit donc $m = (m_1, \dots, m_n) \in \mathrm{M}'(\mathrm{S})_0$; si $m_1 = s$, on a $m' = (m_2, \dots, m_n) \in \mathrm{M}'(\mathrm{S})_0$ et $m_2 \neq s'$, donc $s \cdot m' = (s, m_2, \dots, m_n) = m$; inversement, si $m_1 \neq s$, alors $m' = (s', m_1, \dots, m_n)$ appartient à $\mathrm{M}'(\mathrm{S})_0$ et $s \cdot m' = m$. De plus, l'élément m' donné est l'unique élément de $\mathrm{M}'(\mathrm{S})_0$ tel que $s \cdot m' = m$. Notons alors $\alpha : \mathrm{S} \to \mathfrak{S}(\mathrm{M}'(\mathrm{S})_0)$ l'application qui associe à $s \in \mathrm{S}$ la permutation $m \mapsto s \cdot m$ ainsi définie.

Par la propriété universelle du groupe libre, il existe un unique morphisme de groupes $\alpha : \mathrm{F}(\mathrm{S}) \to \mathfrak{S}(\mathrm{M}'(\mathrm{S})_0)$ tel que $a = \alpha \circ j$. Si $x \in \mathrm{F}(\mathrm{S})$ et $m \in \mathrm{M}'(\mathrm{S})_0$, on note $x \cdot m = \alpha(x)(m)$.

Vérifions par récurrence sur n que l'on a $p(m) \cdot \varepsilon = m$ pour tout $m = (m_1, \dots, m_n) \in \mathrm{M}'(\mathrm{S})_0$. L'assertion est vraie si $n = 0$, car alors $m = \varepsilon$ et $p(m) = e$. Supposons $n \geqslant 1$ et l'assertion vraie pour $n-1$; posons $m' = (m_2, \dots, m_n)$; c'est un élément de $\mathrm{M}'(\mathrm{S})_0$. Par récurrence, on a donc

$$p(m) \cdot \varepsilon = \big(p(m_1)p(m')\big) \cdot \varepsilon = p(m_1) \cdot \big(p(m') \cdot \varepsilon\big) = m_1 \cdot m'.$$

Soit alors s l'élément de S tel que $m_1 = s$ ou s' ; si $m_1 = s$, on a $\alpha(p(m_1)) = a(s)$ et $m_2 \neq s'$, d'où

$$p(m) \cdot \varepsilon = m_1 \cdot m' = m_1 \cdot (m_2, \dots, m_n) = (m_1, m_2, \dots, m_n) = m;$$

sinon, $m_1 = s'$, donc $p(m_1) = p(s)^{-1}$ et $m_2 \neq s$, si bien que

$$s \cdot m = s \cdot (m_1, \dots, m_n) = s \cdot (s', m_2, \dots, m_n) = (m_2, \dots, m_n) = m'$$

d'où $p(m) \cdot \varepsilon = p(s)^{-1} \cdot m' = m$.

Soit maintenant $x \in \mathrm{F}(\mathrm{S})$ et soit $m \in \mathrm{M}'(\mathrm{S})$ un mot de longueur minimale tel que $p(m) = x$; nécessairement m est réduit. D'autre part, si $m \in \mathrm{M}'(\mathrm{S})_0$ est un mot réduit tel que $p(m) = x$, on a $x \cdot \varepsilon = p(m) \cdot \varepsilon = m$. Ainsi, $x \cdot \varepsilon$ est l'unique mot réduit dont l'image dans $\mathrm{F}(\mathrm{S})$ est égale à x. □

Corollaire **(2.8.7)**. — a) *L'application $j : \mathrm{S} \to \mathrm{F}(\mathrm{S})$ est injective.*

b) *Le groupe* $\mathrm{F}(\mathrm{S})$ *est sans torsion.*
c) *Si* $\mathrm{Card}(\mathrm{S}) \geqslant 2$, *le centre de* $\mathrm{F}(\mathrm{S})$ *est réduit à l'élément neutre.*

Démonstration. — a) Pour deux éléments s, t de S tels que $s \neq t$, les mots (s) et (t) sont réduits et distincts, donc leurs images $j(s)$ et $j(t)$ dans $\mathrm{F}(\mathrm{S})$ sont distinctes. Cela prouve que j est injective.

b) Soit g un élément de $\mathrm{F}(\mathrm{S})$ distinct de e et soit $(s_1, \dots, s_n) \in \mathrm{M}'(\mathrm{S})_0$ l'unique mot réduit d'image g. On démontre par récurrence sur n que $g^d \neq e$ pour tout entier $d \geqslant 1$.

Il y a trois cas. Supposons d'abord que (s_1, s_n) ne soit pas de la forme (s, s') ou (s', s), pour $s \in \mathrm{S}$. Dans ce cas, le mot $(s_1, \dots, s_n, s_1, \dots, s_n, \dots, s_1, \dots, s_n) = (s_1, \dots, s_n)^d$ est réduit, pour tout $d \geqslant 1$, et n'est pas le mot vide ; comme son image est égale à g^d, cela entraîne que $g^d \neq e$. Supposons ensuite que s_1 soit un élément s de S et que $s_n = s'$, posons alors $h = (m_2, \dots, m_{n-1})$; on a $g = j(s)hj(s)^{-1}$. Comme la longueur de h est strictement inférieure à celle de g, on a $h^d \neq e$; par suite, $g^d = j(s)h^d j(s)^{-1} \neq e$ pour $d \geqslant 1$. Enfin, si s_n est un élément s de S et $s_1 = s'$, on pose encore $h = (m_2, \dots, m_{n-1})$ et la relation $g = j(s)^{-1}hj(s)$ permet de démontrer de façon analogue que $g^d \neq e$ pour $d \geqslant 1$.

c) Soit g un élément de $\mathrm{F}(\mathrm{S})$ différent de l'élément neutre et soit $(s_1, \dots, s_n)$ l'unique mot réduit d'image g ; on a $n \geqslant 1$. Comme $\mathrm{Card}(\mathrm{S}) \geqslant 2$, il existe un élément $t \in \mathrm{S}$ tel que $s_1 \neq t$ et $s_1 \neq t'$. Alors, $(t, s_1, \dots, s_n)$ est un mot réduit d'image $j(t)g$, et $(s_1, \dots, s_n, t)$ est un mot réduit d'image $gj(t)$. Comme le premier mot débute par t et le second par s_1 (c'est là qu'on utilise l'hypothèse que $g \neq e$), on a $j(t)g \neq gj(t)$, ce qui prouve que g n'appartient pas au centre de $\mathrm{F}(\mathrm{S})$. Ainsi, $\mathrm{Z}(\mathrm{F}(\mathrm{S})) = \{e\}$.

□

2.8.8. — Désormais, on notera s^{-1} le symbole que l'on notait jusque là s' ; on note aussi S^{-1} l'ensemble S'.

Soit R une partie de $\mathrm{M}'(\mathrm{S}) = \mathrm{M}(\mathrm{S} \cup \mathrm{S}^{-1})$ et soit K le plus petit sous-groupe distingué de $\mathrm{F}(\mathrm{S})$ qui contient son image. Soit $\mathrm{G}(\mathrm{S}; \mathrm{R})$ le groupe quotient $\mathrm{F}(\mathrm{S})/\mathrm{K}$; on dit que c'est le groupe défini par l'ensemble générateur S et l'ensemble de relateurs R et on le note parfois $\langle \mathrm{S} \mid \mathrm{R} \rangle$.

On note encore j l'application de S dans $\mathrm{G}(\mathrm{S}; \mathrm{R})$ qui applique un élément $s \in \mathrm{S}$ sur la classe de $p(s)$. Son image engendre $\mathrm{G}(\mathrm{S}; \mathrm{R})$.

d) Soit $a, b \in \mathrm{A}$. Si $a = 0$ ou $b = 0$, on a $ab = 0$ et $v_p(ab) = +\infty = v_p(a) + v_p(b)$ car l'un des deux est infini. Supposons que a et b ne sont pas nuls ; on obtient une décomposition en facteurs irréductibles du produit ab en regroupant des décompositions en facteurs irréductibles de a et b. Le nombre de facteurs associés à p dans cette décomposition de ab est ainsi la somme du nombre de tels facteurs pour a et pour b, c'est-à-dire $v_p(ab) = v_p(a) + v_p(b)$. □

3.11.14. — Soit A un anneau factoriel. Soit $\mathscr{P}$ une famille d'éléments irréductibles de A telle que tout élément irréductible de A soit associé à l'un des éléments de $\mathscr{P}$, et un seul. Pour tout élément non nul a de A, l'ensemble des éléments irréductibles $p \in \mathscr{P}$ tels que $v_p(a) \geqslant 1$ est fini et il existe un unique élément inversible $u \in \mathrm{A}^\times$ tel que

$$a = u \prod_{p \in \mathscr{P}} p^{v_p(a)}. \tag{3.11.14.1}$$

Soit a, b des éléments de A. Si b divise a, il existe $c \in \mathrm{A}$ tel que $a = bc$ et l'on $v_p(a) = v_p(b) + v_p(c) \geqslant v_p(b)$ pour tout $p \in \mathscr{P}$. Inversement, si $v_p(a) \geqslant v_p(b)$ pour tout $p \in \mathscr{P}$, $\prod_{p \in \mathscr{P}} p^{v_p(a)}$ est multiple de $\prod_{p \in \mathscr{P}} p^{v_p(b)}$, donc a est mutiple de b.

Soit $(a_i)_{i \in \mathrm{I}}$ une famille d'éléments de A. Pour tout $p \in \mathscr{P}$, notons $d_p = \inf_i v_p(a_i)$ et $m_p = \sup_i v_p(a_i)$.

Si la famille (a_i) est identiquement nulle, on pose $d = 0$. Sinon, on a $d_p \in \mathbf{N}$ pour tout $p \in \mathscr{P}$ et l'ensemble des $p \in \mathscr{P}$ tels que $d_p \neq 0$ est fini ; on pose alors $a = \prod_{p \in \mathscr{P}} p^{d_p}$. Ainsi, on a $v_p(d) = \inf_{i \in \mathrm{I}} v_p(a_i)$ pour tout $p \in \mathscr{P}$.

S'il existe $p \in \mathscr{P}$ tel que $m_p = +\infty$, ou si l'ensemble des $p \in \mathscr{P}$ tels que $m_p \neq 0$ est infini, on pose $m = 0$. Sinon, la famille (m_p) appartient à $\mathbf{N}^{(\mathscr{P})}$ et on pose $m = \prod_{p \in \mathscr{P}} p^{m_p}$. On a donc $v_p(m) = \sup_{i \in \mathrm{I}} v_p(a_i)$ pour tout $p \in \mathscr{P}$.

L'élément d vérifie la propriété suivante : *pour qu'un élément a de* A *divise chacun des a_i, il faut et il suffit qu'il divise d.* En effet, chacune des assertions équivaut à la suivante :

a) Pour tout i, b divise a_i ;
b) Pour tout p et pour tout i, on a $v_p(b) \leqslant v_p(a_i)$;
c) Pour tout p, on a $v_p(b) \leqslant d_p$;
d) L'élément b divise d.

On dit que d est un *plus grand diviseur commun* de la famille (a_i) et on note (par abus) $d = \mathrm{pgcd}((a_i))$. Il dépend des choix faits pour l'ensemble $\mathscr{P}$, mais

que $\omega(a_n) = \omega(a_m)$ pour $n \geqslant m$; pour $n \geqslant m$, soit $b \in A$ tel que $a_n = ba_m$; on a $\omega(b) = 0$, donc b est inversible et $(a_n) = (a_m)$. Cela prouve que la suite $((a_n))$ d'idéaux est stationnaire.

Soit p un élément irréductible de A ; démontrons que l'idéal (p) est premier. On a $(p) \neq A$, car p n'est pas inversible. Soit a, b des éléments de A tels que $ab \in (p)$ et soit $c \in A$ tel que $ab = pc$. Considérons des décompositions en produit d'éléments irréductibles de a, b, c : disons $a = u\prod_{i=1}^{m} p_i$, $b = v\prod_{j=1}^{n} q_j$ et $c = w\prod_{k=1}^{s} r_k$. L'égalité $ab = pc$ s'écrit $uv\prod_{i=1}^{m} p_i \prod_{j=1}^{n} q_j = wp\prod_{k=1}^{s} r_k$. D'après la propriété d'unicité, il existe un élément inversible e de A tel que ep soit égal à l'un des p_i ou des q_j ; dans le premier cas, a est multiple de p, dans le second, b est multiple de p. Par suite, l'idéal (p) est premier, ce qu'il fallait démontrer. □

3.11.12. — Soit A un anneau commutatif intègre. On dit que deux éléments non nuls a et b de A sont associés s'il existe un élément inversible u de A tel que $b = au$. C'est une relation d'équivalence dans $A - \{0\}$; ses classes d'équivalence sont les orbites de l'action par multiplication de $A^\times$ dans A.

Soit A un anneau factoriel. Soit p un élément irréductible de A et, pour $a \in A$, posons $v_p(a) = \sup\{n \in \mathbf{N} ; a \in (p^n)\}$. Si $a \neq 0$, dire que $v_p(a) \geqslant n$ signifie que dans une décomposition $a = up_1 \dots p_m$ de a en produits d'éléments irréductibles, il existe une partie $I \subset \{1, \dots, m\}$ de cardinal n telle que p et p_i soient associés pour tout $i \in I$.

Si q est un élément irréductible de A, alors $v_p = v_q$ si et seulement si p et q sont associés.

Proposition **(3.11.13)**. — *Soit* A *un anneau factoriel et soit* p *un élément irréductible de* A. *Les propriétés suivantes sont vérifiées :*

a) $v_p(0) = +\infty$;
b) *Pour tout* $a \in A$, *on a* $v_p(a) = 0$ *si et seulement si* p *ne divise pas* a ;
c) *Pour tous* $a, b \in A$, *on a* $v_p(a+b) \geqslant \min(v_p(a), v_p(b))$;
d) *Pour tous* $a, b \in A$, *on a* $v_p(ab) = v_p(a) + v_p(b)$.

Démonstration. — a) Pour tout entier $n \geqslant 0$, p^n divise 0, donc $v_p(0) = +\infty$.

b) Par définition, $v_p(a) = 0$ si p^n ne divise a pour aucun entier $n \geqslant 1$; cela équivaut à ce que p ne divise pas a.

c) Soit $a, b \in A$; soit m un entier tels que $m \leqslant \min(v_p(a), v_p(b))$; alors, p^m divise a et p^m divise b, donc p^m divise $a + b$. Cela entraîne que $v_p(a+b) \geqslant m$, d'où l'assertion.

Proposition **(2.8.9)** (Propriété universelle du groupe défini par générateurs et relations)

Soit A *un groupe et soit* $f : S \to A$ *une application. Soit* $\varphi' : M'(S) \to A$ *l'unique homomorphisme de monoïdes tel que* $\varphi'(j'(s)) = f(s)$ *et* $\varphi'(j'(s^{-1})) = f(s)^{-1}$ *pour tout* $s \in S$. *On suppose que l'on a* $\varphi'(r) = e$ *pour tout* $r \in R$. *Alors, il existe un unique homomorphisme de groupes* $\varphi : G(S;R) \to A$ *tel que* $f = \varphi \circ j$.

Démonstration. — Soit $\psi : F(S) \to A$ l'unique homomorphisme de groupes tel que $\psi(j(s)) = s$ pour tout $s \in S$. On a $\psi \circ p = \varphi'$, donc $p(R) \subset \mathrm{Ker}(\psi)$. Comme $\mathrm{Ker}(\psi)$ est un sous-groupe distingué de F(S), on a $K \subset \mathrm{Ker}(\psi)$, et il existe un homomorphisme de groupes $\varphi : G(S;R) \to A$ tel que $\varphi \circ q = \psi$, où $q : F(S) \to G(S;R)$ est la surjection canonique. Pour tout $s \in S$, on a ainsi $\varphi(j(s)) = \varphi(p(j'(s)) = \varphi'(j'(s)) = f(s)$, ce qui démontre que $\varphi \circ j = f$.

L'unicité d'un tel morphisme résulte de ce que l'image de j engendre G(S;R). □

Exemple **(2.8.10)**. — a) Prenons d'abord pour ensemble $S = \{s\}$ un ensemble réduit à un seul élément.

Tout d'abord l'application de $\mathbf{Z}$ dans F(S) donnée par $n \mapsto s^n$ est surjective. Comme les mots réduits en s et s^{-1} sont exactement ceux de la forme $(s, \dots, s)$ ou $(s^{-1}, \dots, s^{-1})$, cette application est injective et F(S) est isomorphe à $\mathbf{Z}$.

Si n est un entier et $R = \{s^n\}$, alors, G(S;R) est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

b) Prenons pour ensemble S un ensemble $\{s_1, \dots, s_n\}$ à n éléments et pour ensemble R l'ensemble des commutateurs $s_i s_j s_i^{-1} s_j^{-1}$, pour $1 \leqslant i < j \leqslant n$. L'application f de F(S) dans $\mathbf{Z}^n$ qui applique s_i sur le i-ème vecteur de base e_i est surjective. Démontrons que son noyau est le sous-groupe distingué engendré par R. Tout d'abord, $f(s_i s_j s_i^{-1} s_j^{-1}) = e_i + e_j - e_i - e_j = 0$, donc $R \subset \mathrm{Ker}(f)$ et f définit, par passage au quotient, un homomorphisme de groupes $\bar{f}$ de G(S;R) sur $\mathbf{Z}^n$, surjectif.

Pour démontrer que $\bar{f}$ est injectif, on démontre que c'est un isomorphisme et, pour cela, on exhibe son inverse. Considérons l'application g de $\mathbf{Z}^n$ dans G(S;R) qui applique $(m_1, \dots, m_n)$ sur $x_1^{m_1} \dots x_n^{m_n}$. Démontrons que g est un homomorphisme de groupes.

Le groupe G(S;R) est engendré par les images $x_1, \dots, x_n$ des s_i. Pour tout i, la relation $s_i s_j s_i^{-1} s_j^{-1} \in R$ entraîne que x_i commute avec chaque x_j, donc x_j appartient au centralisateur de x_i. Puisque c'est un sous-groupe de G(S;R),

il en découle que le centralisateur de x_i est égal à $G(S;R)$, c'est-à-dire que x_i appartient au centre de $G(S;R)$. Comme le centre de $G(S;R)$ est un sous-groupe de $G(S;R)$, il est égal à $G(S;R)$ et ce groupe est commutatif.

On en déduit alors simplement que g est un homomorphisme de groupes : pour $(m_1,\dots,m_n)$ et $(m'_1,\dots,m'_n) \in \mathbf{Z}^n$, on a

$$\begin{aligned} g((m_1,\dots,m_n))g((m'_1,\dots,m'_n)) &= x_1^{m_1}\dots x_n^{m_n}x_1^{m'_1}\dots x_n^{m'_n} \\ &= x_1^{m_1+m'_1}\dots x_n^{m_n+m'_n} \\ &= g((m_1+m'_1,\dots,m_n+m'_n)). \end{aligned}$$

On a finalement

$$\bar{f}\circ g(m_1,\dots,m_n) = \bar{f}(x_1^{m_1}\dots x_n^{m_n}) = f(s_1^{m_1}\dots s_n^{m_n}) = \sum m_i e_i = (m_1,\dots,m_n),$$

donc $\bar{f}\circ g = \mathrm{id}$. De plus, $g(\bar{f}(x_i)) = g(e_i) = x_i$ pour tout i. Comme $\{x_1,\dots,x_n\}$ engendre $G(S;R)$, on a donc $g\circ\bar{f} = \mathrm{id}$. Cela conclut la preuve que $\bar{f}$ est un isomorphisme de $G(S;R)$ sur $\mathbf{Z}^n$.

Corollaire **(2.8.11)** (Coproduit d'une famille de groupes)

Soit $(A_i)_{i\in I}$ une famille de groupes. Il existe un groupe A et une famille $(j_i)_{i\in I}$, où, pour tout i, j_i est un morphisme de groupes de A_i dans A vérifiant la propriété suivante : pour tout groupe B et toute famille $(f_i)_{i\in I}$, où f_i est un morphisme de groupes de A_i dans B, il existe un unique homomorphisme de groupes $\varphi : A \to B$ tel que $\varphi\circ j_i = f_i$ pour tout $i \in I$.

Un tel groupe est appelé *coproduit* (ou *somme*) de la famille $(A_i)_{i\in I}$; on le note généralement $*_{i\in I} A_i$.

Démonstration. — Soit S l'ensemble somme de la famille $(A_i)_{i\in I}$ (« réunion disjointe ») ; c'est l'ensemble des couples (i,a), où $i \in I$ et $a \in A_i$. Soit A le groupe défini par l'ensemble générateur S et par l'ensemble de relations $(i,a)\cdot(i,b)\cdot(i,ab)^{-1}$ (pour $i \in I$, $a,b \in A_I$) et $(i,e)(j,e)^{-1}$ (pour $i,j \in I$, e désignant l'élément neutre des groupes A_i.). Pour tout $i \in I$ et tout $a \in A_i$, notons $j_i(a)$ la classe de (i,a) dans A. L'application $j_i : A_i \to A$ est un homomorphisme de groupes. Observons aussi que la réunion des parties $j_i(A_i)$ de A engendre le groupe A.

Vérifions alors la propriété universelle indiquée. Il existe un morphisme $\varphi' : M(S) \to B$ qui applique (i,a) sur $f_i(a)$ pour tout $i \in I$ et tout $a \in A$.

Démonstration. — Soit a un élément non nul de A. Supposons par l'absurde que a ne puisse pas s'écrire sous la forme $up_1\dots p_m$, où u est inversible et $p_1,\dots,p_m$ sont irréductibles. Alors a_1 n'est ni inversible (on pourrait sinon poser $m = 0$ et $u = a$) ni irréductible (on pourrait poser $m = 1$, $u = 1$ et $p_1 = a$). Il existe donc des éléments b et c de A qui ne sont pas inversibles tels que $a_1 = bc$. Posons $a_2 = b$; on a $(a_1) \subset (a_2)$ et $(a_1) \neq (a_2)$ car c n'est pas inversible. De plus, ni b, ni c ne peuvent s'écrire sous la forme $up_1\dots p_m$, où u est inversible et $p_1,\dots,p_m$ sont irréductibles. On reprend l'argument avec a_2 et on construit ainsi une suite strictement croissante $(a_n)_{n\geqslant 1}$ d'idéaux principaux de A, ce qui contredit la condition (i) d'un anneau factoriel. Nous avons donc prouvé que a possède une décomposition en produit d'éléments irréductibles.

Démontrons maintenant l'unicité. Soit u,v des éléments inversibles de A, soit $p_1,\dots,p_n,q_1,\dots,q_m$ des éléments irréductibles de A tels que $up_1\dots p_m = vq_1\dots q_n$. Démontrons par récurrence sur n que l'on a $m = n$, et qu'il existe une permutation $\sigma \in \mathfrak{S}_n$ et, pour $i \in \{1,\dots,n\}$, un élément inversible u_i, tels que $q_i = u_i p_{\sigma(i)}$. Si $n = 0$, alors $up_1\dots p_m$ est inversible ; comme un élément irréductible n'est pas inversible, cela impose $m = 0$. Sinon, le produit $up_1\dots p_m$ appartient à l'idéal (q_n) ; comme A est un anneau factoriel, cet idéal est premier, si bien que l'un des facteurs $u,p_1,\dots,p_m$ est multiple de q_n. Ce n'est pas le cas de u, puisqu'il est inversible. Soit alors $i \in \{1,\dots,m\}$ tel que p_i soit multiple de q_n et écrivons $p_i = q_n u_i$, pour un élément $u_n \in A$. Par définition d'un élément irréductible, u_n est inversible. On a alors $uu_nq_n(p_1\dots p_{i-1}p_{i+1}\dots p_m) = vq_1\dots q_n$, d'où $uu_n(p_1\dots p_{i-1}p_{i+1}\dots p_m) = vq_1\dots q_{n-1}$. Par récurrence, on a donc $m-1 = n-1$, donc $m = n$, et il existe une bijection $\sigma : \{1,\dots,n-1\} \to \{1,\dots,i-1,i+1,\dots,m\}$ et, pour tout $j \in \{1,\dots,n-1\}$, un élément inversible u_j tels que $q_j = u_j p_{\sigma(j)}$. L'application de $\{1,\dots,n\}$ dans $\{1,\dots,n\}$ qui applique n sur i et coïncide avec σ sinon est une bijection ; pour tout $j \in \{1,\dots,n\}$, on a $q_j = u_j p_{\sigma(j)}$, d'où le résultat.

Soit maintenant A un anneau commutatif intègre pour lequel les énoncés a) et b) sont vérifiés. Démontrons que A est un anneau factoriel.

Pour tout élément non nul a de A, notons $\omega(a)$ le nombre de facteurs irréductibles de a (l'entier m avec les notations ci-dessus). On a donc $\omega(ab) = \omega(a)+\omega(b)$, et $\omega(a) = 0$ si et seulement si a est inversible. Soit alors $((a_n))$ une suite croissante d'idéaux principaux de A. La suite $(\omega(a_n))$ est une suite décroissante d'entiers naturels ; elle est donc stationnaire. Soit m un entier tel

Démonstration. — Supposons que a soit irréductible et démontrons que l'idéal (a) est un idéal maximal de A. Comme a n'est pas inversible, on a $ab \neq 1$ pour tout $b \in A$, donc $1 \notin (a)$ et l'idéal (a) est distinct de A. Soit I un idéal de A tel que $(a) \subset I$. Comme A est un anneau principal, il existe $b \in A$ tel que $I = (b)$. Comme $a \in I$, il existe $c \in A$ tel que $a = bc$. Par définition d'un élément irréductible, ou bien b, ou bien c est inversible dans A. Si b est inversible dans A, on a $I = A$; si c est inversible dans A, on a $b = ac^{-1} \in (a)$, donc $(b) = (a)$. Cela démontre que (a) est un idéal maximal de A, d'où l'implication (i)⇒(ii).

L'implication (ii)⇒(iii) découle de ce que tout idéal maximal est premier.

Supposons maintenant que l'idéal (a) soit premier et démontrons que l'élément a est irréductible. Comme l'idéal (a) n'est pas égal à A, l'élément a n'est pas inversible. Soit alors b, c des éléments de A tels que $a = bc$; par définition d'un idéal premier, on a donc $b \in (a)$ ou $c \in (a)$. Supposons que $b \in (a)$ et soit $u \in A$ tel que $b = au$; il vient alors $a = auc$, donc $uc = 1$ car a est simplifiable dans A ; par suite, c est inversible. Dans le cas où $c \in (a)$, on démontre de même que b est inversible. Ainsi, a est irréductible. □

Définition **(3.11.9)**. — *On dit qu'un anneau commutatif intègre* A *est* factoriel *si les deux propriétés suivantes sont satisfaites :*

(i) *Toute suite croissante d'idéaux principaux de* A *est stationnaire ;*
(ii) *Tout élément irréductible de* A *engendre un idéal premier.*

Exemple **(3.11.10)**. — Un anneau principal est factoriel. La propriété (i) découle de ce qu'un anneau principal est noethérien, la propriété (ii) est le lemme d'Euclide (proposition 3.11.8).

Théorème **(3.11.11)**. — *Soit* A *un anneau factoriel.*

a) *Pour tout élément non nul a de* A*, il existe un entier $m \geqslant 0$, un élément inversible u et des éléments irréductibles $p_1, \dots, p_m$ de* A *tels que $a = up_1 \dots p_m$ (*existence d'une décomposition en produit d'éléments irréductibles*).*

b) *Soit m, n des entiers $\geqslant 0$, soit u, v des éléments inversibles de* A*, soit $p_1, \dots, p_n, q_1, \dots, q_m$ des éléments irréductibles de* A *tels que $up_1 \dots p_m = vq_1 \dots q_n$. Alors $m = n$, et il existe une permutation $\sigma \in \mathfrak{S}_n$ et, pour $i \in \{1, \dots, n\}$, un élément inversible u_i, tels que $q_i = u_i p_{\sigma(i)}$ (*unicité de la décomposition en produit d'éléments irréductibles*).*

Inversement, un anneau commutatif intègre qui vérifie ces deux propriétés est un anneau factoriel.

En outre, φ' applique toute relation sur l'élément neutre puisque

$$\varphi'\big((i,a)(i,b)(i,ab)^{-1}\big) = f_i(a)f_i(b)f_i(ab)^{-1} = e$$

et $\varphi'\big((i,e)(j,e)^{-1}\big) = f_i(e)f_j(e)^{-1} = e$. Par suite, φ' passage au quotient et définit un homomorphisme de groupes φ de A dans B. Pour tout $i \in I$ et tout $a \in A_i$, on a $\varphi(j_i(a)) = \varphi'((i,a)) = f_i(a)$, donc $\varphi \circ j_i = f_i$. Enfin, comme la réunion des parties $j_i(A_i)$ engendre A, φ est le seul morphisme tel que $\varphi \circ j_i = f_i$ pour tout i. □

2.9. Groupes abéliens

2.9.1. — On dit qu'un groupe A est *de type fini* s'il possède un système générateur fini, *monogène* s'il existe un élément $a \in A$ tel que $A = \langle a \rangle$, et *cyclique* s'il est monogène et fini.

Soit $f : A \to B$ un morphisme de groupes, surjectif. Si A est de type fini (*resp.* monogène, *resp.* cyclique), il en est de même de B.

Remarque **(2.9.2)**. — Soit A un groupe fini et soit a un élément de A ; notons n le cardinal de A et m l'ordre de a.

Le sous-groupe $\langle a \rangle$ engendré par a est constitué des éléments $e, a, \dots, a^{m-1}$ et est ainsi de cardinal m. Par suite, si $\langle a \rangle = A$, alors $m = n$. Inversement, si $m = n$, on a $\mathrm{Card}(\langle a \rangle) = \mathrm{Card}(A)$, donc $\langle a \rangle = A$ et A est cyclique. Cela démontre qu'*un groupe fini est cyclique si et seulement s'il possède un élément dont l'ordre est égal au cardinal de* A.

Proposition **(2.9.3)**. — *Soit* A *un groupe monogène.*

a) *Pour tout entier m, l'application $(m)_A : x \mapsto mx$ est un endomorphisme de* A.

b) *Si* A *est infini, l'application $m \mapsto (m)_A$ est un isomorphisme du monoïde multiplicatif* $\mathbf{Z}$ *sur* $\mathrm{End}(A)$.

c) *Si* A *est fini, de cardinal n, l'application $m \mapsto (m)_A$ induit un isomorphisme du monoïde multiplicatif $\mathbf{Z}/n\mathbf{Z}$ sur* $\mathrm{End}(A)$.

Quand A est infini, $\mathrm{Aut}(A)$ est donc isomorphe à $\{\pm 1\}$, tandis que si A est fini de cardinal n, $\mathrm{Aut}(A)$ est le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$. Pour que l'endomorphisme $(m)_A$ soit un automorphisme, il faut et il suffit que m soit premier à n.

Démonstration. — Soit a un générateur de A ; si le groupe A est fini, l'ordre de a est donc le cardinal de A.

Comme A est abélien, l'application $(m)_A$ est un endomorphisme de A. D'autre part, on a $(m)_A \circ (n)_A(x) = m(nx) = mnx = (mn)_A(x)$, et $(1)_A = \mathrm{id}_A$, donc $m \mapsto (m)_A$ est un morphisme de monoïdes de $(\mathbf{Z}, \times)$ dans $\mathrm{End}(A)$.

Inversement, soit $\varphi \in \mathrm{End}(A)$. Il existe donc un entier m tel que $\varphi(a) = ma$. Par suite, pour tout entier $k \in \mathbf{Z}$, on a $\varphi(ka) = k\varphi(a) = kma = (m)_A(ka)$, ce qui prouve que $\varphi = (m)_A$. Le morphisme $m \mapsto (m)_A$ est donc surjectif.

Soit $m \in \mathbf{Z}$. Pour que $(m)_A = 0$, il faut et il suffit que $ma = 0$, c'est-à-dire que m soit multiple de l'ordre de a si A est fini, et que $m = 0$ si A est infini. Il en résulte un isomorphisme de monoïdes de $\mathbf{Z}$ sur $\mathrm{End}(A)$ si A est infini, et de $\mathbf{Z}/n\mathbf{Z}$ sur $\mathrm{End}(A)$ si A est fini de cardinal n. □

Exemple **(2.9.4)**. — a) Le groupe $\mathbf{Z}$ est monogène, engendré par 1. Pour qu'un élément $a \in \mathbf{Z}$ engendre $\mathbf{Z}$, il faut et il suffit que l'on ait $a \in \{\pm 1\}$. En effet, ± 1 engendrent $\mathbf{Z}$, et inversement, 1 n'est multiple de a que si $a \in \{\pm 1\}$.

b) Pour tout entier naturel $n \geqslant 1$, le groupe $\mathbf{Z}/n\mathbf{Z}$ est cyclique, de cardinal n. Pour que la classe modulo n d'un entier $a \in \mathbf{Z}$ engendre le groupe $\mathbf{Z}/n\mathbf{Z}$, il faut et il suffit que $\mathrm{pgcd}(a, n) = 1$.

Soit en effet $a \in \mathbf{Z}$ et soit $d = \mathrm{pgcd}(a, n)$. Supposons que la classe de 1 appartienne à $\langle a \rangle$; il existe alors un entier u tel que $1 \equiv au \pmod{n}$, donc un entier v tel que $1 = au + nv$, ce qui montre que $\mathrm{pgcd}(a, n) = 1$. Inversement, si a et n sont premiers entre eux, le théorème de Bézout fournit des entiers u et v tels que $1 = au + vn$; cela prouve que $u[a] = [1]$, donc que la classe de 1 appartient au sous-groupe engendré par la classe de u. Par suite, $\langle [a] \rangle = \mathbf{Z}/n\mathbf{Z}$.

c) Soit A un groupe monogène et soit a un élément de A tel que $A = \langle a \rangle$. Soit $f : \mathbf{Z} \to A$ l'homomorphisme de groupes donné par $f(n) = a^n$; il est surjectif.

Soit N son noyau. Si $N = \{0\}$, f induit un isomorphisme de groupes de $\mathbf{Z}$ sur A. Sinon, il existe un entier strictement positif n tel que $N = n\mathbf{Z}$ et f induit un isomorphisme de groupes de $\mathbf{Z}/n\mathbf{Z}$ sur A. En outre, on a $n = \mathrm{Card}(\mathbf{Z}/n\mathbf{Z}) = \mathrm{Card}(A)$.

Lemme **(2.9.5)**. — *Soit m et n des entiers naturels premiers entre eux ; soit* A *et* B *des groupe cycliques d'ordres m et n respectivement, notés multiplicativement. Alors* $A \times B$ *est un groupe cyclique.*

Cela prouve la propriété voulue par récurrence sur n. En particulier, $a_n \in (a, b)$, donc $(a_n) \subset (a, b)$.

On démontre ensuite que pour tout entier $m \leqslant n$, l'idéal (a_m, a_{m+1}) est égal à (a, b). C'est vrai pour $m = 0$ puisque $a = a_m$ et $b = a_1$. Soit m un entier tel que $1 \leqslant m < n$ et telle que la propriété soit vraie pour tout entier $< m$. On a $(a_{m+1}, a_m) = (a_m, a_{m-1} - qa_m)$. Observons que cet idéal $(a_m, a_{m-1} - qa_m)$ contient a_m, il contient aussi a_{m-1} puisque $a_{m-1} = (a_{m-1} - qa_m) + qa_m$; donc il contient $(a_m, a_{m-1} - qa_m)$. Inversement, l'idéal (a_m, a_{m-1}) contient a_m et $a_{m-1} - qa_m)$. Par suite, $(a_m, a_{m+1}) = (a_m, a_{m-1}) = (a, b)$. En particulier, $(a_n) = (a_n, a_{n+1}) = (a, b)$.

Définition **(3.11.6)**. — *Soit* A *un anneau commutatif intègre. On dit qu'un élément $a \in A - \{0\}$ est irréductible s'il n'est pas inversible et si, pour tous $b, c \in A$ tels que $a = bc$, ou bien b ou bien c est inversible.*

Exemple **(3.11.7)**. — a) Les éléments irréductibles de $\mathbf{Z}$ sont les nombres premiers et leurs opposés.

b) Soit K un corps et soit $A = K[T]$. Tout polynôme f de degré 1 est irréductible. En effet, f n'est pas inversible ; soit ensuite $g, h \in K[T]$ tels que $f = gh$, on a $1 = \deg(f) = \deg(g) + \deg(h)$, donc $\deg(g) = 0$ ou $\deg(h) = 0$, c'est-à-dire que g ou h est inversible.

Supposons de plus que K soit algébriquement clos, c'est-à-dire que tout polynôme non constant possède une racine dans K ; c'est par exemple le cas si $K = \mathbf{C}$ (théorème de D'Alembert-Gauß). Alors tout polynôme irréductible $f \in K[T]$ est de degré 1. En effet, puisque f n'est pas inversible, on a $\deg(f) \geqslant 1$, donc f n'est pas constant. Soit alors $a \in K$ une racine de f ; le reste de la division euclidienne de f par $T - a$ est égal à $f(a) = 0$, donc il existe $g \in K[T]$ tel que $f = (T - a)g$. Puisque f est irréductible et que $T - a$ n'est pas inversible, g est inversible, c'est-à-dire constant non nul, donc f est de degré 1.

Proposition **(3.11.8)** (« Lemme d'Euclide »). — *Soit* A *un anneau principal et soit a un élément non nul de* A. *Les conditions suivantes sont équivalentes :*

(i) *L'élément a est irréductible dans* A ;
(ii) *L'idéal (a) est un idéal maximal de* A.
(iii) *L'idéal (a) est un idéal premier de* A ;

Définition **(3.11.3)**. — *Soit* A *un anneau commutatif intègre. On dit que* A *est un anneau principal si tout idéal de* A *est principal, c'est-à-dire engendré par un seul élément.*

Un anneau principal est donc un anneau noethérien (définition 3.6.8).

Proposition **(3.11.4)**. — *Un anneau euclidien est un anneau principal.*

Démonstration. — Soit A un anneau euclidien et soit j un stathme euclidien sur A. Soit I un idéal de A. Si $I = \{0\}$, l'idéal $I = (0)$ est principal. Sinon, soit a un élément de $I - \{0\}$ pour lequel $j(a)$ est minimal. Démontrons que $I = (a)$. Comme I est un idéal, on a $ax \in A$ pour tout $x \in A$. Inversement, soit $b \in I$ et soit $b = aq + r$ une division euclidienne de b par a. Si $r \neq 0$, on a $j(r) < j(a)$ par hypothèse, et $r = b - aq \in (a)$, ce qui contredit le choix de a. On a donc $r = 0$, d'où $b = aq \in (a)$. □

Remarque **(3.11.5)** (Algorithme d'Euclide). — Soit A un anneau euclidien et soit j un stathme euclidien sur A. Soit a, b des éléments de A ; l'algorithme d'Euclide (étendu) permet de calculer un générateur d de l'idéal (a, b) ainsi que des éléments $u, v \in A$ tels que $d = au + bv$.

On définit trois suites (a_n), (u_n), (v_n) comme suit. Posons d'abord

$$a_0 = a \qquad u_0 = 1 \qquad v_0 = 0$$
$$a_1 = b \qquad u_1 = 0 \qquad v_1 = 1.$$

Puis, si ces suites sont définies jusqu'au rang $n \geqslant 1$ et si $a_n \neq 0$, on considère une division euclidienne $a_{n-1} = a_n q + r$ de a_{n-1} par a_n et on pose

$$a_{n+1} = a_{n-1} - qa_n = r \qquad u_{n+1} = u_{n-1} - qu_n v_{n+1} = v_{n-1} - qv_n$$

Il existe un plus petit entier n tel que $a_{n+1} = 0$; l'élément a_n est un générateur de l'idéal (a, b) et l'on a $a_n = au_n + bv_n$. En outre,

En effet, si la suite (a_n) est définie jusqu'au rang r, on a $j(a_n) < j(a_{n-1})$ pour $1 \leqslant n \leqslant r$, donc $r \leqslant j(a_0)$. Il existe donc un entier n tel que la suite soit définie jusqu'au rang $n + 1$ et $a_{n+1} = 0$; on a donc $a_m \neq 0$ pour $m \leqslant n$.

Démontrons par récurrence sur m que $a_m = au_m + bv_m$ pour tout entier m tel que $0 \leqslant m \leqslant n + 1$; c'est vrai pour $m = 0$ et $m = 1$. Si c'est vrai pour tout entier $\leqslant m$ et $m < n$, alors

$$a_{m+1} = a_{m-1} - qa_m = (au_{m-1} + bv_{m-1}) - q(au_m + bv_m) = a(u_{m-1} - qu_m) + b(v_{m-1} - qv_m) = au_{m+1}$$

Démonstration. — Le cardinal du groupe $A \times B$ est égal à mn ; démontrons que ce groupe possède un élément d'ordre mn. Soit a un générateur de A et soit b un générateur de B ; posons $c = (a, b)$. Soit $p \in \mathbf{Z}$; on a $c^p = (a, b)^p = (a^p, b^p) = e$. Ainsi, $c^p = e$ si et seulement si $a^p = e$ et $b^p = e$, c'est-à-dire si et seulement si p est multiple à la fois de m et de n. Comme m et n sont premiers entre eux, cela équivaut à ce que p soit multiple de mn, si bien que l'ordre de c est égal à mn.

Les mn éléments $e, c, c^2, \ldots, c^{mn-1}$ sont deux à deux distincts et épuisent donc le groupe $A \times B$, qui est ainsi cyclique. □

Théorème **(2.9.6)**. — *Soit* K *un corps commutatif et soit* A *un sous-groupe* fini *du groupe multiplicatif de* K. *Alors* A *est cyclique.*

Démonstration. — Soit n le cardinal de A et écrivons $n = \prod p_i^{m_i}$ sa décomposition en facteurs premiers. Fixons un indice i ; dans un corps, un polynôme de degré d a au plus d racines, donc A contient au plus n/p_i éléments a tels que $a^{n/p_i} = 1$; il existe donc un élément $x_i \in A$ tel que $a^{n/p_i} \neq 1$. Posons $a_i = x_i^{n/p_i^{m_i}}$. D'après le théorème de Lagrange, on a $a_i^{p_i^{m_i}} = x_i^n = 1$, donc l'ordre de a_i divise $p_i^{m_i}$. Comme $a_i^{p_i^{m_i-1}} = x_i^{n/p_i} \neq 1$, l'ordre de a_i est égal à $p_i^{m_i}$.

Comme les ordres de a_i sont premiers entre eux deux à deux, leur produit $a = \prod a_i$ est d'ordre $\prod p_i^{m_i} = n$. Cela prouve que A est cyclique. □

Remarque **(2.9.7)**. — Lorsque K est un corps commutatif fini, cette preuve se prête bien à un calcul effectif d'un générateur du groupe multiplicatif $K^\times$. Pour déterminer l'élément x_i, il suffit d'essayer les éléments un par un.

2.9.8. — Soit A un groupe abélien dont la loi de groupe est notée additivement. On dit qu'une partie $(x_1, \ldots, x_n)$ de A est une quasi-base si elle engendre A est si pour tout n-uplet $(m_1, \ldots, m_n)$ d'entiers tels que $\sum_{i=1}^n m_i x_i = 0$, on a $m_i x_i = 0$ pour tout i.

En particulier, l'application canonique du produit des groupes monogènes $\prod_{i=1}^n \langle x_i \rangle$ dans A est un isomorphisme. Si l'on note d_i l'ordre de x_i, si celui-ci est fini, et $d_i = 0$ sinon, on voit aussi que A est isomorphe au groupe $\prod_{i=1}^n (\mathbf{Z}/d_i\mathbf{Z})$.

Lemme **(2.9.9)**. — *Soit* A *un groupe abélien et soit* $(x_1, \ldots, x_n)$ *une famille génératrice de* A. *Soit* $(m_1, \ldots, m_n)$ *une suite d'éléments de* **Z**, *premiers entre eux dans leur ensemble. Il existe alors une famille génératrice* $(y_1, \ldots, y_n)$ *de* A *telle que* $y_1 = \sum_{i=1}^n m_i x_i$.

Démonstration. — On raisonne par récurrence sur l'entier $m = \sum_{i=1}^{n} |m_i|$.

Comme les m_i sont premiers entre eux dans leur ensemble, ils ne sont pas tous nuls et $m \geqslant 1$. Si $m = 1$, il existe un entier i tel que $m_i = \pm 1$ et $m_j = 0$ si $j \neq i$. Alors la suite $(y_1, \ldots, y_n)$ obtenue en posant $y_1 = m_i x_i$ $y_i = x_1$ (si $i \neq 1$) et $y_j = x_j$ si $j \notin \{1, i\}$ convient.

Supposons maintenant $m > 1$, de sorte qu'au moins deux termes de la suite $(m_1, \ldots, m_n)$ ne sont pas nuls; quitte à réordonner la suite $(x_1, \ldots, x_n)$, on suppose que $|m_1| \geqslant |m_2| > 0$; soit ε le signe de $m_1 m_2$. On observe que la suite $(x_1, x_2 + \varepsilon x_1, x_3, \ldots, x_n)$ engendre A et que $y_1 = \sum_{i=1}^{n} m_i x_i = (m_1 - \varepsilon m_2) x_1 + m_2(x_2 + \varepsilon x_1) + m_3 x_3 + \cdots + m_n x_n$. Comme $|m_1 - \varepsilon m_2| < |m_1|$, l'hypothèse de récurrence permet de conclure. □

Proposition **(2.9.10)**. — *Tout groupe abélien de type fini possède une quasi-base.*

Démonstration. — Soit A un groupe abélien de type fini. Parmi toutes les suites finies $(x_1, \ldots, x_n)$ qui engendrent A, choisissons-en une pour laquelle l'entier n est minimal, puis parmi celles-ci, telles que l'ordre de x_1 (fini ou infini) soit minimal. Soit A_1 le sous-groupe de A engendré par x_1 et B_1 le sous-groupe de A engendré par $x_2, \ldots, x_n$.

L'application $f : A_1 \times B_1 \to A$ donnée par $f(a, b) = a + b$, est un morphisme de groupes surjectif. Démontrons qu'il est injectif. Soit (a, b) un élément de son noyau; soit $(m_1, \ldots, m_n)$ une famille d'entiers telle que $a = m_1 x_1$ et $b = m_2 x_2 + \cdots + m_n x_n$. Si x_1 est d'ordre fini, on peut remplacer m_1 par le reste de sa division euclidienne par l'ordre de x_1, ce qui permet de supposer que m_1 est strictment inférieur à l'ordre de x_1 et est positif ou nul.

Supposons par l'absurde que $m_1 \neq 0$. Soit alors $d = \operatorname{pgcd}(m_1, \ldots, m_n)$ et, pour tout i, posons $p_i = m_i/d$; par construction, les entiers $p_1, \ldots, p_n$ sont premiers entre eux dans leur ensemble. D'après le lemme précédent, il existe donc une famille $(y_1, \ldots, y_n)$ qui engendre A et telle que $y_1 = \sum_{i=1}^{n} p_i x_i$; on a $d y_1 = 0$. La famille $(y_1, \ldots, y_n)$ est de cardinal n et l'ordre de l'élément y_1 divise d, donc est strictement inférieur à l'ordre de x_1 (qu'il soit fini ou infini). Cette contradiction prouve que $m_1 = 0$, donc $a = 0$ puis $b = 0$. Ainsi, f est injectif. □

Théorème **(2.9.11)**. — *Soit* A *un groupe abélien de type fini. Il existe une unique suite* $(r, d_1, \ldots, d_s)$*, où* r *est un entier naturel et* $(d_1, \ldots, d_s)$ *une suite d'entiers* $\geqslant 2$ *tels que* $d_s | d_{s-1} | \ldots | d_2 | d_1$*, de sorte que* A *soit isomorphe à* $\mathbf{Z}^r \times \prod_{i=1}^{s} (\mathbf{Z}/d_i\mathbf{Z})$.

Traitons maintenant le cas général. L'inclusion $\sqrt{I} \subset \mathscr{I}(\mathscr{V}(\sqrt{I}))$ et l'égalité $\mathscr{V}(E) = \mathscr{V}(\sqrt{I})$, déjà démontrées, entraînent l'inclusion $\sqrt{I} \subset \mathscr{I}(\mathscr{V}(E))$. Inversement, soit $f \in \mathscr{I}(\mathscr{V}(E))$ et démontrons que $f \in \sqrt{I}$.

Soit E′ la partie de $\mathbf{C}[T_1, \ldots, T_n, T_{n+1}]$ donnée par $E' = E \cup \{1 - f T_{n+1}\}$. La partie $\mathscr{V}(E')$ de $\mathbf{C}^{n+1}$ est vide; en effet, si $(a_1, \ldots, a_n, a_{n+1}) \in \mathscr{V}(E')$, alors $(a_1, \ldots, a_n) \in \mathscr{V}(E)$, donc $f(a_1, \ldots, a_n) = 0$, ce qui contredit la relation $1 = f(a_1, \ldots, a_n) a_{n+1}$. Par suite, l'idéal I′ de $\mathbf{C}[T_1, \ldots, T_{n+1}]$ engendré par E′ contient 1 et il existe des polynômes $f_1, \ldots, f_m \in E$, et $g_1, \ldots, g_m, h \in \mathbf{C}[T_1, \ldots, T_{n+1}]$ tels que

$$1 = \sum_{i=1}^{m} f_i g_i + (1 - f T_{n+1}) h.$$

Soit e un entier supérieur au degré en T_{n+1} des polynômes g_i. En écrivant $T_{n+1} f = 1 - (1 - f T_{n+1})$, on déduit de l'égalité précédente qu'il existe des polynômes $g_1', \ldots, g_m' \in \mathbf{C}[T_1, \ldots, T_n]$ et un polynôme $h' \in \mathbf{C}[T_1, \ldots, T_{n+1}]$ tels que

$$f^e = \sum_{i=1}^{m} f_i g_i' + (1 - f T_{n+1}) h'.$$

Par suite, le polynôme $f^e - \sum_{i=1}^{m} f_i g_i'$ est multiple de $1 - f T_{n+1}$; comme il est de degré 0 en T_{n+1}, il est nul. Cela démontre que $f^e \in I$, et donc $f \in \sqrt{I}$. □

3.11. Anneaux euclidiens, principaux, factoriels

Définition **(3.11.1)**. — *Soit* A *un anneau commutatif intègre. On appelle* stathme euclidien *sur* A *une fonction* $j : A - \{0\} \to \mathbf{N}$ *vérifiant les propriétés suivantes :*

(i) *Pour tous* $a, b \in A - \{0\}$*, on a* $j(ab) \geqslant j(a)$*;*

(ii) *Pour tous* $a, b \in A$ *tels que* $b \neq 0$*, il existe des éléments* $q, r \in A$ *tels que* $a = bq + r$ *et tels que* $r = 0$ *ou* $j(r) < j(b)$.

On dit que A *est un anneau* euclidien *s'il existe un stathme euclidien sur* A.

Dans les conditions de (ii), on dit que q est le quotient d'une division euclidienne de a par b et que r est son reste.

Exemple **(3.11.2)**. — a) La fonction $n \mapsto |n|$ est un stathme euclidien sur l'anneau $\mathbf{Z}$.

b) Soit K un corps. La fonction $f \mapsto \deg(f)$ est un stathme euclidien sur l'anneau $K[T]$ des polynômes en une indéterminée et à coefficients dans K.

Démonstration. — Les assertions *a*), *b*) et *c*) découlent directement de la définition.

Démontrons *d*). Soit $a \in \mathscr{V}(\mathrm{E})$; pour tout $f \in \mathrm{E}$ et tout $g \in \mathrm{E}'$, on a $fg(a) = f(a)g(a) = 0$, donc $a \in \mathscr{V}(\mathrm{EE}')$. De même, si $a \in \mathscr{V}(\mathrm{E}')$, alors $a \in \mathscr{V}(\mathrm{EE}')$. Inversement, supposons que $a \notin \mathscr{V}(\mathrm{E}) \cup \mathscr{V}(\mathrm{E}')$; il existe donc $f \in \mathrm{E}$ et $g \in \mathrm{E}'$ tels que $f(a) \neq 0$ et $g(a) \neq 0$; alors, $fg \in \mathrm{EE}'$ et $fg(a) \neq 0$, ce qui prouve que $a \notin \mathscr{V}(\mathrm{EE}')$.

Démontrons *e*). Les inclusions $\mathrm{E} \subset \mathrm{I} \subset \sqrt{\mathrm{I}}$ entraînent que $\mathscr{V}(\sqrt{\mathrm{I}}) \subset \mathscr{V}(\mathrm{I}) \subset \mathscr{V}(\mathrm{E})$. Inversement, soit $a \in \mathscr{V}(\mathrm{E})$ et démontrons que $a \in \mathscr{V}(\sqrt{\mathrm{I}})$. Soit $f \in \sqrt{\mathrm{I}}$; soit $m \geqslant 1$ tel que $f^m \in \mathrm{I}$; il existe des familles finies (f_i) et (g_i) de polynômes tels que $f_i \in \mathrm{E}$ pour tout i et $f^m = \sum f_i g_i$. Par hypothèse, $f_i(a) = 0$ pour tout i. On a donc $f^m(a) = 0$, d'où $f(a) = 0$. Cela démontre que $a \in \mathscr{V}(\sqrt{\mathrm{I}})$. □

3.10.4. — Si A est une partie de $\mathbf{C}^n$, on note $\mathscr{I}(\mathrm{A})$ l'ensemble des polynômes $f \in \mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ tels que $f(a) = 0$ pour tout $a \in \mathrm{A}$.

Il contient 0; si $f, g \in \mathscr{I}(\mathrm{A})$, alors $(f+g)(a) = f(a) + g(a) = 0$, donc $f+g \in \mathscr{I}(\mathrm{A})$; enfin, si $f \in \mathscr{I}(\mathrm{A})$ et $g \in \mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$, alors $fg(a) = f(a)g(a) = 0$, donc $fg \in \mathscr{I}(\mathrm{A})$. Cela démontre que $\mathscr{I}(\mathrm{A})$ est un idéal de $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$.

Les définitions entraînent les faits suivants :

a) On a $\mathscr{I}(\varnothing) = \mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ et $\mathscr{I}(\mathbf{C}^n) = \{0\}$.
b) Si A et A′ sont des parties de $\mathbf{C}^n$ telles que $\mathrm{A} \subset \mathrm{A}'$, on a $\mathscr{I}(\mathrm{A}') \subset \mathscr{I}(\mathrm{A})$.
c) Si $(\mathrm{A}_i)_{i \in \mathrm{I}}$ est une famille de parties de $\mathbf{C}^n$, on a $\mathscr{I}(\bigcup_{i \in \mathrm{I}} \mathrm{A}_i) = \bigcap_{i \in \mathrm{I}} \mathscr{I}(\mathrm{A}_i)$.

3.10.5. — Soit E une partie de $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$. On a l'inclusion $\mathrm{E} \subset \mathscr{I}(\mathscr{V}(\mathrm{E}))$.

Soit A une partie de $\mathbf{C}^n$. On a l'inclusion $\mathrm{A} \subset \mathscr{V}(\mathscr{I}(\mathrm{A}))$. Si l'on a égalité $\mathrm{A} = \mathscr{V}(\mathscr{I}(\mathrm{A}))$, alors A est un ensemble algébrique. Inversement, supposons que A soit un ensemble algébrique et soit E une partie de $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ telle que $\mathrm{A} = \mathscr{V}(\mathrm{E})$. On a donc $\mathrm{E} \subset \mathscr{I}(\mathrm{A})$, d'où $\mathscr{V}(\mathscr{I}(\mathrm{A})) \subset \mathscr{V}(\mathrm{E}) = \mathrm{A}$. Cela entraîne que $\mathrm{A} = \mathscr{V}(\mathscr{I}(\mathrm{A}))$.

Théorème **(3.10.6)**. — *Soit* E *une partie de* $\mathbf{C}^n$ *et soit* I *l'idéal qu'elle engendre; on a* $\mathscr{I}(\mathscr{V}(\mathrm{E})) = \sqrt{\mathrm{I}}$. *En particulier, si* $\mathscr{V}(\mathrm{E}) = \varnothing$, *alors* $\mathrm{I} = (1)$.

Démonstration. — Démontrons d'abord le cas particulier. Supposons que $\mathrm{I} \neq (1)$ et soit M un idéal maximal de $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ tel que $\mathrm{I} \subset \mathrm{M}$. D'après le théorème 3.10.1, il existe $a \in \mathbf{C}^n$ tel que $\mathrm{M} = \mathrm{M}_a = (\mathrm{T}_1 - a_1, \ldots, \mathrm{T}_n - a_n)$. On a donc $a \in \mathrm{V}(\mathrm{M}_a) \subset \mathrm{V}(\mathrm{I}) = \mathrm{V}(\mathrm{E})$ et, en particulier, $\mathrm{V}(\mathrm{E}) \neq \varnothing$.

On dit que *r* est le *rang* de A et que les entiers $d_1, \ldots, d_s$ sont ses *facteurs invariants.*

Démonstration. — Soit $(x_1, \ldots, x_n)$ une quasi-base de A; quitte à réordonner cette suite, on suppose que $x_1, \ldots, x_r$ sont d'ordre infini et que $x_{r+1}, \ldots, x_n$ sont d'ordre fini; notons alors m_i l'ordre de x_i si $i >$. D'après la définition d'une quasi-base, le groupe A est isomorphe à $\mathbf{Z}^r \times \prod_{i=r+1}^n (\mathbf{Z}/m_i\mathbf{Z})$.

La fin de la preuve du théorème consiste à récrire le groupe $\mathrm{T} = \prod_{i=r+1}^n (\mathbf{Z}/m_i\mathbf{Z})$ sous la forme requise. Soit $m_i = \prod p^{k_{i,p}}$ la décomposition de m_i en facteurs premiers. (Dans ces produits, seuls les nombres premiers qui divisent l'un des m_i apparaissent avec un exposant non nul.) Pour tout i, on a un isomorphisme $\mathbf{Z}/m_i\mathbf{Z} \simeq \prod_p (\mathbf{Z}/p^{k_{i,p}}\mathbf{Z})$, de sorte que T est isomorphe au groupe produit $\prod_p \prod_i (\mathbf{Z}/p^{k_{i,p}}\mathbf{Z})$. On va maintenant regrouper les facteurs premiers différemment. Pour tout nombre premier p, soit $(\ell_{p,1}, \ldots)$ la suite décroissante des entiers $k_{i,p}$, chacun récrit autant de fois qu'il apparaît. Chacune de ces suites est nulle à partir d'un certain rang (au plus égal à $n - r$), et pour tout nombre premier p qui ne divise pas le ppcm des m_i, la suite $(\ell_{p,1}, \ldots)$ est identiquement nulle. Soit s la borne supérieure de l'ensemble des $j \in \mathbf{N}$ tels qu'il existe un nombre premier p avec $\ell_{p,j} \neq 0$ (on a $s = 0$ si $\ell_{p,j} = 0$ pour tout nombre premier p et tout entier j). Pour tout $j \in \{1, \ldots, s\}$, posons alors $d_j = \prod_p p^{\ell_{p,j}}$, de sorte que $\mathbf{Z}/d_j\mathbf{Z}$ est isomorphe à $\prod_p (\mathbf{Z}/p^{\ell_{p,j}}\mathbf{Z})$ et T est isomorphe au groupe $\prod_{j=1}^s (\mathbf{Z}/d_j\mathbf{Z})$. Comme les suites $(\ell_{p,j})_j$ sont décroissantes, d_1 est multiple de d_2, qui est multiple de d_3, etc., ce qui démontre l'existence d'un isomorphisme vérifiant les propriétés annoncées.

Supposons maintenant que A soit isomorphe à $\mathbf{Z}^r \times \prod_{j=1}^s (\mathbf{Z}/d_j\mathbf{Z})$, où $d_s | d_{s-1} | \ldots | d_1$, et démontrons comment calculer les d_j directement en terme du groupe A; cela entraînera l'assertion d'unicité. On va utiliser le lemme suivant.

Lemme **(2.9.12)**. — *Soit* A *un groupe monogène, soit p un nombre premier et soit n un entier naturel non nul. Le groupe* $p^{n-1}\mathrm{A}/p^n\mathrm{A}$ *est ou bien nul, ou bien cyclique de cardinal p. Pour qu'il soit nul, il faut et il suffit que le cardinal de* A *soit fini mais non multiple de* p^n.

Démonstration. — Posons $\mathrm{A}_n = p^{n-1}\mathrm{A}/p^n\mathrm{A}$. Soit a un générateur de A. Alors, $p^{n-1}a$ engendre $p^{n-1}\mathrm{A}$ ce qui prouve que ce groupe est monogène; De même, la classe $[p^{n-1}a]$ de $p^{n-1}a$ engendre le groupe quotient A_n qui est donc également

monogène. Comme $p[p^{n-1}a] = [p^n a] \in p^n\mathrm{A}$, l'élément $[p^{n-1}a]$ est d'ordre fini et son ordre divise p. En particulier, le groupe A_n est cyclique de cardinal 1 ou p.

Supposons que A_n soit de cardinal 1. Alors, $p^{n-1}a$ appartient à $p^n\mathrm{A}$, c'est-à-dire qu'il existe $m \in \mathbf{Z}$ tel que que $p^{n-1}a = p^n ma$; cela entraîne que $(1-pm)p^{n-1}a = 0$. Comme $(1-pm)p^{n-1}$ n'est pas nul, l'élément a est d'ordre fini et cet ordre divise $(1-pm)p^{n-1}$. En particulier, si A est infini, alors A_n est de cardinal p.

Supposons maintenant que A soit fini et soit d son cardinal, qui est l'ordre de a. Si d est multiple de p^n, il ne peut diviser $(1-pm)p^{n-1}$, car $1-pm$ n'est pas multiple de p, donc $\mathrm{Card}(\mathrm{A}_n) = p$ dans ce cas. Soit alors e l'exposant de p dans la décomposition en facteur premiers de d ; supposons $e < n$ et posons $v = d/p^e$, de sorte que p ne divise pas v. Ainsi, p et v sont premiers entre eux, et il existe des entiers m et q tels que $1 = pm + vq$. Par suite, $(1-pm)p^e a = vqp^e a = dqa = 0$. Comme $n-1 \geqslant e$, on a aussi $(1-pm)p^{n-1}a$ ce qui prouve que $p^{n-1}a \in p^n\mathrm{A}$; dans ce cas, $\mathrm{A}_n = \{0\}$. □

Soit p un nombre premier et soit n un entier naturel tel que $n \geqslant 1$. Le groupe $p^{n-1}\mathrm{A}/p^n\mathrm{A}$ est isomorphe au produit

$$(p^{n-1}\mathbf{Z}/p^n\mathbf{Z})^r \times \prod_{j=1}^{s} p^{n-1}(\mathbf{Z}/d_j\mathbf{Z})/p^n(\mathbf{Z}/d_j\mathbf{Z}).$$

Son cardinal est $p^{r+s(p^n)}$ où $s(p^n)$ est le nombre des entiers j tels que p^n divise d_j. Comme $d_1|d_2|\ldots|d_s$, $s(p^n)$ est le plus grand entier j tel que p^n divise d_j. Dit autrement, p^n divise d_j si et seulement si $s(p^n) \geqslant j$, donc si et seulement si $\mathrm{Card}(p^{n-1}\mathrm{A}/p^n\mathrm{A}) \geqslant p^{r+j}$.

Pour tout nombre premier p qui ne divise pas d_1, cette formule entraîne que $\mathrm{Card}(\mathrm{A}/p\mathrm{A}) = p^r$; l'entier r est ainsi déterminé par le groupe abélien A. Pour chaque nombre premier p, on déduit alors de cette formule les exposants de la décomposition en facteurs premiers de d_j. L'unicité annoncée en découle. □

Exemple **(2.9.13)**. — Comme $6 = 2\cdot 3$ et $12 = 4\times 3$, on a des isomorphismes

$$\begin{aligned}(\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/6\mathbf{Z}) &\simeq (\mathbf{Z}/4\mathbf{Z}) \times ((\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})) \\ &\simeq (\mathbf{Z}/2\mathbf{Z}) \times ((\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})) \\ &\simeq (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/12\mathbf{Z}).\end{aligned}$$

En évaluant cette expression en $\mathrm{T} = a_j$, on trouve

$$u_j \prod_{p\neq j}(a_j - a_p) = 0,$$

d'où $u_j = 0$ puisque $a_j \neq a_p$ si $p \neq j$.

Pour tout entier d, notons V_d le sous-ensemble de l'anneau $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ formé des polynômes de degrés $\leqslant d$; c'est un sous-espace vectoriel de dimension finie. Posons aussi $\mathrm{W}_d = f(\mathrm{V}_d)$; c'est un sous-$\mathbf{C}$-espace vectoriel de dimension finie de K et l'on a $\mathrm{K} = \bigcup_d \mathrm{W}_d$. Pour tout entier d, l'ensemble S_d des éléments $a \in \mathrm{A}$ tels que $w_a \in \mathrm{W}_d$ est donc fini. Puisque $\mathrm{K} = \bigcup_d \mathrm{W}_d$, on a $\bigcup_d \mathrm{S}_d = \mathbf{C}$. Cela prouve que $\mathbf{C}$ est réunion d'une famille dénombrable d'ensembles finis, donc est dénombrable. Cette contradiction prouve que l'homomorphisme φ n'est pas injectif, c'est-à-dire qu'il existe un polynôme $\mathrm{P} \in \mathbf{C}[\mathrm{T}]$, non nul, tel que $\mathrm{P}(w) = 0$; prenons P de degré minimal. Le polynôme P n'est pas constant, donc il a une racine, disons a. Soit $\mathrm{P} = (\mathrm{T}-a)\mathrm{Q} + \mathrm{R}$ la division euclidienne de P par $\mathrm{T}-a$; on a $\deg(\mathrm{R}) < 1$, donc R est constant, de valeur $\mathrm{R}(a) = \mathrm{P}(a) = 0$; ainsi $\mathrm{P} = (\mathrm{T}-a)\mathrm{Q}$ et $(w-a)\mathrm{Q}(w) = \mathrm{P}(w) = 0$. Comme $\deg(\mathrm{Q}) < \deg(\mathrm{P})$, on a $\mathrm{Q}(w) \neq 0$; comme K est un corps, on a donc $w - a = 0$, c'est-à-dire $\mathrm{T}_i - a \in \mathrm{M}$.

En définitive, nous avons donc démontré qu'il existe des éléments $a_1, \ldots, a_n \in \mathbf{C}$ tels que $\mathrm{T}_i - a_i \in \mathrm{M}$ pour tout i. Ainsi, l'idéal $\mathrm{M}_a = (\mathrm{T}_1 - a_1, \ldots, \mathrm{T}_n - a_n)$ est contenu dans M, donc $\mathrm{M} = \mathrm{M}_a$ puisque M_a est un idéal maximal de $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$. □

3.10.2. — Si E est une partie de $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$, on note $\mathscr{V}(\mathrm{E})$ l'ensemble des points $a \in \mathbf{C}^n$ tels que $f(a) = 0$ pour tout $f \in \mathrm{E}$. On dit que c'est l'*ensemble algébrique* de $\mathbf{C}^n$ défini par E.

Lemme **(3.10.3)**. — a) *On a* $\mathscr{V}(\varnothing) = \mathbf{C}^n$ *et* $\mathscr{V}(1) = \varnothing$.

b) *Si* E, E' *sont des parties de* $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ *telles que* $\mathrm{E} \subset \mathrm{E}'$, *on a* $\mathscr{V}(\mathrm{E}') \subset \mathscr{V}(\mathrm{E})$.

c) *Pour toute famille* $(\mathrm{E}_i)_{i\in\mathrm{I}}$ *de parties de* $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$, *on a* $\mathscr{V}(\bigcup_{i\in\mathrm{I}} \mathrm{E}_i) = \bigcap_{i\in\mathrm{I}} \mathscr{V}(\mathrm{E}_i)$.

d) *Soit* E, E' *des parties de* $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ *et soit* EE' *l'ensemble des produits* fg, *pour* $f \in \mathrm{E}$ *et* $g \in \mathrm{E}'$; *on a* $\mathscr{V}(\mathrm{EE}') = \mathscr{V}(\mathrm{E}) \cup \mathscr{V}(\mathrm{E}')$.

e) *Soit* E *une partie de* $\mathbf{C}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ *et soit* I *l'idéal engendré par* E. *On a* $\mathscr{V}(\mathrm{E}) = \mathscr{V}(\mathrm{I}) = \mathscr{V}(\sqrt{\mathrm{I}})$.

Démonstration. — Soit $a \in \mathbf{C}^n$. L'application φ_a de $\mathbf{C}[T_1, \dots, T_n]$ dans $\mathbf{C}$ donnée par $\varphi_a(f) = f(a)$ est un homomorphisme d'algèbres, surjectif, et M_a est son noyau. Par passage au quotient, il induit donc un isomorphisme de $\mathbf{C}[T_1, \dots, T_n]/M_a$ sur $\mathbf{C}$, ce qui prouve que M_a est un idéal maximal de $\mathbf{C}[T_1, \dots, T_n]$.

On a $T_i - a_i \in M_a$ pour tout $i \in \{1, \dots, n\}$, donc $(T_1 - a_1, \dots, T_n - a_n) \subset M_a$. Inversement, soit $f \in \mathbf{C}[T_1, \dots, T_n]$. Pour tout $i \in \{1, \dots, n\}$, on a $T_i \equiv a_i \pmod{T_i - a_i}$, donc $T_i \equiv a_i \pmod{(T_1 - a_1, \dots, T_n - a_n)}$; par suite, pour tout $m \in \mathbf{N}^n$, on a $T^m = \prod T_i^{m_i} \equiv \prod a_i^{m_i} \pmod{(T_1 - a_1, \dots, T_n - a_n)}$. Il en résulte que $f = \sum f_m T^m \equiv f(a) \pmod{(T_1 - a_1, \dots, T_n - a_n)}$. Cela démontre que $f(a) = 0$ si et seulement si $f \in (T_1 - a_1, \dots, T_n - a_n)$.

Soit $b \in \mathbf{C}^n$ tel que $b \neq a$; soit $i \in \{1, \dots, n\}$ tel que $b_i \neq a_i$. Alors $T_i - a_i \in M_a$ mais $T_i - a_i \notin M_b$; cela prouve que $M_a \neq M_b$.

Soit M un idéal maximal de $\mathbf{C}[T_1, \dots, T_n]$, soit K l'anneau quotient $\mathbf{C}[T_1, \dots, T_n]/M$ et soit $f : \mathbf{C}[T_1, \dots, T_n] \to K$ la surjection canonique ; posons $w = f(T_i)$. Soit $i \in \{1, \dots, n\}$ et démontrons qu'il existe $a_i \in \mathbf{C}$ tel que $T_i - a_i \in M$, c'est-à-dire $w = a_i$.

Soit $\varphi : \mathbf{C}[T] \to K$ l'unique homomorphisme de $\mathbf{C}$-algèbres qui applique T sur w. Supposons d'abord que l'homomorphisme φ soit injectif. On a donc $w \neq a$ pour tout $a \in \mathbf{C}$; posons alors $w_a = 1/(w - a)$. La famille $(w_a)_{a \in \mathbf{C}}$ est linéairement indépendante sur $\mathbf{C}$. C'est essentiellement une conséquence de la décomposition en éléments simples mais nous allons le démontrer directement. Soit $a_1, \dots, a_m$ des nombres complexes deux à deux distincts et soit $u_1, \dots, u_m$ des nombres complexes tels que $\sum_{j=1}^m u_j w_{a_j} = 0$. On a donc

$$\sum_{j=1}^{m} u_j \prod_{\substack{p=1 \\ p \neq j}}^{m} (w - a_p) = 0,$$

soit encore

$$\varphi\left(\sum_{j=1}^{m} u_j \prod_{\substack{p=1 \\ p \neq j}}^{m} (T - a_p) \right) = 0.$$

Comme φ est injectif, on a donc

$$\sum_{j=1}^{m} u_j \prod_{\substack{p=1 \\ p \neq j}}^{m} (T - a_p) = 0.$$

2.10. Le groupe des permutations $\mathfrak{S}_n$

Lemme **(2.10.1)**. — *Pour tout entier $n \geqslant 3$, le centre $Z(\mathfrak{S}_n)$ du groupe symétrique $\mathfrak{S}_n$ est réduit à l'identité.*

Démonstration. — Soit $\sigma \in \mathfrak{S}_n$ une permutation distincte de l'identité. Soit $i \in \{1, \dots, n\}$ tel que $\sigma(i) \neq i$. Posons $j = \sigma(i)$ et soit k un élément de $\{1, \dots, n\}$ distinct de i et de j ; soit τ la transposition $(i\ k)$. On a $\tau \circ \sigma(i) = \tau(j) = j$ et $\sigma \circ \tau(i) = \sigma(k) \neq \sigma(i) = j$. Ainsi, $\tau \circ \sigma \neq \sigma \circ \tau$ et σ n'appartient pas au centre de $\mathfrak{S}_n$. □

2.10.2. — Soit $\sigma \in \mathfrak{S}_n$ une permutation de l'ensemble $\{1, \dots, n\}$. On déduit de σ une opération du groupe $\mathbf{Z}$ dans l'ensemble $\{1, \dots, n\}$, pour laquelle $1 \cdot i = \sigma(i)$, pour tout i. Les orbites de cette opération sont appelées les orbites de σ.

On dit qu'une permutation est un *cycle* si elle possède exactement une orbite de cardinal $\geqslant 2$.

On appelle *support* de σ l'ensemble des éléments $i \in \{1, \dots, n\}$ tels que $\sigma(i) \neq i$; c'est la réunion des orbites de cardinal $\geqslant 2$ de σ.

Lemme **(2.10.3)**. — *Deux permutations de supports disjoints commutent.*

Démonstration. — Considérons en effet deux permutations σ et τ de supports disjoints. Soit i un élément de $\{1, \dots, n\}$. Si i n'appartient ni au support de σ, ni à celui de τ, alors $\sigma(i) = \tau(i) = i$, d'où $\sigma(\tau(i)) = \sigma(i) = i = \tau(\sigma(i))$. Supposons maintenant que i appartient au support de σ, c'est-à-dire $\sigma(i) \neq i$; alors, $\sigma(\sigma(i)) \neq \sigma(i)$, donc $\sigma(i)$ appartient aussi au support de σ. Puisque les supports de σ et de τ sont disjoints, on a donc $\tau(i) = i$ et $\tau(\sigma(i)) = \sigma(i)$. Par suite, $\sigma(\tau(i)) = \sigma(i) = \tau(\sigma(i))$. On prouve cette relation de façon analogue lorsque i appartient au support de τ. Cela prouve que $\sigma \circ \tau = \tau \circ \sigma$. □

2.10.4. — Soit $\sigma \in \mathfrak{S}_n$; notons $\mathrm{Orb}(\sigma)$ l'ensemble de ses orbites. Pour chaque orbite O, soit σ_O la permutation qui coïncide avec σ en tout point de O et qui est l'identité hors de O. On a $\sigma_O = e$ si $\mathrm{Card}(O) = 1$; sinon, son support est égal à O. De plus, O est une orbite de σ_O, et les autres orbites sont réduites à un élément.

Compte tenu du lemme précédent, cela prouve en particulier que les permutations σ_O commutent deux à deux. On peut ainsi considérer le produit $\prod_{O \in \mathrm{Orb}(\sigma)} \sigma_O$ sans préciser l'ordre des facteurs. Démontrons que l'on a $\sigma =$

$\prod_{O\in\mathrm{Orb}(\sigma)} \sigma_O$ (*décomposition d'une permutation en produit de cycles de supports disjoints*).

Soit i un élément de $\{1,\dots,n\}$ et soit ω l'unique orbite de σ qui contient i. Si O est une orbite de σ distincte de ω, on a $\sigma_O(i) = i$. Par suite,

$$\prod_{O\in\mathrm{Orb}(\sigma)} \sigma_O(i) = \sigma_\omega(i) = \sigma(i),$$

par définition de σ_ω.

2.10.5. — Soit $\sigma \in \mathfrak{S}_n$. On appelle *type* de la permutation σ la suite des cardinaux de ses orbites, classés par ordre décroissant. Par exemple, le type de l'identité est $(1,\dots,1)$, celui d'une transposition est $(2,1,\dots,1)$, tandis que le type de la permutation circulaire $(1\ 2\ \dots\ n)$ est (n). Dans tous les cas, la somme de ses termes est égale à n; on dit que c'est une *partition* de n.

Proposition **(2.10.6)**. — *Pour que deux permutations soient conjuguées, il faut et il suffit qu'elles aient même type.*

Démonstration. — Soit σ une permutation; soit $(m_1,\dots,m_r)$ son type et écrivons-la comme produit de cycles de supports disjoints :

$$\sigma = (a_1\ \dots\ a_{m_1})(a_{m_1+1}\ \dots\ a_{m_1+m_2})\dots(a_{m_1+\cdots+m_{r-1}+1}\ \dots\ a_n).$$

Soit $\tau \in \mathfrak{S}_n$; on a alors

$$\tau\sigma\tau^{-1} = (\tau(a_1)\ \dots\ \tau(a_{m_1}))(\tau(a_{m_1+1})\ \dots\ \tau(a_{m_1+m_2}))\dots(\tau(a_{m_1+\cdots+m_{r-1}+1})\ \dots\ \tau(a_n)),$$

ce qui prouve que le type de $\tau\sigma\tau^{-1}$ est le même que celui de σ.

Soit maintenant σ' une permutation ayant même type que σ; écrivons-la comme produit de cycles de supports disjoints :

$$\sigma' = (b_1\ \dots\ b_{m_1})(b_{m_1+1}\ \dots\ b_{m_1+m_2})\dots(b_{m_1+\cdots+m_{r-1}+1}\ \dots\ b_n).$$

Soit alors τ la permutation de $\{1,\dots,n\}$ telle que $\tau(a_i) = b_i$ pour tout i. On a $\sigma' = \tau\sigma\tau^{-1}$. □

de A si et seulement si J/I est un idéal premier de A/I. Ainsi, $p^{-1}(N_{A/I})$ est l'intersection de la famille des idéaux premiers de A qui contiennent I, ce qu'il fallait démontrer. □

Proposition **(3.9.9)**. — *Soit* X *un espace topologique compact métrisable. Pour tout* $x \in X$, *l'ensemble* $M_x = \{f \in \mathscr{C}(X;\mathbf{R})\,;\, f(x) = 0\}$ *est un idéal maximal de l'anneau* $\mathscr{C}(X;\mathbf{R})$. *Inversement, pour tout idéal maximal* M *de* $\mathscr{C}(X;\mathbf{R})$, *il existe un unique point* $x \in X$ *tel que* $M = M_x$.

Démonstration. — Soit d une distance qui définit la topologie de X. L'ensemble M_x est le noyau de l'homomorphisme surjectif de $\mathbf{R}$-algèbres $\varepsilon_x : \mathscr{C}(X;\mathbf{R}) \to \mathbf{R}$ donné par $f \mapsto f(x)$; c'est donc un idéal de $\mathscr{C}(X;\mathbf{R})$. Par passage au quotient, on déduit de ε_x un isomorphisme de l'algèbre $\mathscr{C}(X;\mathbf{R})/M_x$ sur $\mathbf{R}$; par suite, M_x est un idéal maximal.

Soit $x \in X$. L'application $d_x : p \mapsto d(x,p)$ est continue et appartient à M_x, mais n'appartient pas à M_y si $y \neq x$, car $d(x,y) \neq 0$. Cela prouve que $M_x \neq M_y$ si $x \neq y$.

Enfin, soit M un idéal maximal de $\mathscr{C}(X;\mathbf{R})$ et démontrons qu'il existe $x \in X$ tel que $f(x) = 0$ pour tout $f \in M$. Pour tout $f \in M$, posons $Z_f = f^{-1}(0)$; c'est une partie fermée de X. Soit Z l'intersection des Z_f, pour $f \in M$.

Supposons par l'absurde que Z est vide. Il existe alors une suite finie $(f_1,\dots,f_n)$ d'éléments de M telle que $Z_{f_1} \cap \dots \cap Z_{f_n} = \varnothing$; alors la fonction $f = \sum f_i^2$ est continue et appartient à M, pour tout $x \in M$, il existe i tel que $f_i(x) \neq 0$, donc $f(x) \neq 0$. Soit g la fonction sur X donnée par $g(x) = 1/f(x)$; elle est continue donc on a $1 = gf \in M$. Par suite, $M = \mathscr{C}(X;\mathbf{R})$, contrairement à l'hypothèse que M est un idéal maximal.

Donc Z n'est pas vide; soit x un point de Z. On a $f(x) = 0$ pour tout $f \in M$, donc $M \subset M_x$. Comme M est un idéal maximal de $\mathscr{C}(X;\mathbf{R})$, cela entraîne $M = M_x$. □

3.10. Le théorème des zéros de Hilbert

Théorème **(3.10.1)** (Théorème des zéros de Hilbert, « Nullstellensatz »)

Soit n *un entier. Pour tout* $a \in \mathbf{C}^n$, *l'ensemble* $M_a = \{f \in \mathbf{C}[T_1,\dots,T_n]\,;\, f(a) = 0\}$ *est un idéal maximal de l'anneau* $\mathbf{C}[T_1,\dots,T_n]$, *égal à* $(T_1 - a_1,\dots,T_n - a_n)$. *Inversement, pour tout idéal maximal* M *de* $\mathbf{C}[T_1,\dots,T_n]$, *il existe un unique élément* $a \in \mathbf{C}^n$ *tel que* $M = M_a$.

alors $ba \in M_s$ car M_s est un idéal de A, donc $ba \in M$. Cela démontre que M est un idéal de A qui contient I. Pour tout $s \in S$, on a $M_s \neq A$, par hypothèse; en particulier, $1 \notin M_s$. Par suite, $1 \notin M$ et $M \neq A$.

Il résulte alors du théorème de Zorn (théorème 1.1.18) que l'ensemble $\mathscr{M}$ possède un élément maximal, disons M. C'est un idéal de A qui contient I et qui est distinct de A. Démontrons que M est un idéal maximal de A. Soit M' un idéal de A tel que $M \subset M'$ et $M' \neq A$. Alors M' est un élément de $\mathscr{M}$ qui majore M; par définition d'un élément maximal, on a $M' = M$, ce qu'il allait démontrer. □

Corollaire **(3.9.6)**. — *Soit* A *un anneau commutatif et soit* a *un élément de* A. *Pour que* a *ne soit pas inversible, il faut et il suffit qu'il existe un idéal maximal* M *de* A *tel que* $a \in M$.

Corollaire **(3.9.7)**. — *Soit* A *un anneau commutatif. Pour qu'un élément* a *de* A *soit nilpotent, il faut et il suffit qu'il appartienne à tout idéal premier de* A.

Démonstration. — Soit a un élément nilpotent de A soit n un entier $\geqslant 1$ tel que $a^n = 0$. Soit P un idéal premier de A. On a donc $a^n \in P$. Appliquant la définition d'un idéal premier, on démontre alors par récurrence sur n que $a \in P$.

Inversement, supposons que a ne soit pas nilpotent. Soit S la partie multiplicative $\{1, a, \ldots\}$; elle ne contient pas 0, donc l'anneau de fractions A_S n'est pas nul. Soit M un idéal maximal de A_S et soit P son image réciproque par l'homomorphisme canonique j de A dans A_S (de sorte que $x \in P$ si et seulement si $j(x) = x/1 \in M$). L'idéal P est un idéal premier de A. Comme l'image $j(s)$ de s dans A_S est inversible, elle n'appartient pas à M, donc $s \notin P$. Cela démontre qu'il existe un idéal premier de A ne contenant pas S, et conclut la preuve du corollaire. □

Corollaire **(3.9.8)**. — *Soit* A *un anneau commutatif et soit* I *un idéal de* A. *Le radical de* I *est l'intersection de la famille des idéaux premiers de* A *qui contiennent* I.

Démonstration. — Soit $p : A \to A/I$ la surjection canonique Par définition, un élément de a appartient à $\sqrt{I}$ si et seulement $p(a)$ appartient au nilradical $N_{A/I}$ de A/I. Par suite, $\sqrt{I} = p^{-1}(N_{A/I})$. D'après le corollaire précédent, $N_{A/I}$ est l'intersection de la famille des idéaux premiers de A/I. Les idéaux de A/I sont de la forme J/I, où $J = p^{-1}(J/I)$ est un idéal de A qui contient I; comme l'anneau quotient $(A/I)/(J/I)$ est isomorphe à A/J, on voit que J est un idéal premier

2.10.7. — Soit $\sigma \in \mathfrak{S}_n$. On appelle *signature* de la permutation σ l'élément

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

A priori, $\varepsilon(\sigma)$ est un nombre rationnel non nul, mais nous allons voir que l'on a $\varepsilon(\sigma) \in \{-1, 1\}$.

Appelons *inversion* d'une permutation σ un couple (i, j) tel que $i < j$ et $\sigma(i) > \sigma(j)$. Soit $i(\sigma)$ le nombre d'inversions de σ, et démontrons que

(2.10.7.1) $$\varepsilon(\sigma) = (-1)^{i(\sigma)}.$$

Tout d'abord, le facteur $(\sigma(j) - \sigma(i))/(j - i)$ est positif si (i, j) n'est pas une inversion, et négatif sinon. Cela prouve que $\varepsilon(\sigma)$ est du même signe que $(-1)^{i(\sigma)}$. Considérons d'autre part le produit $P = \prod_{1 \leqslant i \neq j \leqslant n} (\sigma(j) - \sigma(i))$. Comme σ est une bijection de $\{1, \ldots, n\}$ sur lui-même, on a $P = \prod_{1 \leqslant i \neq j \leqslant n} (j - i)$. D'autre part, en regroupant pour $i < j$ le facteur correspondant au couple (i, j) avec celui correspondant au couple (j, i), on voit que

$$P = \prod_{1 \leqslant i < j \leqslant n} (\sigma(j) - \sigma(i)) \prod_{1 \leqslant i < j \leqslant n} (\sigma(i) - \sigma(j)) = (-1)^{n(n-1)/2} \prod_{1 \leqslant i < j \leqslant n} (\sigma(j) - \sigma(i))^2.$$

De même, $P = (-1)^{n(n-1)/2} \prod_{1 \leqslant i < j < n} (j - i)^2$, si bien que $\varepsilon(\sigma)^2 = 1$. La formule annoncée en résulte.

On dit qu'une permutation est *paire* si sa signature est égale à 1, et impaire sinon.

Exemple **(2.10.8)**. — Soit a et b deux éléments distincts de $\{1, \ldots, n\}$ et soit τ la transposition $(a\ b)$. Alors, $i(\tau) = 2|b - a| + 1$ et $\varepsilon(\tau) = -1$.

On peut supposer que $a < b$. Soit (i, j) un couple d'éléments de $\{1, \ldots, n\}$ tel que $i < j$. Si $i < a$ ou si $j > b$, alors (i, j) n'est pas une inversion. On peut donc supposer que $a \leqslant i < j \leqslant b$. Si $i \neq a$, alors (i, j) est une inversion si et seulement si $j = b$. Supposons enfin que $i = a$; pour que (a, j) soit une inversion il faut et il suffit que $a < j \leqslant b$. Ainsi, les inversions de τ sont les couples (i, b) pour $a + 1 \leqslant i \leqslant b - 1$ et les couples (a, j) pour $a + 1 \leqslant j \leqslant b$. Leur nombre est égal à $(b - 1 - a) + (b - a) = 2(b - a) - 1$. En particulier, $i(\tau)$ est impair, d'où $\varepsilon(\tau) = -1$.

Proposition **(2.10.9)**. — *L'application* $\sigma \mapsto \varepsilon(\sigma)$ *est un homomorphisme de groupes de* $\mathfrak{S}_n$ *dans* $\{\pm 1\}$.

Son noyau $\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$ qu'on appelle *groupe alterné*.

Démonstration. — On a $\varepsilon(\mathrm{id}) = 1$. Soit σ et τ des éléments de $\mathfrak{S}_n$. On a

$$\begin{aligned}\varepsilon(\sigma\tau) &= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j-i} \\ &= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)} \prod_{1\leqslant i<j\leqslant n} \frac{\tau(j)-\tau(i)}{j-i}.\end{aligned}$$

Le second facteur est égal à $\varepsilon(\tau)$. Démontrons que le premier vaut $\varepsilon(\sigma)$; en effet, pour tout couple (a, b) d'éléments de $\{1, \dots, n\}$ tels que $a < b$, il existe un unique couple (i, j) tel que $i < j$ et $\{\tau(i), \tau(j)\} = \{a, b\}$: l'entier i est le plus petit des deux $\tau^{-1}(a)$, $\tau^{-1}(b)$, et j est le plus grand. Si $i = \tau^{-1}(a)$, on a $j = \tau^{-1}(b)$, et $(\sigma(\tau(j)) - \sigma(\tau(i)))/(\tau(j) - \tau(i)) = (\sigma(b) - \sigma(a))/(b-a)$; sinon, $i = \tau^{-1}(b)$, $j = \tau^{-1}(a)$ et $(\sigma(\tau(j)) - \sigma(\tau(i)))/(\tau(j) - \tau(i)) = (\sigma(a) - \sigma(b))/(a-b) = (\sigma(b) - \sigma(a))/(b-a)$. Ainsi, les mêmes facteurs que ceux de $\varepsilon(\sigma)$ apparaissent dans le premier produit, d'où l'égalité voulue. Cela démontre que $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Ainsi, ε est un homomorphisme de groupes. □

Exemple **(2.10.10)**. — Soit p un entier tel que $2 \leqslant p \leqslant n$; démontrons que la signature d'un p-cycle est égale à $(-1)^{p-1}$.

Soit en effet $\sigma = (a_1 \ \dots \ a_p)$ un p-cycle et décomposons-le en produit de transpositions. On a en effet $(a_2 \ a_1)\sigma = (a_2 \ a_3 \ \dots \ a_p)$; par récurrence sur p, on a donc

$$\sigma = (a_1 \ \dots \ a_p) = (a_{p-1} \ a_p)(a_{p-2} \ a_{p-1}) \dots (a_1 \ a_2).$$

Ainsi, σ est le produit de $p-1$ transpositions ; chacune est de signature -1, si bien que $\varepsilon(\sigma) = (-1)^{p-1}$.

Lemme **(2.10.11)**. — a) *L'ensemble des 3-cycles engendre le groupe* $\mathfrak{A}_n$.

b) *Si* $n \geqslant 5$, *les 3-cycles sont deux à deux conjugués dans* $\mathfrak{A}_n$.

Démonstration. — On a déjà démontré qu'un 3-cycle appartient à $\mathfrak{A}_n$. Soit maintenant $\sigma \in \mathfrak{A}_n$; lorsqu'on écrit σ comme produit de transpositions, leur nombre est pair car $\varepsilon(\sigma) = 1$. Considérons un produit deux transpositions consécutives : $(a \ b)(c \ d)$, où $a \neq b$ et $c \neq d$. Ce produit vaut e si $\{c, d\} = \{a, b\}$. Supposons maintenant qu'il y ait trois entiers distincts parmi a, b, c, d, par

Soit $b \in \mathrm{A}$ tel que $v = ab$; on a $1 = p(u+v) = p(u) + p(v) = p(ab) = p(a)p(b) = xp(b)$, ce qui prouve que x est inversible dans A/I, d'inverse $p(b)$. □

Exemple **(3.9.3)**. — a) Dans l'anneau $\mathbf{Z}$, les idéaux maximaux sont ceux qui sont engendrés par un nombre premier ; outre ceux-ci, le seul idéal premier est l'idéal (0).

b) Dans l'anneau $\mathbf{C}[\mathrm{T}]$ des polynômes en une indéterminée à coefficients complexes, les idéaux maximaux sont ceux qui sont engendrés par un polynôme de la forme $\mathrm{T} - a$, pour $a \in \mathbf{C}$; outre ceux-ci, le seul idéal premier est l'idéal (0).

Exemple **(3.9.4)**. — Soit $f : \mathrm{A} \to \mathrm{B}$ un homomorphisme d'anneaux commutatifs, soit J un idéal premier de B et soit $\mathrm{I} = f^{-1}(\mathrm{J})$. Démontrons que I est un idéal premier de A.

C'est en effet un idéal de A et, comme $f(1_\mathrm{A}) = 1_\mathrm{B} \notin \mathrm{J}$, on a $1_\mathrm{A} \notin \mathrm{I}$, de sorte que $\mathrm{I} \neq \mathrm{A}$. Soit a, b des éléments de A tels que $ab \in \mathrm{I}$. Alors $f(a)f(b) = f(ab) \in \mathrm{J}$, donc $f(a) \in \mathrm{J}$ ou $f(a) \in \mathrm{J}$ car J est un idéal premier de B. Par suite, $a \in \mathrm{I}$ ou $b \in \mathrm{I}$. Cela démontre que I est un idéal premier de A.

On peut aussi démontrer ce résultat comme suit. Soit $p : \mathrm{B} \to \mathrm{B/J}$ la surjection canonique. Alors, l'homomorphisme $p \circ f : \mathrm{A} \to \mathrm{B/J}$ a pour noyau I ; il induit par passage au quotient un homomorphisme injectif de l'anneau A/I dans l'anneau B/J. Par hypothèse, l'anneau B/J est un anneau intègre, car J est un idéal premier de B. Par suite, l'anneau A/I, isomorphe à un sous-anneau de B/J, est également intègre, si bien que I est un idéal premier de A.

Théorème **(3.9.5)** (Krull). — *Soit* A *un anneau commutatif et soit* I *un idéal de* A *tel que* $\mathrm{I} \neq \mathrm{A}$. *Il existe un idéal maximal* M *de* A *tel que* $\mathrm{I} \subset \mathrm{M}$. *En particulier, l'ensemble des idéaux maximaux d'un anneau non nul n'est pas vide.*

Démonstration. — Soit $\mathscr{M}$ l'ensemble des idéaux J de A tels que $\mathrm{I} \subset \mathrm{J}$ et $\mathrm{J} \neq \mathrm{A}$. Munissons-le de la relation d'ordre donnée par l'inclusion. Démontrons que toute famille totalement ordonnée d'éléments de $\mathscr{M}$ est majorée. Soit donc $(\mathrm{M}_s)_{s\in\mathrm{S}}$ une telle famille. Si elle est vide, l'idéal I est un élément de $\mathscr{M}$ qui la majore. Supposons donc $\mathrm{S} \neq \varnothing$ et soit M la réunion de la famille (M_s) ; démontrons que M est un idéal de A tel que $\mathrm{I} \subset \mathrm{M}$ et $\mathrm{M} \neq \mathrm{A}$. Comme $\mathrm{S} \neq \varnothing$, il existe $s \in \mathrm{S}$, de sorte $\mathrm{M}_s \subset \mathrm{M}$; en particulier, $\mathrm{I} \subset \mathrm{M}$. Soit $a, b \in \mathrm{M}$; soit $s, t \in \mathrm{S}$ tels que $a \in \mathrm{M}_s$ et $b \in \mathrm{M}_t$; comme la famille (M_s) est totalement ordonnée, quitte à échanger a et b, on peut supposer que $\mathrm{M}_s \subset \mathrm{M}_t$; alors $a, b \in \mathrm{M}_t$ donc $a + b \in \mathrm{M}_t$ car M_t est un idéal de A. Soit $a \in \mathrm{M}$ et soit $b \in \mathrm{A}$; soit $s \in \mathrm{S}$ tel que $a \in \mathrm{M}_s$;

Comme un corps est un anneau intègre, un idéal maximal est un idéal premier. Comme l'anneau nul n'est pas intègre, l'idéal I = A n'est pas un idéal premier.

Proposition **(3.9.2)**. — *Soit* A *un anneau commutatif et soit* I *un idéal de* A *tel que* $I \neq A$.

a) *Les conditions suivantes sont équivalentes :*

(i) *L'idéal* I *est un idéal premier ;*

(ii) *Pour tout couple* (a, b) *d'éléments de* A *tels que* $ab \in I$, *on a* $a \in I$ *ou* $b \in I$.

b) *Les conditions suivantes sont équivalentes :*

(i) *L'idéal* I *est un idéal maximal ;*

(ii) *Pour tout* $a \in A - I$, *il existe* $b \in A$ *tel que* $1 - ab \in I$;

(iii) *Les seuls idéaux de* A *qui contiennent* I *sont* I *et* A.

Démonstration. — Dans toute la preuve, on note $p : A \to A/I$ la surjection canonique.

a) Supposons que I soit un idéal premier ; soit a, b des éléments de A tels que $ab \in I$. Alors $p(a)p(b) = 0$. Par hypothèse, l'anneau A/I est intègre ; on a donc $p(a) = 0$ ou $p(b) = 0$, c'est-à-dire $a \in I$ ou $b \in I$.

Inversement, supposons cette condition (ii) satisfaite et démontrons que l'anneau A/I est intègre. Il est non nul car $I \neq A$. Soit x, y des éléments de A/I tels que $xy = 0$; soit $a, b \in A$ tels que $x = p(a)$ et $y = p(b)$. Alors, $0 = xy = p(a)p(b) = p(ab)$, donc $ab \in I$. Par hypothèse, on a donc $a \in I$ ou $b \in I$; dans le premier cas, $x = 0$, dans le second $y = 0$.

b) Supposons que I soit un idéal maximal et soit $a \in A - I$. Alors, $p(a) \neq 0$; comme l'anneau A/I est un corps, il existe $y \in A/I$ tel que $p(a)y = 1$. Soit $b \in A$ tel que $y = p(b)$; on a donc $p(ab) = 1 = p(1)$, donc $p(1 - ab) = 0$, c'est-à-dire $1 - ab \in I$.

Supposons la condition (ii) satisfaite et soit J un idéal de A qui contient I. Supposons $J \neq I$ et soit alors $a \in J - I$. Par hypothèse, il existe $b \in A$ tel que $1 - ab \in I$. Alors, $1 = (1 - ab) + ab$ appartient à J, ce qui entraîne J = A.

Supposons enfin la condition (iii) satisfaite et démontrons que l'anneau A/I est un corps. Comme l'idéal I est distinct de A, l'anneau A/I n'est pas nul. Soit x un élément non nul de A/I, soit $a \in A$ tel que $x = p(a)$ et soit J l'idéal $I + (a)$ de A. Il contient I ; comme $x \neq 0$, $a \notin I$, et comme $a \in J$, on a donc $I \neq J$. Par hypothèse, on a donc J = A et, en particulier, $1 \in J$. Il existe donc $u \in I$ et $v \in (a)$ tels que $1 = u + v$.

exemple a, b, c, et que $d = a$; alors, $(a\ b)(c\ d) = (a\ c\ b)$ est un 3-cycle. Enfin, si les quatre entiers a, b, c, d sont deux à deux distincts, on a

$$(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d)$$

et ce produit est le produit de deux 3-cycles.

Considérons maintenant deux 3-cycles$(1\ 2\ 3)$ et $(a\ b\ c)$. Soit σ une permutation telle que $\sigma(1) = a$, $\sigma(2) = b$ et $\sigma(3) = c$. On a donc $\sigma(1\ 2\ 3)\sigma^{-1} = (a\ b\ c)$. Si $\varepsilon(\sigma) = 1$, cela prouve que $(1\ 2\ 3)$ et $(a\ b\ c)$ sont conjugués dans $\mathfrak{A}_n$; sinon, on remplace σ par la transposition $\sigma \circ (4\ 5)$ (c'est là qu'on utilise l'hypothèse que $n \geqslant 5$) et l'on obtient encore le résultat voulu. □

Proposition **(2.10.12)**. — a) *On a* $D(\mathfrak{S}_n) = \mathfrak{A}_n$;

b) *Pour* $n \geqslant 5$, *on a* $D(\mathfrak{A}_n) = \mathfrak{A}_n$;

Démonstration. — a) Pour toute permutation σ, on a $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$, ce qui entraîne qu'un commutateur est une permutation paire donc $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$. Inversement, notons A le groupe quotient $\mathfrak{S}_n/D(\mathfrak{S}_n)$ et considérons la surjection canonique $f : \mathfrak{S}_n \to A$. Les transpositions sont deux à deux conjuguées dans $\mathfrak{S}_n$, donc ont même image dans le groupe commutatif A ; notons a cette image. Comme $\mathfrak{S}_n$ est engendré par les transpositions, a engendre A. Enfin, comme une transposition est d'ordre 2, on a $a^2 = e$. Enfin, $a \neq e$ car une transposition, de signature -1, n'appartient pas à $\mathfrak{A}_n$. Il en résulte que $A = \{e, a\}$ est de cardinal 2 et $\mathrm{Card}(D(\mathfrak{S}_n)) = \frac{1}{2}\mathrm{Card}(\mathfrak{S}_n) = \mathrm{Card}(\mathfrak{A}_n)$. Finalement, l'inclusion $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$ entraîne que $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

b) Raisonnons de façon analogue. Soit B le groupe quotient $\mathfrak{A}_n/D(\mathfrak{A}_n)$ et notons $g : \mathfrak{A}_n \to B$ la surjection canonique. Puisque $n \geqslant 5$, les 3-cycles sont deux à deux conjugués dans $\mathfrak{A}_n$, donc ont même image dans B ; notons-la b. Remarquons que le carré du 3-cycle $(1\ 2\ 3)$ est égal à $(1\ 3\ 2)$, donc est encore un 3-cycle ; par suite, $b = b^2$, si bien que $b = e$. Enfin, les 3-cycles engendrant $\mathfrak{A}_n$, B est engendré par b, si bien que $B = \{e\}$. Cela prouve que $D(\mathfrak{A}_n) = \mathfrak{A}_n$.

□

Remarque **(2.10.13)**. — Lorsque $n \leqslant 3$, le groupe alterné $\mathfrak{A}_n$ est commutatif et $D(\mathfrak{A}_n) = \{e\}$. Lorsque $n = 4$, le groupe $D(\mathfrak{A}_4)$ est le sous-groupe $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$; il est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.

Théorème **(2.10.14)**. — *Pour* $n \geqslant 5$, *le groupe* $\mathfrak{A}_n$ *est simple.*

Démonstration. — Soit G un sous-groupe distingué de $\mathfrak{A}_n$, distinct de $\{e\}$, et démontrons que $G = \mathfrak{A}_n$. Soit σ un élément de G, distinct de e, et dont le support est de cardinal minimal ; démontrons que σ est un 3-cycle. Pour tout élément τ de $\mathfrak{S}_n$, on a

$$[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau = \sigma^{-1}(\tau^{-1}\sigma\tau)\,;$$

comme G est un sous-groupe distingué de $\mathfrak{A}_n$, on a $\tau^{-1}\sigma\tau \in G$, si bien que $[\sigma, \tau] \in G$. Si σ n'est pas un 3-cycle, nous allons montrer que l'on peut choisir τ de façon convenable de sorte que le commutateur $[\sigma, \tau]$ soit différent de l'identité mais que le cardinal de son support soit strictement inférieur à celui de σ.

Écrivons la décomposition de σ en produit de cycles à supports disjoints de longueurs $m_1 \geqslant m - 2 \geqslant \cdots \geqslant m_r$:

$$\sigma = (a_1 \ \ldots \ a_{m_1})(a_{m_1+1} \ \ldots \ a_{m_1+m_2}) \ldots (a_{m_1+\cdots+m_{r-1}+1} \ \ldots \ a_n).$$

Comme $\sigma \neq \mathrm{id}$, on a $m_1 \geqslant 2$.

Premier cas : $m_1 \geqslant 4$. — On pose alors $\tau = (a_1\ a_2\ a_3)$. Par construction, on a $\tau(a_i) = a_i$ pour $i > m_1$, donc $\tau^{-1}\sigma\tau(a_i) = \sigma(a_i)$, puis $\varphi(a_i) = a_i$. Pour la même raison, si $4 \leqslant i \leqslant m_1 - 1$, alors

$$\tau^{-1}\sigma\tau(a_i) = \tau^{-1}\sigma(a_i) = \tau^{-1}(a_{i+1}) = a_{i+1} = \sigma(a_i),$$

de sorte que $[\sigma, \tau](a_i) = a_i$. Par suite, le support de $[\sigma, \tau]$ est contenu dans $\{a_1, a_2, a_3, a_{m_1}\}$. En calculant explicitement $\tau^{-1}\sigma\tau(a_i)$ pour $i = 1$ et 2, on obtient

$$[\sigma, \tau](a_1) = \sigma^{-1}\tau^{-1}\sigma\tau(a_1) = \sigma^{-1}\tau^{-1}\sigma(a_2) = \sigma^{-1}\tau^{-1}(a_3) = \sigma^{-1}(a_2) = a_1,$$
$$[\sigma, \tau](a_2) = \sigma^{-1}\tau^{-1}\sigma\tau(a_2) = \sigma^{-1}\tau^{-1}\sigma(a_3) = \sigma^{-1}\tau^{-1}(a_4) = \sigma^{-1}(a_4) = a_3,$$

ce qui prouve que $[\sigma, \tau] \neq \mathrm{id}$ et que son support est contenu dans $\{a_2, a_2, a_{m_1}\}$, ce qui contredit l'hypothèse que le support de σ est de cardinal minimal. (On peut vérifier que $[\sigma, \tau] = (a_2\ a_3\ a_{m_1})$ est un 3-cycle.)

Deuxième cas : $m_1 = 3$. — Si $m_2 = 1$, alors σ est un 3-cycle. Si $m_2 = 2$, observons que $\sigma^2 = (a_1\ a_3\ a_2)$ est un 3-cycle. Supposons donc $m_2 \geqslant 3$ et posons $\tau = (a_1\ a_2\ a_4)$. On a

$$\sigma^{-1}\tau^{-1}\sigma\tau(a_1) = \sigma^{-1}\tau^{-1}\sigma(a_1) = \sigma^{-1}\tau^{-1}(a_2) = \sigma^{-1}(a_1) = a_3,$$

donc $[\sigma, \tau] \neq e$. Soit $i \geqslant 5$ et soit j tel que $\sigma(a_i) = a_j$; observons que l'on a $j \geqslant 5$ sauf si $i = m_1 + m_2$, auquel cas on a $j = m_1 + 1 = 4$. Par suite, si $i \geqslant 5$ et $i \neq m_1 + m_2$,

le coefficient de T^n dans f ; on a $a \in J_n$ par définition. Posons $p = \min(m, n)$, de sorte que $p \leqslant m$ et $a \in J_p$. Il existe donc une famille $(c_s)_{s\in S_p}$ d'éléments de A $\sum c_s s$ soit un polynôme appartenant à I, de degré $\leqslant p$, et dont le coefficient de T^p est égal à a. Posons $g = f - \sum c_s T^{n-p} s$; c'est un polynôme appartenant à I de degré $\leqslant n$ et dont le coefficient de T^n est nul ; on a donc $\deg(g) < n$. Par récurrence, on a $g \in \langle S\rangle$; par ailleurs, comme $S_p \subset S$, le polynôme $\sum_{s\in S_p} c_s T^{n-p} s$ appartient à $\langle S\rangle$, par définition de l'idéal engendré par une partie. Cela entraîne que $f \in \langle S\rangle$, d'où le théorème. □

Corollaire **(3.8.12)**. — *Soit* A *un anneau commutatif noethérien. Pour tout entier $n \geqslant 0$, l'anneau $A[T_1, \ldots, T_n]$ est noethérien.*

Démonstration. — Compte tenu des isomorphismes $A[T_1, \ldots, T_n] \simeq A[T_1, \ldots, T_{n-1}][T_n]$, cela se déduit du théorème 3.8.11, par récurrence sur n. □

Un corps commutatif est un anneau noethérien ; on en déduit le cas particulier suivant :

Corollaire **(3.8.13)**. — *Soit* K *un corps commutatif. Pour tout entier $n \geqslant 0$, l'anneau $K[T_1, \ldots, T_n]$ est noethérien.*

Corollaire **(3.8.14)**. — *Si* A *est un anneau commutatif noethérien, alors toute* A*-algèbre commutative de type fini est un anneau noethérien.*

Démonstration. — Soit B une A-algèbre commutative de type fini et soit $b = (b_1, \ldots, b_n)$ une suite finie d'éléments de B qui engendre B. L'homomorphisme de A-algèbres $\mathrm{ev}_b : A[T_1, \ldots, T_n] \to B$ est surjectif car son image contient les b_i ; par suite, l'homomorphisme ev_b induit, par passage au quotient, un isomorphisme de $A[T_1, \ldots, T_n]/\operatorname{Ker}(\mathrm{ev}_b)$ sur B. D'après le corollaire 3.8.12, $A[T_1, \ldots, T_n]$ est un anneau noethérien, donc son quotient $A[T_1, \ldots, T_n]/\operatorname{Ker}(\mathrm{ev}_b)$ en est également un. Cela entraîne que B est un anneau noethérien. □

3.9. Idéaux premiers, idéaux maximaux

Définition **(3.9.1)**. — *Soit* A *un anneau commutatif et soit* I *un idéal de* A. *On dit que* I *est* premier *si l'anneau* A/I *est intègre ; on dit que* I *est* maximal *si l'anneau* A/I *est un corps.*

On a alors

$$f = ab^{-1}\mathrm{T}^{m-n}g + ug + v = (ab^{-1}\mathrm{T}^{m-n} + u)\cdot g + v;$$

il suffit donc de poser $q = ab^{-1}\mathrm{T}^{m-n} + u$ et $r = v$.

Soit (q', r') un couple de polynômes tel que $f = q'g + r'$ et $\deg(r') < \deg(g)$. On a alors $r' - r = (q - q')g$. Si $q \neq q'$, alors $\deg(q - q') \geqslant 0$, si bien que $\deg(r' - r) = \deg(g) + \deg(q - q') \geqslant \deg(g)$; cela contredit l'hypothèse que $\deg(r), \deg(r') < \deg(g)$. Donc $q = q'$ et $r = r'$. □

Théorème **(3.8.11)** (Hilbert). — *Si* A *est un anneau commutatif noethérien, l'anneau* $\mathrm{A}[\mathrm{T}]$ *est noethérien.*

Démonstration. — Soit I un idéal de $\mathrm{A}[\mathrm{T}]$; démontrons que I possède une partie génératrice finie.

Pour tout entier n, notons J_n l'ensemble des coefficients de T^n des polynômes $f \in \mathrm{I}$ tels que $\deg(f) \leqslant n$. Démontrons que pour tout entier n, J_n est un idéal de A contenu dans J_{n+1}.

On a $0 \in \mathrm{J}_n$, car c'est le coefficient de T^n du polynôme nul. Soit $a, b \in \mathrm{J}_n$ et $c \in \mathrm{A}$ et démontrons que $a + b \in \mathrm{J}_n$ et $ca \in \mathrm{J}_n$. Soit $f, g \in \mathrm{I}$ des polynômes de degrés $\leqslant n$ et dont les coefficients de T^n sont égaux à a, b respectivement. Alors, $f + g$ et cf sont des polynômes de degrés $\leqslant n$, dont le coefficient de T^n est égal à $a + b$ et ca respectivement. Par suite, $a + b$ et ca appartiennent à J_n. Cela démontre que J_n est un idéal de A.

Soit enfin $a \in \mathrm{J}_n$ et soit $f \in \mathrm{I}$ un polynôme de degré $\leqslant n$ dont a est le coefficient de T^n. Alors $\mathrm{T}f$ est un polynôme de degré $\leqslant n + 1$ dans lequel a est le coefficient de T^{n+1}. On a donc $a \in \mathrm{J}_{n+1}$.

La suite (J_n) est une suite croissante d'idéaux de A. Comme A est un anneau noethérien,, ces idéaux possèdent donc une partie génératrice fini, et cette suite est stationnaire Soit m un entier tel que $\mathrm{J}_n = \mathrm{J}_m$ pour tout entier $n \geqslant m$. D'autre part, pour tout entier $n \leqslant m$, soit S_n une partie finie de I formée de polynômes de degré $\leqslant n$ dont les coefficients de T^n engendrent l'idéal J_n. Soit S la réunion des ensembles S_n, pour $n \leqslant m$; c'est une partie finie et nous allons démontrer que l'idéal engendré par S est égal à I.

On a tout d'abord $\mathrm{S} \subset \mathrm{I}$, par construction, donc l'idéal $\langle \mathrm{S} \rangle$ engendré par S est contenu dans I. Inversement, démontrons par récurrence sur le degré d'un élément $f \in \mathrm{I}$ qu'il appartient à $\langle \mathrm{S} \rangle$. C'est vrai si $f = 0$. Posons alors $n = \deg(f)$ et que $\langle \mathrm{S} \rangle$ contient tout polynôme appartenant à I dont le degré est $< n$. Soit a

on a

$$[\sigma, \tau](a_i) = \sigma^{-1}\tau^{-1}\sigma\tau(a_i) = \sigma^{-1}\tau^{-1}\sigma(a_i) = \sigma^{-1}\tau^{-1}(a_j) = \sigma^{-1}(a_j) = a_i.$$

Le support de $[\sigma, \tau]$ est donc contenu dans $\{a_1, \ldots, a_4, a_{m_1+m_2}\}$. Il est de cardinal $\leqslant 5$, alors que le support de σ est de cardinal $\geqslant 6$, ce qui contredit le choix de σ.

Troisième cas : $m_1 = 2$. — Si $m_2 = 1$, alors σ est une transposition, contrairement à l'hypothèse que σ est une permutation paire. Supposons donc $m_2 \geqslant 2$ et posons $\tau = (a_1, a_2, a_5)$. On vérifie d'abord que $[\sigma, \tau](a_i) = a_i$ pour $i = 3$ ou 4. Soit alors $i \geqslant 6$ et soit j tel que $\sigma(a_i) = a_j$; on a $j \geqslant 6$ à moins que $i = 6$ et $m_3 = 2$ auquel cas, on a $j = 5$. Alors, pour $i \geqslant 6$ (et différent de 6 si $m_3 = 2$), on a

$$[\sigma, \tau](a_i) = \sigma^{-1}\tau^{-1}\sigma\tau(a_i) = \sigma^{-1}\tau^{-1}\sigma(a_i) = \sigma^{-1}\tau^{-1}(a_j) = \sigma^{-1}(a_j) = a_i.$$

Par suite, le support de $[\sigma, \tau]$ est contenu dans $\{3, 4, 5, 6\}$ si $m_3 = 2$ et dans $\{3, 4, 5\}$ si $m_3 = 1$, donc son cardinal est strictement inférieur à celui de σ. En outre,

$$[\sigma, \tau](a_5) = \sigma^{-1}\tau^{-1}\sigma\tau(a_5) = \sigma^{-1}\tau^{-1}\sigma(a_1) = \sigma^{-1}\tau^{-1}(a_2) = \sigma^{-1}(a_1) = a_2,$$

si bien que $[\sigma, \tau] \neq e$. Cela contredit donc le choix de σ.

Finalement, σ est un 3-cycle. Comme G est un sous-groupe distingué de G et que les 3-cycles sont deux à deux conjugués dans $\mathfrak{A}_n$, le groupe G contient tous les 3-cycles. Puisque ceux-ci forment un ensemble générateur de $\mathfrak{A}_n$, on a $\mathrm{G} = \mathfrak{A}_n$, et cela conclut la démonstration. □

2.11. Théorèmes de Sylow

2.11.1. — Soit p un nombre premier. On dit qu'un groupe fini S est un p-groupe si son cardinal est une puissance de p. Soit G un groupe ; on dit qu'un sous-groupe S de A est un p-sous-groupe de Sylow de G si c'est un p-groupe et si son indice $(\mathrm{G} : \mathrm{S})$ est premier à p.

Dans ce paragraphe, nous allons démontrer l'existence de sous-groupes de Sylow et leurs premières propriétés. Nous verrons ainsi trois méthodes à l'œuvre pour produire des sous-groupes : constructions explicites ; stabilisateurs ; conjugaison et intersections.

Exemple **(2.11.2)**. — Soit $\mathrm{G} = \mathrm{GL}(n, \mathbf{Z}/p\mathbf{Z})$. Notons T l'ensemble des matrices triangulaires supérieures dont la diagonale est formée de 1 ; c'est un sous-groupe

de G de cardinal $\mathrm{Card}(T) = p^{(n-1)n/2}$; c'est donc un p-groupe. D'autre part, le groupe G est en bijection avec l'ensemble des bases du $(\mathbf{Z}/p\mathbf{Z})$-espace vectoriel $(\mathbf{Z}/p\mathbf{Z})^n$; on obtient une telle base en prenant un vecteur non nul e_1 (il y a $p^n - 1$ tels vecteurs), un vecteur e_2 non colinéaire à e_1 (il y en a $p^n - p$), un vecteur e_3 qui n'appartient pas au plan engendré par e_1 et e_2 (il y en a $p^n - p^2$), etc. Par suite,

$$\begin{aligned}\mathrm{Card}(G) &= (p^n-1)(p^n-p)\dots(p^n-p^{n-1}) \\ &= p^{1+2+\dots+(n-1)}(p^n-1)(p^{n-1}-1)\dots(p-1) \\ &= p^{(n-1)n/2}\prod_{i=1}^{n}(p^i-1).\end{aligned}$$

Ainsi, $(G : T) = \prod_{i=1}^{n}(p^i - 1)$ n'est pas multiple de p. Cela prouve que T est un p-sous-groupe de Sylow de G.

Exemple **(2.11.3)**. — Soit n un entier et soit $G = \mathbf{Z}/n\mathbf{Z}$; soit a l'exposant de p dans la décomposition en facteurs premiers de n et posons $m = n/p^a$. Alors $S = m\mathbf{Z}/n\mathbf{Z}$ est un p-sous-groupe de Sylow de G. C'est même le seul p-sous-groupe de Sylow. Soit en effet T un p-groupe contenu dans G et soit g un élément de T. L'ordre de g divise le cardinal de T, donc est une puissance de p ; il divise aussi le cardinal de G, qui est égal à n ; par suite, l'ordre de g divise p^a et l'on a $p^a g = 0$. Si g est la classe d'un entier x, cela signifie que $p^a x$ est multiple de n ; autrement dit, x est multiple de m et l'on a $g \in S$. Par suite, $T \subset S$ et la condition que p ne divise pas $(G : T)$ impose que $S = T$.

Proposition **(2.11.4)**. — *Soit* G *un groupe fini, soit p un nombre premier et soit a un entier tel que* p^a *divise le cardinal de* G. *Il existe alors un sous-groupe* S *de* G *de cardinal égal à* p^a.

Démonstration, d'après Wielandt *(1959)*. — Soit X l'ensemble des parties de G de cardinal p^a ; on le munit de l'opération de G par translations à gauche, donnée par $g \cdot A = gA$ pour toute partie $A \in X$ et tout $g \in G$. Soit $A \in X$ et soit $a \in A$; pour tout élément g du stabilisateur G_A de A, on a $ga \in A$, et l'application $g \mapsto ga$ de G_A dans A est injective. Par suite, $\mathrm{Card}(G_A) \leqslant \mathrm{Card}(A) = p^a$. Écrivons d'autre part que le cardinal de X est la somme des cardinaux des orbites de cette opération ; soit $R \subset X$ une partie telle que toute orbite soit l'orbite

homogène de degré $m + n$. De plus, la formule $fg = \sum_{i=0}^{m}\sum_{j=0}^{n} f_i g_j$ démontre que $fg - f_m g_n$ est une somme de polynômes de degrés $< m + n$, si bien que $\deg(fg - f_m g_n) < m + n$. Par suite, $\deg(fg) = \deg(f_m g_n) = m + n$.

Traitons enfin le cas général. L'ensemble S′ des $s \in S$ tels qu'il existe $m \in \mathbf{N}^{(S)}$ tel que $m_s \neq 0$ et $f_m \neq 0$ ou $g_m \neq 0$ est fini. Les indéterminées T_s, pour $s \in S'$, sont celles qui apparaissent effectivement dans f et g. Les polynômes f, g, fg appartiennent ainsi à la sous-algèbre $A[(T_s)_{s\in S'}]$ de $A[(T_s)_{s\in S}]$, et leurs degrés dans cette sous-algèbre coïncident avec ceux dans $A[(T_s)_{s\in S}]$. Comme S′ est fini, la relation $\deg(fg) = \deg(f) + \deg(g)$ est vraie dans l'algèbre $A[(T_s)_{s\in S'}]$, donc elle est vraie dans $A[(T_s)_{s\in S}]$. En particulier, $fg \neq 0$ si $f \neq 0$ et $g \neq 0$. □

Corollaire **(3.8.9)**. — *Soit* A *un anneau commutatif et soit* S *un ensemble. Si* A *est un anneau intègre, les éléments inversibles de* $A[(T_s)_{s\in S}]$ *sont les polynômes constants égaux à un élément inversible de* A.

Démonstration. — Pour tout élément inversible a de A, le polynôme constant de valeur a est inversible dans $A[(T_s)_{s\in S}]$, d'inverse le polynôme constant de valeur a^{-1}.

Soit f un polynôme inversible et soit $g \in A[(T_s)_{s\in S}]$ son inverse ; alors $fg = 1$ donc $\deg(f) + \deg(g) = \deg(1) = 0$, car A est intègre. Cela entraîne $\deg(f) = 0$, donc f est constant. De plus, le terme constant de fg est égal à $f_0 g_0 = 1$, donc f_0 est inversible dans A. □

Théorème **(3.8.10)** (Division euclidienne). — *Soit* A *un anneau commutatif, soit* $f, g \in A[T]$ *des polynômes en* une *indéterminée* T *à coefficient dans* A. *On suppose que le coefficient dominant de g est inversible dans* A. *Il existe alors un couple* (q, r) *de polynômes, et un seul, tels que* $f = qg + r$ *et* $\deg(r) < \deg(g)$.

On dit que r est le reste de la division euclidienne de f par g et que q est son quotient.

Démonstration. — Démontrons l'existence d'un tel couple par récurrence sur $\deg(f)$. Si $\deg(f) < \deg(g)$, on pose $q = 0$ et $r = f$. Sinon, notons $m = \deg(f)$, $n = \deg(g)$, a le coefficient dominant de f et b celui de g ; posons $h = f - ab^{-1}T^{m-n}g$. Le polynôme $ab^{-1}T^{m-n}g$ est de degré m et son coefficient dominant est égal à a ; par suite, le polynôme h est de degré $< n$. Par récurrence, il existe un couple (u, v) de polynômes tel que $h = ug + v$ et $\deg(v) < \deg(g)$.

Le coefficient f_0 de T^0 est appelé le terme constant de f. On dit qu'un polynôme est constant s'il est de degré $\leqslant 0$, c'est-à-dire si $f = f_0$. Les polynômes constants forment une sous-algèbre de $A[(T_s)_{s\in S}]$ qui s'identifie à l'anneau A.

Proposition **(3.8.8)**. — *Soit* A *un anneau commutatif et soit* $f, g \in A[(T_s)_{s\in S}]$.

a) *On a* $\deg(f+g) \leqslant \max(\deg(f), \deg(g))$*; si* $\deg(f) \neq \deg(g)$*, on a* $\deg(f+g) = \max(\deg(f), \deg(g))$.

b) *On a* $\deg(fg) \leqslant \deg(f) + \deg(g)$.

c) *Supposons que l'anneau* A *soit intègre. Alors l'anneau* $A[(T_s)_{s\in S}]$ *est intègre et l'on a* $\deg(fg) = \deg(f) + \deg(g)$.

Démonstration. — a) Notons (f_m) et (g_m) les coefficients de f et g. On a $f + g = \sum(f_m + g_m)T^m$; si $m > \max(\deg(f), \deg(g))$, on a $f_m = g_m = 0$, donc $f_m + g_m = 0$. Par suite, $\deg(f+g) \leqslant \max(\deg(f), \deg(g))$.

Supposons maintenant que $\deg(f) > \deg(g)$. On a déjà $\deg(f+g) \leqslant \deg(f)$. En outre, si m est un élément de $\mathbf{N}^{(S)}$ tel que $|m| = \deg(f)$ et $f_m \neq 0$, le monôme $f_m T^m$ apparaît dans $f+g$, ce qui prouve que $\deg(f+g) \geqslant |m|$. On a donc égalité.

b) Soit $p \in \mathbf{N}^{(S)}$; par définition, le coefficients de T^p dans fg est égal à $\sum_{m+n=p} f_m g_n$. Pour tous $m, n \in \mathbf{N}^{(S)}$ tels que $m+n = p$, $f_m \neq 0$ et $g_n \neq 0$, on a $|m| \leqslant \deg(f)$ et $|n| \leqslant \deg(g)$. Par suite, si $|p| > \deg(f) + \deg(g)$, on a ou bien $|m| > \deg(f)$, ou bien $|n| > \deg(g)$ et $f_m g_n = 0$. Cela prouve que $\deg(fg) \leqslant \deg(f) + \deg(g)$.

c) Commençons par supposer que l'ensemble S est réduit à un seul élément et notons T l'indéterminée. Si m et n sont des entiers $\geqslant 0$ tels que $m+n = \deg(f) + \deg(g)$, alors $f_m = 0$ ou $g_n = 0$ à moins que l'on ait $m = \deg(f)$ et $n = \deg(g)$; par suite, le coefficient de $T^{\deg(f)+\deg(g)}$ dans fg est égal à $f_{\deg(f)} g_{\deg(g)}$; comme A est intègre, il n'est pas nul, ce qui prouve que $\deg(fg) = \deg(f) + \deg(g)$ dans ce cas.

Pour démontrer le reste de l'assertion, on suppose d'abord que S est un ensemble fini $\{1, \dots, d\}$. Alors, l'isomorphisme $A[T_1, \dots, T_{d-1}][T_d] \simeq A[T_1, \dots, T_d]$ entraîne, par récurrence sur d, que $A[T_1, \dots, T_d]$ est intègre. Posons $m = \deg(f)$ et écrivons $f = \sum_{i=0}^{m} f_i$, où f_i est le polynôme homogène de degré i défini par la somme des monômes de degré i apparaissant dans f. Posons de même $n = \deg(g)$ et écrivons $g = \sum_{j=0}^{n} g_j$, où g_j est la somme des monômes de degré j apparaissant dans j. On a $f_m \neq 0$ et $g_n \neq 0$; puisque l'anneau $A[T_1, \dots, T_d]$ est intègre, on a donc $f_m g_n \neq 0$ et $f_m g_n$ est un polynôme

d'exactement un élément de R. On a donc

$$\mathrm{Card}(X) = \sum_{A\in R} \mathrm{Card}(G\cdot R) = \sum_{A\in R} (G : G_A).$$

Posons $n = \mathrm{Card}(X)$; soit aussi b la plus grande puissance de p qui divise n, de sorte que $a \leqslant b$; posons enfin $m = n/p^b$. Le cardinal de X est égal à $\binom{n}{p^a}$, donc

$$\mathrm{Card}(X) = \prod_{i=0}^{p^a-1} \frac{n-i}{p^a-i}.$$

Pour $i \geqslant 1$, notons aussi a_i l'exposant de p dans la décomposition en facteurs premiers de i et $m_i = i/p^{a_i}$. Pour tout entier i tel que $1 \leqslant i < p^a$, on a $a_i < a$, de sorte que $n - i = p^b m - p^{a_i} m_i = p^{a_i}(p^{b-a_i} m - m_i)$, si bien que la puissance de p qui apparaît au numérateur est égale à $b + \sum_{i=1}^{p^a-1} a_i$. De même, pour tout entier i tel que $1 \leqslant i < p^a$, on a $p^a - i = p^{a_i}(p^{a-a_i} - 1)$, de sorte que la puissance de p qui apparaît au dénominateur est égale à $a + \sum_{i=1}^{p^a-1} a_i$. Cela démontre que le cardinal de X est multiple de p^{b-a} mais pas de p^{b+1-a}.

Il existe donc un élément $A \in R$ tel que $(G : G_A)$ ne soit pas multiple de p^{b+1-a}. Comme $(G : G_A) = n/\mathrm{Card}(G_A)$, cela entraîne que $\mathrm{Card}(G_A)$ est multiple de p^a. Puisque $\mathrm{Card}(G_A) \leqslant p^a$, on a donc $\mathrm{Card}(G_A) = p^a$, ce qu'il fallait démontrer. □

Lemme **(2.11.5)**. — *Soit* X *un ensemble fini, soit* p *un nombre premier et soit* P *un* p*-groupe fini opérant dans* X*; soit* X^P *l'ensemble des points fixes. On a* $\mathrm{Card}(X) \equiv \mathrm{Card}(X^P) \pmod p$.

Démonstration. — L'orbite d'un élément de X^P est réduite à cet élément. Inversement, soit $x \in X - X^P$; le cardinal de l'orbite de x divise celui de G donc est une puissance de p; si ce cardinal n'est pas égal à 1, c'est un multiple de p. Soit enfin R une partie de X telle que toute orbite contienne un élément de R et un seul; on a

$$\mathrm{Card}(X) = \sum_{x\in R} \mathrm{Card}(P\cdot x) = \sum_{x\in X^P} 1 + \sum_{x\in R - X^P} \mathrm{Card}(P\cdot x) \equiv \mathrm{Card}(X^P) \pmod p,$$

comme il fallait démontrer. □

Proposition **(2.11.6)**. — *Soit* G *un groupe fini, soit* p *un nombre premier, soit* S *un* p*-sous-groupe de Sylow de* G*. Pour tout sous-groupe* P *de* G *qui est un* p*-groupe, il existe un élément* $g \in G$ *tel que* $P \subset gSg^{-1}$.

Démonstration. — Soit $X = G/S$ l'ensemble des classes à droite de G modulo S ; faisons agir P sur X par translations à gauche. On a $\mathrm{Card}(X) \equiv \mathrm{Card}(X^P) \pmod{p}$. Par définition d'un p-sous-groupe de Sylow, $\mathrm{Card}(X) = (G : S)$ n'est pas multiple de p ; par suite, $\mathrm{Card}(X^P)$ n'est pas multiple de p et est en particulier *non vide* ! Soit $x \in X^P$ et soit $g \in G$ tel que $x = gS$. Pour tout $h \in P$, on a $hgS = h \cdot x = x = gS$; en particulier, $hg \in gS$, c'est-à-dire $h \in gSg^{-1}$. On a donc démontré que $P \subset gSg^{-1}$. □

Remarque **(2.11.7)**. — Soit G un groupe et soit A, B des sous-groupes de G ; soit $g \in G$. Le raisonnement fait dans la preuve précédente se généralise ainsi : Pour que A soit contenu dans le sous-groupe gBg^{-1} de G, conjugué de B, il faut et il suffit que gB soit fixé par tout élément de A opérant dans G/B par translations à gauche.

Corollaire **(2.11.8)**. — *Soit* G *un groupe fini et soit* p *un nombre premier. Deux* p*-sous-groupes de Sylow de* G *sont conjugués.*

Démonstration. — Soit P, S des p-sous-groupes de Sylow de G. D'après la proposition 2.11.6, il existe $g \in G$ tel que $P \subset gSg^{-1}$; comme $\mathrm{Card}(P) = \mathrm{Card}(S) = \mathrm{Card}(gSg^{-1})$, on a donc $P = gSg^{-1} = g \cdot S$. □

Théorème **(2.11.9)**. — *Soit* G *un groupe fini et soit* p *un nombre premier ; notons* a *la plus grande puissance de* p *qui divise* $\mathrm{Card}(G)$ *et posons* $m = \mathrm{Card}(G)/p^a$. *Le cardinal de l'ensemble des* p*-sous-groupes de Sylow de* G *divise* m *et est congru à* 1 *modulo* p.

Démonstration. — Soit Σ l'ensemble des p-sous-groupes de Sylow de G, c'est-à-dire des sous-groupes de G de cardinal p^a. Il découle de la proposition 2.11.4 que Σ n'est pas vide. Pour tout $S \in \Sigma$ et tout $g \in G$, gSg^{-1} est l'image de S par l'automorphisme intérieur $\mathrm{Int}(g)$, donc est un p-sous-groupe de Sylow de G. Cette formule munit ainsi Σ d'une opération de G. D'après le corollaire 2.11.8, les p-sous-groupes de Sylow de G sont conjugués. Ainsi, l'opération de G sur Σ est transitive.

Soit $S \in \Sigma$ un p-sous-groupe de Sylow de G. Le fixateur de S pour cette action est l'ensemble des $g \in G$ tels que $gSg^{-1} = S$; c'est le normalisateur $N_G(S)$ de S dans G. On a donc $\mathrm{Card}(\Sigma) = (G : N_G(S)) = \mathrm{Card}(G)/\mathrm{Card}(N_G(S))$. Comme $N_G(S)$ est un sous-groupe de G qui contient S, $(G : N_G(S))$ divise $(G : S)$; ainsi, $\mathrm{Card}(\Sigma)$ divise m.

c'est donc l'identité. Par suite, $f \circ g$ est un homomorphisme de $A[X]$-algèbres ; comme il vérifie $f \circ g(Y_s) = f(T_s) = Y_s$ pour tout $s \in S''$, c'est l'identité.

Inversement, $g \circ f$ est un homomorphisme de A-algèbres de $A[T]$ dans elle-même ; pour tout $s \in S$, on a $g \circ f(T_s) = g(X_s) = T_s$ si $s \in S'$, et $g \circ f(T_s) = g(Y_s) = T_s$ si $s \in S''$, si bien que $g \circ f$ est l'identité.

Cela démontre que f est un isomorphisme. □

3.8.6. — Soit A un anneau commutatif, soit B une A-algèbre commutative et soit $b \in B^n$. Il existe un unique morphisme de A-algèbres ev_a de $A[T_1, \dots, T_n]$ dans B qui applique T_i sur b_i pour tout $i \in \{1, \dots, n\}$. On l'appelle morphisme d'évaluation en a. Pour tout $m \in \mathbf{N}^m$, on a $\mathrm{ev}_b(T^m) = \mathrm{ev}_b(T_1)^{m_1} \dots \mathrm{ev}_b(T_n)^{m_n} = b_1^{m_1} \dots b_n^{m_n} = b^m$. Plus généralement, pour tout $f \in A[T_1, \dots, T_n]$, de coefficients (f_m), on a

$$\mathrm{ev}_b(f) = \mathrm{ev}_b\Big(\sum_m f_m T^m\Big) = \sum_m f_m b^m.$$

On note aussi $f(b)$ cet élément.

Exemple **(3.8.7)**. — a) Soit $f \in A[T]$ et soit $a \in A$. Pour que $f(a) = 0$, il faut et il suffit que $T - a$ divise f.

En effet, écrivons $f = (T - a)q + r$ la division euclidienne de f par $T - a$. Pour que $T - a$ divise f, il faut et il suffit que $r = 0$. Le polynôme r est de degré < 1, donc constant, de valeur $r(a)$. D'autre part, on a $f(a) = (0 - a)q(a) + r(a) = r(a)$.

b) Soit K un corps commutatif et soit V un K-espace vectoriel ; soit $u \in \mathrm{End}_K(V)$. Il existe ainsi un unique homomorphisme de la K-algèbre $K[T]$ dans $\mathrm{End}_K(V)$ qui applique T sur u. C'est le début de la théorie des polynômes d'endomorphismes.

3.8.7.1. *Degré.* — Soit A un anneau commutatif et soit S un ensemble ; pour tout $m \in \mathbf{N}^{(S)}$, notons $|m| = \sum m_s$. Pour $f = \sum f_m T^m \in A[(T_s)_{s \in S}]$, on pose alors

$$\deg(f) = \sup_{\substack{m \in M \\ f_m \neq 0}} |m|.$$

Cette borne supérieure est prise dans $\mathbf{Z}$; on a donc $\deg(0) = \infty$.

On dit qu'un monôme $f_m T^m$ apparaissant dans f est de degré $|m|$, de sorte que $\deg(f)$ est la borne supérieure des degrés des monômes apparaissant dans f. La somme $f' = \sum_{|m| = \deg(f)} f_m T^m$ des monômes de degré maximal (égal à $\deg(f)$) est le terme dominant de f. Si tous les monômes apparaissant dans f ont même degré, on dit que f est *homogène*.

deux à deux, il existe un unique morphisme de A*-algèbres* $\varphi : A[(T_s)]_{s\in S}$ *tel que* $\varphi(T_s) = b_s$ *pour tout* $s \in S$.

Démonstration. — Si φ est un morphisme vérifiant les propriétés demandées, on a

$$\varphi(T^m) = \varphi\Big(\prod_{s\in S} T_s^{m_s}\Big) = \prod_{s\in S} \varphi(T_s)^{m_s} = \prod_{s\in S} b_s^{m_s}.$$

Par suite, pour tout polynôme P, de coefficients $(c_m)_{m\in\mathbf{N}^{(S)}}$, on a $P = \sum_{m\in\mathbf{N}^{(S)}} c_m T^m$, donc

$$\varphi(P) = \varphi\Big(\sum_{m\in\mathbf{N}^{(S)}} c_m T^m\Big) = \sum_{m\in\mathbf{N}^{(S)}} c_m \varphi(T^m) = \sum_{m\in\mathbf{N}^{(S)}} c_m \prod_{s\in S} b_s^{m_s}.$$

Cela prouve qu'il existe au plus un tel morphisme d'algèbres.

Inversement, comme les b_s commutent deux à deux, l'application $m \mapsto \prod_{s\in S} b_s^{m_s}$ est un morphisme de M dans le monoïde multiplicatif de B, qui, pour tout $s \in S$, applique ε_s sur b_s. D'après la propriété universelle de l'algèbre du monoïde M, il existe un morphisme de A-algèbres de $A^{(M)}$ dans B, notons-le φ, tel que $\varphi(T^m) = \prod_{s\in S} b_s^{m_s}$ pour tout $m = (m_s) \in \mathbf{N}^{(S)}$. En particulier, le morphisme φ applique $T_s = T^{\varepsilon_s}$ sur b_s. □

Corollaire **(3.8.5)**. — *Soit* A *un anneau commutatif, soit* S *un ensemble, soit* S′ *une partie de* S *et soit* S″ = S − S′ *son complémentaire. Il existe un unique homomorphisme de* A*-algèbres de* $A[(T_s)_{s\in S}]$ *sur* $A[(X_s)_{s\in S'}][(Y_s)_{s\in S''}]$ *qui applique* T_s *sur* X_s *si* $s \in S'$ *et sur* Y_s *si* $s \in S''$. *C'est un isomorphisme.*

On a en particulier un isomorphisme

$$A[T_1, \dots, T_n] \simeq A[T_1, \dots, T_{n-1}][T_n].$$

Démonstration. — Pour abréger les notations, on abrège $(T_s)_{s\in S}$, $(X_s)_{s\in S'}$ et $(Y_s)_{s\in S''}$ en T, X et Y. L'existence et l'unicité d'un tel homomorphisme de A[T] dans A[X][Y] résulte de la propriété universelle ; notons-le f. Soit $g_1 : A[X] \to A[T]$ l'unique homomorphisme de A-algèbres qui applique X_s sur T_s, pour tout $s \in S'$. Il permet de considérer l'anneau A[T] comme une A[X]-algèbre. Il existe alors un unique homomorphisme de A[X]-algèbres, $g : A[X][Y] \to A[T]$, qui applique Y_s sur T_s, pour tout $s \in S''$.

Alors, $f \circ g$ est un homomorphisme de A-algèbres tel que $f \circ g(X_s) = f(T_s) = X_s$ pour tout $s \in S'$. En particulier, la restriction de $f \circ g$ à la sous-algèbre A[X] est un homomorphisme de A-algèbres qui applique X_s sur X_s, pour tout $s \in S'$;

Restreignons au sous-groupe S l'opération de G dans Σ. Comme S est un p-groupe, on a $\mathrm{Card}(\Sigma) \equiv \mathrm{Card}(\Sigma^S) \pmod p$, où Σ^S est l'ensemble des p-sous-groupes de Sylow P qui sont fixés par S, c'est-à-dire tels que $S \subset N_G(P)$. Dans ce cas, P et S sont deux p-sous-groupes de Sylow de $N_G(P)$; il existe donc $g \in N_G(P)$ tel que $S = gPg^{-1}$, d'où S = P ! Cela prouve que $\Sigma^S = \{S\}$ et $\mathrm{Card}(\Sigma) \equiv 1 \pmod p$. □

2.12. Exercices

Exercice **(2.12.1)**. — Soit A un groupe commutatif et soit a un élément de A d'ordre fini n. Pour tout entier m, démontrer que a^m est d'ordre fini et calculer son ordre.

Exercice **(2.12.2)**. — Soit A un groupe fini opérant dans un ensemble fini X. Pour tout $a \in A$, on pose $X^a = \{x \in X ; a \cdot x = x\}$ (ensemble des points fixes de a).

a) En comptant de deux façons l'ensemble des couples $(a, x) \in A \times X$ tels que $a \cdot x = x$, démontrer que l'on a

$$\sum_{a\in A} \mathrm{Card}(X^a) = \sum_{x\in X} \mathrm{Card}(A_x).$$

b) En déduire la « formule de Burnside »[6] :

$$\mathrm{Card}(X/A) = \frac{1}{\mathrm{Card}(A)} \sum_{a\in A} \mathrm{Card}(X^a).$$

c) Soit n et q deux entiers. On s'intéresse à des colliers de n perles pour lesquelles on dispose de q modèles. Combien y a-t-il de colliers possibles lorsqu'on identifie deux colliers qui se déduisent l'un de l'autre par une rotation ?

d) On suppose que A opère transitivement dans X. Démontrer qu'il existe un élément $a \in A$ tel que $a \cdot x \neq x$ pour tout x.[7]

Exercice **(2.12.3)**. — Soit A un groupe.

a) On suppose que $A/Z(A)$ est monogène ; démontrer que A est commutatif.

[6] Attribuée à Frobenius (1887) par Burnside (1897), cette formule était déjà connue de Cauchy (1845).
[7] C'est un théorème de C. Jordan (1872).

b) On suppose dans la suite que A est fini. Soit n son cardinal et c le nombre de classes de conjugaisons de A. Soit p la probabilité que deux éléments de A commutent (cardinal de l'ensemble des couples (a, b) tels que $ab = ba$, divisé par n^2). Démontrer que $p = c/n$.

c) On suppose que A n'est pas commutatif; démontrer que $p \leqslant 5/8$.

Exercice **(2.12.4)**. — Soit p un nombre premier et soit A un groupe fini, non réduit à $\{e\}$, dont le cardinal est une puissance de p.

a) Démontrer que le centre de A n'est pas trivial.

b) Soit K un corps fini de caractéristique p, soit V un K-espace vectoriel de dimension finie et soit ρ une représentation linéaire de A dans V, c'est-à-dire un homomorphisme de groupes de A dans $\mathrm{GL}(\mathrm{V})$. Démontrer qu'il existe un vecteur non nul $v \in \mathrm{V}$ tel que $\rho(a) \cdot v = v$ pour tout $a \in \mathrm{A}$.

c) (*suite*) Démontrer qu'il existe une base de V telle que pour tout $a \in \mathrm{A}$, la matrice de $\rho(a)$ dans cette base soit triangulaire supérieure, à diagonale formée de 1.

Exercice **(2.12.5)**. — On reprend les notations de l'exemple 2.3.7. Pour chacun des trois ensembles générateurs, trouver un entier N, si possible minimal, tel que tout élément soit un produit d'au plus N éléments parmi les générateurs donnés et leurs inverses. Quels éléments de $\mathfrak{S}_n$ atteignent cette borne?

Exercice **(2.12.6)**. — Soit a et b des élements de $\{1, \dots, n\}$; pour que le n-cycle $(1 \ \dots \ n)$ et la transposition $(a \ b)$ engendrent $\mathfrak{S}_n$, il faut et il suffit que $\mathrm{pgcd}(n, b - a) = 1$.

Exercice **(2.12.7)**. — Si un ensemble S de transpositions engendre $\mathfrak{S}_n$, on a $\mathrm{Card}(\mathrm{S}) \geqslant n - 1$.

Exercice **(2.12.8)**. — Soit A un groupe et soit B un sous-groupe. Démontrer que B est un sous-groupe distingué de A si et seulement toute classe à droite modulo B est une classe à gauche modulo B.

Exercice **(2.12.9)**. — Soit A un groupe. On appelle sous-groupe maximal de A un sous-groupe B tel que $\mathrm{B} \neq \mathrm{A}$ et tel que pour tout sous-groupe C tel que $\mathrm{B} \subset \mathrm{C} \subset \mathrm{A}$, on ait $\mathrm{C} = \mathrm{B}$ ou $\mathrm{C} = \mathrm{A}$.

L'algèbre $\mathrm{A}^{(\mathrm{M})}$ du monoïde M sur A est donc une A-algèbre associative. Son élément unité est la fonction δ_0 qui applique 0 sur 1 et tout élément non nul de M sur 0. Comme M est commutatif, l'anneau $\mathrm{A}^{(\mathrm{M})}$ est commutatif.

Pour $s \in \mathrm{S}$, notons ε_s l'élément de $\mathbf{N}^{(\mathrm{S})}$ dont le terme d'indice s est égal à 1 et dont tous les autres termes sont nuls. Noton T_s l'élément δ_{ε_s} de $\mathrm{A}^{(\mathrm{M})}$; on dit que c'est l'*indéterminée* d'indice s. Soit $m = (m_s)_{s\in\mathrm{S}}$ un élément de $\mathbf{N}^{(\mathrm{S})}$; on a $m = \sum_{s\in\mathrm{S}} m_s \varepsilon_s$ (ce peut être une somme infinie, mais seulement un nombre fini de termes en sont non nuls) de sorte que $\delta_m = \prod_{s\in\mathrm{S}} \mathrm{T}_s^{m_s}$ (ce peut être un produit infini, mais seulement un nombre fini de facteurs en sont différent de 1). Pour $m = (m_s) \in \mathbf{N}^{(\mathrm{S})}$, notons T^m l'élément δ_m, de sorte que $\mathrm{T}^m = \prod_{s\in\mathrm{S}} \mathrm{T}_s^{m_s}$. Ainsi, la fonction $f \in \mathrm{A}^{(\mathrm{M})}$ s'écrit-elle

$$f = \sum_{m\in\mathrm{M}} f(m)\delta_m = \sum_{m\in\mathrm{M}} f(m)\mathrm{T}^m.$$

On dit que $f(m)\mathrm{T}^m$ est le *monôme* de degré m de f et que $f(m)$ est son *coefficient de degré m*. En pratique, on note plutôt les coefficients en indice, c'est-à-dire qu'on écrit

$$f = \sum_{m\in\mathrm{M}} f_m \mathrm{T}^m.$$

Définition **(3.8.2)**. — *La* A*-algèbre* $\mathrm{A}^{(\mathrm{M})}$ *est appelé* algèbre des polynômes *à coefficients dans* A *et d'indéterminées* $(\mathrm{T}_s)_{s\in\mathrm{S}}$*; on la note* $\mathrm{A}[(\mathrm{T}_s)_{s\in\mathrm{S}}]$.

3.8.3. — Le cas le plus important pour les applications est celui d'un ensemble S fini; soit n son cardinal — le cas où $n = 1$ sera d'ailleurs primordial. Le monoïde $\mathrm{M} = \mathbf{N}^n$ est l'ensemble des suites $(m_1, \dots, m_n)$ de n entiers naturels, muni de l'addition; les indéterminées sont notées $\mathrm{T}_1, \dots, \mathrm{T}_n$ et l'anneau est noté $\mathrm{A}[\mathrm{T}_1, \dots, \mathrm{T}_n]$. Lorsque cas où n est petit, on note parfois les indéterminées de lettres distinctes : T, X, Y, Z, ... — on parle ainsi de l'anneau des polynômes $\mathrm{A}[\mathrm{T}]$ en une indéterminée T, ou de l'anneau des polynômes $\mathrm{A}[\mathrm{X}]$ en une indéterminée X, ou de l'anneau $\mathrm{A}[\mathrm{X}, \mathrm{Y}]$ des polynômes en deux indéterminées X, Y, ou de l'anneau $\mathrm{A}[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$ des polynômes en trois indéterminées X, Y, Z.

Proposition **(3.8.4)** (Propriété universelle des algèbres de polynômes)

Soit A *un anneau commutatif, soit* S *un ensemble et soit* $\mathrm{A}[(\mathrm{T}_s)_{s\in\mathrm{S}}]$ *l'anneau des polynômes à coefficients dans* A *et à indéterminées dans* S*. Pour toute* A*-algèbre (commutative ou non) et toute famille* $(b_s)_{s\in\mathrm{S}}$ *d'éléments de* B *qui commutent*

b) *Pour que deux fractions a/s et b/t de* A *soient égales, il faut et il suffit que* $sb = ta$.

Démonstration. — Notons S l'ensemble des éléments simplifiables de A. Soit $a \in A$ tel que $j(a) = a/1 = 1$. Par définition de la relation d'équivalence sur $A \times S$ dont B est l'ensemble des classes, il existe $s \in S$ tel que $as = 0$. Par hypothèse, s est simplifiable, donc $a = 0$. Cela prouve que j est injectif.

De même, si $a/s = b/t$, il existe $u \in S$ tel que $(at - bs)u = 0$; par hypothèse, u est simplifiable, d'où $at = bs$. □

Proposition **(3.7.10)**. — *Sot* A *un anneau commutatif intègre, soit* K *l'anneau total des fractions de* A *et soit* $j : A \to K$ *l'homomorphisme canonique. Alors* K *est un corps commutatif et* j *est un homomorphisme injectif. De plus, pour tout corps* E *et tout homomorphisme injectif* f *de* A *dans* E*, il existe un unique homomorphisme* $\varphi : K \to E$ *tel que* $f = \varphi \circ j$.

En particulier, j induit un isomorphisme de A un sous-anneau $j(A)$ de K et K est le corps engendré par $j(A)$. En pratique, on identifie l'anneau A au sous-anneau $j(A)$ de K.

Démonstration. — Il résulte du lemme 3.7.9 que l'homomorphisme j est injectif. Démontrons que K est un corps commutatif. Comme A est intègre, on a $1_A \neq 0_A$ dans A, donc $1_K = j(1_A) \neq j(0_A) = 0_K$; cela démontre que $K \neq \{0\}$. Soit x un élément non nul de K ; soit $a \in A$ et $b \in A - \{0\}$ tels que $x = a/b$; alors $a \neq 0$ et la fraction b/a est l'inverse de x. Ainsi, K est un corps commutatif.

Démontrons enfin la propriété universelle. Soit $f : A \to E$ un homomorphisme injectif de A dans un corps commutatif E. Puisque f est injectif, tout élément de $A - \{0\}$ a pour image un élément non nul, donc inversible, de E. Il résulte de la propriété universelle des anneaux de fractions qu'il existe un unique homomorphisme de corps de K dans E tel que $f = \varphi \circ j$. □

3.8. Polynômes

3.8.1. — Soit A un anneau commutatif. Soit S un ensemble et prenons pour monoïde l'ensemble $M = \mathbf{N}^{(S)}$ des applications de S dans **N** à support fini, muni de l'addition ; il est commutatif.

a) Soit $\mathscr{B}$ un ensemble non vide de sous-groupes de A qui est totalement ordonné pour l'inclusion (c'est-à-dire que si B et B′ appartiennent à $\mathscr{B}$, alors $B \subset B'$ ou $B' \subset B$). Démontrer que la réunion des éléments de $\mathscr{B}$ est un sous-groupe de A.

b) On suppose que A possède une partie génératrice finie. Démontrer que tout sous-groupe de A distinct de A est contenu dans un sous-groupe maximal. (*Utiliser le théorème de Zorn.*)

c) Reprendre la question précédente en remplaçant « sous-groupe maximal » par « sous-groupe distingué maximal », *resp.* « sous-groupe caractéristique maximal ».

d) Démontrer que le groupe additif **Q** ne possède pas de sous-groupe maximal.

Exercice **(2.12.10)** (Frattini–Neumann). — Soit G un groupe. On dit qu'un élément $g \in G$ est non-générateur si pour toute partie S de G qui n'est pas génératrice, $S \cup \{g\}$ n'est pas génératrice. On note $\Phi(G)$ l'ensemble des éléments non-générateurs de G (*sous-groupe de Frattini*).

a) Démontrer que $\Phi(G)$ est un sous-groupe caractéristique de G.

b) Soit g un élément de G. Démontrer qu'il existe un sous-groupe A de G qui est maximal parmi l'ensemble des sous-groupes de G qui ne contiennent pas g. (*Utiliser le théorème de Zorn.*)

c) Démontrer que $\Phi(G)$ est l'intersection de l'ensemble des sous-groupes maximaux de G.[8]

Exercice **(2.12.11)** (Lemme de Zassenhaus). — Soit G un groupe, soit A, B des sous-groupes de G. Soit A′ un sous-groupe distingué de A et soit B′ un sous-groupe distingué de B.

a) Démontrer que $A' \cdot (A \cap B)$ est un sous-groupe de G et que $A' \cdot (A \cap B')$ en est un sous-groupe distingué.

b) Démontrer de même que $(A \cap B) \cdot B'$ est un sous-groupe de G dont $(A' \cap B) \cdot B'$ est un sous-groupe distingué.

c) Démontrer que $(A' \cap B) \cdot (A \cap B')$ est un sous-groupe distingué de $A \cap B$.

[8] Ce résultat est dû à G. Frattini (1885) lorsque G est fini, et à B. H. Neumann (1937) en général.

d) Démontrer que les trois groupes quotients

$$(A' \cdot (A \cap B)) / (A' \cdot (A \cap B')),$$
$$((A \cap B) \cdot B') / ((A' \cap B) \cdot B'),$$
$$(A \cap B) / ((A' \cap B) \cdot (A \cap B'))$$

sont isomorphes.

Exercice **(2.12.12)** (Jordan-Hölder). — Soit A un groupe. On dit qu'une suite $(A_0, \dots, A_n)$ de sous-groupes de A est une *suite de composition* si $A_0 = \{e\}$, $A_n = A$ et si A_{i-1} est un sous-groupe distingué de A_i pour tout $i \in \{1, \dots, n\}$; l'entier n est appelé sa *longueur*.

a) Soit $(A_0, \dots, A_n)$ une suite de composition de A. Démontrer que les propriétés suivantes sont équivalentes :

(i) Pour tout $i \in \{1, \dots, n\}$, le groupe quotient A_i/A_{i-1} est simple ;

(ii) Pour tout $i \in \{1, \dots, n\}$, A_{i-1} est un sous-groupe distingué maximal de A_i ;

(iii) Il n'existe pas de suite de composition $(B_0, \dots, B_m)$ de A et d'application $f : \{0, \dots, n\} \to \{0, \dots, m\}$ telle que $m > n$ et $A_i = B_{f(i)}$ pour tout i.

Si elles sont vérifiées, on dit que la suite $(A_0, \dots, A_n)$ est une *suite de Jordan-Hölder*.

b) On suppose que A est fini. Démontrer qu'il possède une suite de Jordan-Hölder.

c) Soit n un entier ; décrire toutes les suites de Jordan-Hölder du groupe $\mathbf{Z}/n\mathbf{Z}$.

d) Soit $(A_0, \dots, A_n)$ et $(B_0, \dots, B_m)$ des suites de Jordan-Hölder de A. On pose $f(0) = 0$; pour $i \in \{1, \dots, n\}$, soit $f(i)$ le plus petit entier j tel que $A_{i-1} \cdot (A_i \cap B_j) = A_i$. Démontrer que f est une bijection de $\{0, \dots, n\}$ sur $\{0, \dots, m\}$ (en particulier, $n = m$) et que pour tout $i \in \{1, \dots, n\}$, les groupes A_i/A_{i-1} et $B_{f(i)}/B_{f(i)-1}$ sont isomorphes.

Exercice **(2.12.13)**. — Soit Q le groupe quaternionique d'ordre 8.

a) Démontrer que tout sous-groupe de Q est distingué, bien que ce groupe ne soit pas commutatif.

b) Quels sont les sous-groupes caractéristiques de Q ?

Exercice **(2.12.14)**. — Identifier les groupes engendrés par générateurs et relations suivants : $\langle x \mid x^n \rangle$ (pour $n \in \mathbf{N}$) ; $\langle x, y \mid xyx^{-1}y^{-1} \rangle$; $\langle i, j \mid jiji^{-1}, ijij^{-1} \rangle$.

Vérifions que φ est un homomorphisme d'anneaux. On a $\varphi(0) = \varphi(j(0)) = f(0) = 0$ et $\varphi(1) = \varphi(j(1)) = f(1) = 1$. Soit alors $(a, s), (b, t) \in A \times S$. On a

$$\begin{aligned}\varphi\Big(\frac{a}{s} + \frac{b}{t}\Big) &= \varphi\Big(\frac{at + bs}{st}\Big) \\ &= f(at + bs)f(st)^{-1} = f(a)f(s)^{-1} + f(b)f(t)^{-1} \\ &= \varphi\Big(\frac{a}{s}\Big) + \varphi\Big(\frac{b}{t}\Big).\end{aligned}$$

De même,

$$\begin{aligned}\varphi\Big(\frac{a}{s} \cdot \frac{b}{t}\Big) &= \varphi\Big(\frac{ab}{st}\Big) \\ &= f(ab)f(st)^{-1} = f(a)f(s)^{-1} \cdot f(b)f(t)^{-1} \\ &= \varphi\Big(\frac{a}{s}\Big) \cdot \varphi\Big(\frac{b}{t}\Big).\end{aligned}$$

Cela prouve que φ est un homomorphisme d'anneaux et conclut la preuve de la proposition. □

Remarque **(3.7.7)**. — a) La définition de la relation d'équivalence semble compliquée ; néanmoins, la définition naïve qui postulerait $(a, s) \sim (b, t)$ si et seulement si $at = bs$ ne donne pas lieu à une relation d'équivalence en général. Voir l'exercice 3.13.1.

b) À aucun moment de la discussion n'est intervenue l'hypothèse que S ne contient pas 0 ; autrement dit, on peut définir l'anneau A_S dans ce cas. Cependant, dans l'anneau A_S, $0/1$ est inversible ; il existe donc $(a, s) \in A \times S$ tel que $(0/1) \cdot (a/s) = (1/1)$, ce qui entraîne $0 = 1$ dans A_S : l'anneau de fractions est alors nul.

Définition **(3.7.8)**. — *Soit* A *un anneau commutatif et soit* S *l'ensemble des éléments simplifiables de* A. *L'anneau des fractions de* A *à dénominateurs dans* S *est appelé* anneau total des fractions de A.

Dans le cas où A est intègre, l'ensemble des éléments simplifiables de A est égal à $A - \{0\}$ et l'anneau total des fractions de A est appelé *corps des fractions* de A ; d'après la prop. 3.7.10 ci-dessous, c'est en effet un corps.

Lemme **(3.7.9)**. — *Soit* A *un anneau commutatif, soit* B *l'anneau total des fractions de* A *et soit* $j : A \to B$ *l'homomorphisme canonique.*

a) *L'homomorphisme* j *est injectif ;*

Observons enfin que l'application f est un homomorphisme d'anneaux. On a d'abord $j(0) = 0/1$ et $j(1) = 1/1$, si bien que j respecte les deux éléments neutres. Enfin, pour $a, b \in A$, on a $j(a+b) = (a+b)/1 = (a/1) + (b/1) = j(a) + j(b)$ et $j(ab) = (ab)/1 = (a/1)(b/1) = j(a)j(b)$.

On dit que l'anneau A_S est l'anneau des fractions de A à dénominateurs dans S et que $j : A \to A_S$ est l'homomorphisme canonique.

Proposition **(3.7.6)** (Propriété universelle de l'anneau des fractions)

Soit A *un anneau commutatif, soit* S *une partie multiplicative de* A, *soit* A_S *l'anneau des fractions de* A *à dénominateurs dans* S *et soit* $j : A \to A_S$ *l'homomorphisme canonique.*

a) *Pour tout élément* $s \in S$, $j(s)$ *est inversible dans* A_S.

b) *Soit* B *un anneau et soit* $f : A \to B$ *un homomorphisme d'anneaux tel que* $f(s)$ *soit inversible, pour tout* $s \in S$. *Il existe alors un homomorphisme d'anneaux* $\varphi : A_S \to B$, *et un seul, tel que* $f = \varphi \circ j$.

Démonstration. — La première propriété découle de ce que, pour tout $s \in S$, on a $j(s) \cdot (1/s) = (s/1) \cdot (1/s) = s/s = 1$. Démontrons la seconde.

Soit d'abord $\varphi : A_S \to B$ un homomorphisme d'anneaux tel que $\varphi \circ j = f$. Soit $(a, s) \in A \times S$. On écrit $a/s = (a/1) \cdot (1/s) = j(a)j(s)^{-1}$ car $1/s$ est l'inverse de $s/1$ dans A_S. Par suite, on a

$$\varphi(a/s) = \varphi(j(a)j(s)^{-1}) = \varphi(j(a))\varphi(j(s))^{-1} = f(a)f(s)^{-1}.$$

Cela prouve qu'il existe au plus un morphisme d'anneaux φ de A_S dans B tel que $\varphi \circ j = f$.

Pour démontrer son existence, on commence par vérifier qu'il existe une application de A_S dans B qui applique a/s sur $f(a)f(s)^{-1}$ pour tout $(a, s) \in A \times S$. Soit ainsi (a, s) et $(b, t) \in A \times S$ tels que $a/s = b/t$; soit $u \in S$ tel que $atu = bsu$. On a donc $f(a)f(t)f(u) = f(b)f(s)f(u)$. Comme $f(s)$, $f(t)$ et $f(u)$ sont inversibles dans B, on a alors $f(a)f(s)^{-1} = f(b)f(t)^{-1}$. Il existe donc une unique application $\varphi : A_S \to B$ telle qe $\varphi(a/s) = f(a)f(s)^{-1}$ pour tout $(a, s) \in A \times S$. On a $\varphi \circ j(a) = \varphi(a/1) = f(a)$ pour tout $a \in A$, donc $f = \varphi \circ j$.

Exercice **(2.12.15)**. — Soit G le groupe défini par l'ensemble générateur $\{x_1, \dots, x_n\}$ et les relations x_i^2 (pour $1 \leqslant i \leqslant n$), $x_i x_j x_i^{-1} x_j^{-1}$ (pour $1 \leqslant i, j \leqslant n$ et $j - i \geqslant 2$), $(x_i x_{i+1})^3$.

a) Démontrer qu'il existe un unique homomorphisme de groupes φ de G dans $\mathfrak{S}_{n+1}$ qui applique x_i sur la transposition $(i\ i+1)$, pour tout $i \in \{1, \dots, n\}$. Démontrer que φ est surjectif.

b) Démontrer que l'on a $G/H = \{H, x_n H, x_{n-1}x_n H, \dots, x_1 \dots x_n H\}$.

c) En déduire que par récurrence sur n que $\mathrm{Card}(G) \leqslant (n+1)!$, puis que φ est un isomorphisme.

Exercice **(2.12.16)**. — Démontrer qu'un groupe libre est sans torsion.

Exercice **(2.12.17)**. — Soit n un entier. Démontrer que l'ensemble des homomorphismes du groupe libre F_n dans le groupe $\mathbf{Z}/2\mathbf{Z}$ est fini et calculer son cardinal. En déduire que si m et n sont des entiers distincts, les groupes F_m et F_n ne sont pas isomorphes.

Exercice **(2.12.18)**. — Soit G un groupe, soit N un sous-groupe distingué de G; on suppose que G/N est isomorphe à un groupe libre. Démontrer qu'il existe un sous-groupe F de G tel que $G = F \cdot N$ et $F \cap N = \{e\}$.

Exercice **(2.12.19)** (« Ping-pong », Felix Klein). — Soit G un groupe opérant dans un ensemble E et soit a, b des éléments de G. On suppose qu'il existe des parties A, B de E, non vides, telles que $A \not\subset B$, et telles que $a^n \cdot A \subset B$ et $b^n \cdot B \subset A$ pour tout entier $n \in \mathbf{Z}$ tel que $n \neq 0$. Soit $\varphi : F(a, b) \to G$ l'homomorphisme canonique du groupe libre sur $\{a, b\}$ dans G qui applique a et b sur a et b respectivement.

a) Soit $m \in M'(a, b)$ un mot réduit débutant et finissant par a ou a^{-1}. Démontrer que l'on a $\varphi(m) \cdot A \subset B$ et en déduire que $\varphi(m) \neq e$.

b) Démontrer que φ est injectif.

Exercice **(2.12.20)**. — On fait opérer $GL(2, \mathbf{C})$ sur $\mathbf{C}^2$ de façon usuelle. Soit A (*resp.* B) l'ensemble des couples $(x, y) \in \mathbf{C}^2$ tels que $|x| < |y|$ (*resp.* $|x| > |y|$). Soit u et v des nombres complexes tels que $|u| \geqslant 2$ et $|v| \geqslant 2$; on pose $a = \left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right)$ et $b = \left(\begin{smallmatrix} 1 & 0 \\ v & 1 \end{smallmatrix}\right)$.

a) Démontrer que $a \cdot A \subset B$ et $b \cdot B \subset A$.

b) Démontrer que l'unique homomorphisme de $F(a, b)$ dans $GL(2, \mathbf{C})$ qui applique a et b sur a et b respectivement est injectif.

Exercice **(2.12.21)** (Jeu de taquin[10]). — Le jeu de taquin, inventé dans les années 1870 et traditionnellement attribué à Sam Loyd, consiste en 15 pièces carrées placées à l'intérieur d'une boîte 4×4 ; il reste donc une case vide et chaque étape du jeu consiste à faire coulisser une des pièces vers la case vide. Le problème initial était, partant de l'agencement

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

de retrouver l'agencement initial

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

dans lesquels les cases 14 et 15 ont retrouvées leur place.

a) On considère un état du jeu comme une permutation d'un ensemble à 16 éléments, $\{1, 2, \dots, 15, \square\}$, où $\square$ représente la case vide. Démontrer que chaque étape du jeu consiste à multiplier la permutation précédente par une transposition. Évaluer la parité du nombre d'étapes effectuées en fonction de la position finale de la case vide. Que pensez-vous du problème posé par Sam Loyd ?

b) Pour analyser le jeu plus précisément, et notamment déterminer l'ensemble des configurations qui permettent de remettre le puzzle dans son état initial, on décide de numéroter les pièces comme suit :

[10] Cet exercice est issu de la présentation de Michel Coste, *http://agreg-maths.univ-rennes1.fr/documentation/docs/taquin.pdf*.

Cette loi est commutative (c'est évident). Elle est associative car si (a, s), (b, t), $(c, u) \in \mathrm{A} \times \mathrm{S}$, on a

$$\left(\frac{a}{s} + \frac{b}{t}\right) + \frac{c}{u} = \frac{at + bs}{st} + \frac{c}{u} = \frac{atu + bsu + cst}{stu} = \frac{a}{s} + \left(\frac{b}{t} + \frac{c}{u}\right).$$

En outre, $0/1$ est un élément neutre car

$$\frac{0}{1} + \frac{a}{s} = \frac{0s + 1a}{s1} = \frac{a}{s}$$

pour tout $(a, s) \in \mathrm{A} \times \mathrm{S}$. Notons aussi que $0/1 = 0/s$ pour tout $s \in \mathrm{S}$. Enfin, pour tout $(a, s) \in \mathrm{A} \times \mathrm{S}$, $(-a)/s$ est l'opposé de a/s puisque

$$\frac{-a}{s} + \frac{a}{s} = \frac{-a + a}{s} = \frac{0}{s} = \frac{0}{1}.$$

Ainsi, $(\mathrm{A_S}, +)$ est un groupe abélien.

Soit (a, s), (b, t), (a', s'), (b', t') des éléments de $\mathrm{A} \times \mathrm{S}$ tels que $a/s = a'/s'$ et $b/t = b'/t'$. Soit $u, v \in \mathrm{S}$ tels que $as'u = a'su$ et $bt'v = b'tv$. On a alors

$$abs't' \cdot uv = (as'u)(bt'v) = (a'su)(b'tv) = a'b'st \cdot uv,$$

ce qui prouve que $ab/st = a'b'/s't'$. Il existe donc une unique loi de composition sur $\mathrm{A_S}$, notée $\cdot$, telle que

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

pour tous $a, b \in \mathrm{A}$ et tous $s, t \in \mathrm{S}$.

Cette loi est commutative (c'est évident). Elle est associative car si (a, s), (b, t), $(c, u) \in \mathrm{A} \times \mathrm{S}$, on a

$$\left(\frac{a}{s} \cdot \frac{b}{t}\right) \cdot \frac{c}{u} = \frac{ab}{st} \cdot \frac{cu}{=} \frac{abc}{stu} = \frac{a}{s} \cdot \left(\frac{b}{t} \cdot \frac{c}{u}\right).$$

En outre, $1/1$ est un élément neutre pour cette loi car

$$\frac{1}{1} \cdot \frac{a}{s} = \frac{1a}{1s} = \frac{a}{s}$$

pour tout $(a, s) \in \mathrm{A} \times \mathrm{S}$. Cela prouve que $(\mathrm{A_S}, \cdot)$ est un monoïde commutatif.

Démontrons enfin que la multiplication de $\mathrm{A_S}$ est distributive par rapport à l'addition. En effet, si (a, s), (b, t), $(c, u) \in \mathrm{A} \times \mathrm{S}$, on a

$$\frac{a}{s} \cdot \left(bt + \frac{c}{u}\right) = \frac{a}{s} \cdot \frac{bu + ct}{tu} = \frac{a(bu + ct)}{stu} = \frac{abu}{stu} + \frac{act}{stu} = \frac{ab}{st} + \frac{ac}{su} = \frac{a}{s} \cdot \frac{b}{t} + \frac{a}{s} \cdot \frac{c}{u}.$$

Cela démontre que $(\mathrm{A_S}, +, \cdot)$ est un anneau.

a/s et b/t sont « égales » ; ensuite vérifier que les formules classiques donnent bien lieu à un anneau.

3.7.4. — On définit une relation dans l'ensemble $A \times S$ de la façon suivante : pour $(a,s),(b,t) \in A \times S$, on dit que $(a,s) \sim (b,t)$ s'il existe $u \in S$ tel que $a \cdot tu = b \cdot su$.

Démontrons que c'est une relation d'équivalence :

– Elle est réflexive : si $(a,s) \in A \times S$, la relation $as1 = as1$ prouve que $(a,s) \sim (a,s)$.

– Elle est symétrique : si $(a,s) \sim (b,t)$, soit $u \in S$ tel que $at \cdot u = bs \cdot u$; alors $bsu = atu$ ce qui prouve que $(b,t) \sim (a,s)$.

– Elle est transitive : supposons que $(a,s) \sim (b,t)$ et $(b,t) \sim (c,u)$ et soit $v, w \in S$ tels que $at \cdot v = bs \cdot v$ et $bu \cdot w = ct \cdot w$; alors,

$$au \cdot tvw = atv \cdot uw = bsv \cdot uw = buw \cdot sv = ctw \cdot sv = cs \cdot tvw,$$

si bien que $(a,s) \sim (c,u)$.

Notons A_S l'ensemble quotient de l'ensemble $A \times S$ pour cette relation d'équivalence. Notons aussi a/s la classe d'un couple $(a,s) \in A \times S$ et $j : A \to A_S$ l'application donnée par $j(a) = a/1$ pour $a \in A$.

On a $(at)/(st) = a/s$ pour tout $a \in A$ et tous $s, t \in S$.

3.7.5. — Démontrons que les formules usuelles pour le calcul des fractions permettent de définir une structure d'anneau sur A_S.

Soit (a,s), (b,t), (a',s'), (b',t') des éléments de $A \times S$ tels que $a/s = a'/s'$ et $b/t = b'/t'$. Soit $u, v \in S$ tels que $as'u = a'su$ et $bt'v = b'tv$. On a alors

$$(at+bs)s't'uv = as'u \cdot tt'v + bt'v \cdot ss'u = a'su \cdot tt'v + b'tv \cdot ss'u = (a't' + b's')stuv,$$

ce qui prouve que $(at+bs)/st = (a't'+b's')/s't'$. Il existe donc une unique loi de composition sur A_S, notée $+$, telle que

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$$

pour tous $a, b \in A$ et tous $s, t \in S$. Observons aussi que pour $a, b \in A$ et $s \in S$, on a

$$\frac{a}{s} + \frac{b}{s} = \frac{as+bs}{s^2} = \frac{(a+b)s}{s^2} = \frac{a+b}{s}.$$

4	3	2	1
5	6	7	8
12	11	10	9
13	14	15	16

Une état du puzzle est alors la suite des 15 numéros des cases, lorsqu'on les lit comme dans la configuration précédente, et en omettant la case vide.

Vérifier que la position de la case vide n'a pas d'importance.

c) On considère ces suites comme des permutations de l'ensemble à 15 éléments, $\{1, \dots, 15\}$. Démontrer qu'une étape du jeu consiste à multiplier la permutation précédente par un cycle de longueur impaire. En déduire que seules les permutations paires permettent de ranger le puzzle dans son état initial.

d) Soit i un entier tel que $1 \leqslant i \leqslant 13$. Trouver une suite d'étapes du jeu qui revient à multiplier une permutation à droite par le 3-cycle $(i\ i+1\ i+2)$.

e) Soit n un entier ; démontrer que les permutations de la forme $(i\ i+1\ i+2)$, pour $1 \leqslant i \leqslant n-2$, engendrent le groupe $\mathfrak{A}_n$.

f) Démontrer que les permutations qui permettent de ranger le puzzle dans son état initial sont exactement les permutations paires.

Exercice **(2.12.22)**. — Soit A un groupe et soit B un sous-groupe de A.

a) On pose $N = \bigcap_{a \in A} aBa^{-1}$; démontrer que N est un sous-groupe distingué de A.

b) On suppose que B est d'indice fini dans A. Démontrer que N est d'indice fini dans A.

c) On suppose que A est un groupe fini et que l'indice de B dans A est égal au plus petit facteur premier de $\mathrm{Card}(A)$ (par exemple, que $(A : B) = 2$). Démontrer que B est un sous-groupe distingué de A.

Exercice **(2.12.23)**. — Déterminer « tous » les groupes abéliens de cardinal $\leqslant 100$.

Exercice **(2.12.24)**. — *a*) Déduire du théorème de structure des groupes abéliens finis qu'un sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

b) Observer que le groupe quaternionique d'ordre 8 est un sous-groupe fini du corps **H** des quaternions mais n'est pas cyclique.

Exercice **(2.12.25)**. — Soit n un entier.

a) Soit $\sigma \in \mathfrak{S}_n$. Déterminer l'ordre de σ et sa signature en fonction de son type.

b) Quels sont les ordres des éléments de $\mathfrak{S}_5$?

c) Quel est le plus petit entier n tel que $\mathfrak{S}_n$ contienne un élément d'ordre 12 ? deux éléments d'ordre 12 qui ne soient pas conjugués l'un de l'autre ?

Exercice **(2.12.26)**. — Soit n un entier.

a) Soit $\pi = (m_1, \dots, m_r)$ une partition de n ; pour tout $i \geqslant 1$, soit p_i le nombre d'indices j tel que $m_j = i$. Vérifier que $\sum i p_i = n$.

b) Combien y a-t-il de permutations de type π ?

c) Soit $\sigma \in \mathfrak{S}_n$ une permutation de type π et soit Z_σ son centralisateur. Démontrer que $\mathrm{Card}(Z_\sigma) = \prod_{i=1}^n p_i! i^{p_i}$.

Exercice **(2.12.27)**. — *a*) Faire la liste des différentes classes de conjugaison du groupe $\mathfrak{A}_5$ et, pour chacune d'entre elles, calculer leur cardinal.

b) Démontrer que $\{e\}$ est la seule partie de $\mathfrak{A}_5$ vérifiant les propriétés suivantes : elle contient e, elle est une réunion de classes de conjugaisons, et son cardinal divise celui de $\mathfrak{A}_5$.

c) En déduire que le groupe $\mathfrak{A}_5$ est simple.

d) Soit $n \geqslant 6$ et soit N un sous-groupe distingué de $\mathfrak{A}_n$ tel que $N \neq \{e\}$. Soit g un élément de $N - \{1\}$; trouver un élément $h \in \mathfrak{A}_n$ tel que $[g, h] \neq e$ mais $[g, h]$ fixe un élément de $\{1, \dots, n\}$. En déduire par récurrence que $N = \mathfrak{A}_n$.

Exercice **(2.12.28)**. — Soit n un entier $\geqslant 5$.

a) Soit A un sous-groupe distingué de $\mathfrak{S}_n$. Démontrer que $A = \{e\}$, $A = \mathfrak{A}_n$ ou $A = \mathfrak{S}_n$.

b) Soit A un sous-groupe de $\mathfrak{S}_n$ et soit $a = (\mathfrak{S}_n : A)$. Déduire de l'action par translations à gauche de $\mathfrak{S}_n$ sur l'ensemble $\mathfrak{S}_n/A$ des classes à droite modulo A un homomorphisme de $\mathfrak{S}_n$ dans $\mathfrak{S}(\mathfrak{S}_n/A)$. En déduire l'alternative : soit $A = \mathfrak{A}_n$, soit $A = \mathfrak{S}_n$, soit $a \geqslant n$.

$q(u) = 1$; de même, $v = 1 - u \equiv 1 \pmod{I}$ et $p(v) = 1$. On a donc $f(u) = (0, 1)$, $f(v) = (1, 0)$. Soit $x \in A/I$ et soit $y \in A/J$; soit $a \in A$ tel que $p(a) = x$, soit $b \in A$ tel que $p(b) = y$. On a alors

$$f(av + bu) = (p(a), q(a))(1, 0) + (p(b), q(b))(0, 1) = (x, 0) + (0, y) = (x, y).$$

Cela prouve que l'homomorphisme f est surjectif. Par définition, un élément a de A appartient à $\mathrm{Ker}(f)$ si et seulement si $p(a) = 0$ et $q(a) = 0$, c'est-à-dire $a \in I \cap J$. Le théorème en résulte. □

Corollaire **(3.6.20)**. — *Soit* A *un anneau, soit* $(I_1, \dots, I_n)$ *une suite d'idéaux bilatères de* A*, deux à deux comaximaux. Pour tout* $i \in \{1, \dots, n\}$*, notons* $p_i : A \to A/A_i$ *la surjection canonique. L'homomorphisme* $p : A \to \prod_{i=1}^n (A/A_i)$ *donné par* $p(a) = (p_i(a))_{1 \leqslant i \leqslant n}$ *est alors surjectif, son noyau est égal à* $\bigcap_{i=1}^n I_i$*. Il induit donc, par passage au quotient, un isomorphisme de* $A/\bigcap_{i=1}^n I_i$ *sur* $\prod_{i=1}^n (A/I_i)$.

3.7. Anneaux de fractions

Dans tout ce paragraphe, on ne considère que des anneaux commutatifs.

Définition **(3.7.1)**. — *Soit* A *un anneau commutatif. On dit qu'une partie* S *de* A *est multiplicative si elle vérifie les deux propriétés suivantes :*

(i) *On a* $1 \in S$;
(ii) *Pour* $a, b \in S$*, on a* $ab \in S$.

Cela veut donc dire que c'est un sous-monoïde du monoïde multiplicatif de A.

Exemple **(3.7.2)**. — Soit A un anneau commutatif.

a) Pour tout $a \in A$, l'ensemble $S = \{1, a, a^2, \dots\}$ des puissances de a est une partie multiplicative.

b) L'ensemble des éléments simplifiables de A est une partie multiplicative.

c) Si P est un idéal premier de A, l'ensemble $S = A - P$ est une partie multiplicative.

3.7.3. — Soit A un anneau commutatif et soit S une partie multiplicative de A. Nous allons définir l'ensemble des « fractions à dénominateur dans S » et, via les formules classiques, le munir d'une structure d'anneau. Nous devons pour cela résoudre deux difficultés : d'abord élucider la condition à laquelle deux fractions

a) *L'application* $\mathrm{J} \mapsto p(\mathrm{J})$ *induit une bijection de l'ensemble des idéaux à gauche (*resp. *à droite,* resp. *bilatères) de* A *qui contiennent* J *sur l'ensemble des idéaux à gauche (*resp. *à droite,* resp. *bilatères) de* A/I. *Sa bijection réciproque est donnée par* $\mathrm{K} \mapsto p^{-1}(\mathrm{K})$.

b) *Soit* J *un idéal bilatère de* A *qui contient* I. *L'homomorphisme composé des surjections canoniques de* A *sur* A/I *et de* A/I *sur* $(\mathrm{A}/\mathrm{I})/p(\mathrm{J})$ *induit, par passage au quotient, un isomorphisme d'anneaux de* A/J *sur* $(\mathrm{A}/\mathrm{I})/p(\mathrm{J})$.

Démonstration. — a) On sait que l'application $\mathrm{J} \mapsto p(\mathrm{J})$ est une bijection de l'ensemble des sous-groupes de A contenant I sur l'ensemble des sous-groupes de A/I. Il suffit de vérifier que J est un idéal à gauche (*resp.* à droite, *resp.* bilatère) de A si $p(\mathrm{J})$ est un idéal à gauche (*resp.* à droite, *resp.* bilatère) de A/I.

Supposons donc que J soit un idéal à gauche de A. Soit $x \in \mathrm{A}/\mathrm{I}$ et soit $y \in p(\mathrm{J})$; soit $a \in \mathrm{A}$ tel que $x = p(a)$, soit $b \in \mathrm{J}$ tel que $y = p(b)$. On a $xy = p(a)p(b) = p(ab)$; comme J est un idéal à gauche, $ab \in \mathrm{J}$, ce qui prouve que $xy \in p(\mathrm{J})$. Cela démontre que $p(\mathrm{J})$ est un idéal à gauche de A/J.

Inversement, supposons que $p(\mathrm{J})$ soit un idéal à gauche de A/J. Soit $a \in \mathrm{A}$ et soit $x \in \mathrm{J}$. Alors, $p(ax) = p(a)p(x)$ appartient à $p(\mathrm{J})$ puisque $p(x) \in p(\mathrm{J})$. Par suite, il existe $y \in \mathrm{J}$ tel que $p(ax) = p(y)$, et donc $ax - y \in \mathrm{I}$. Comme $\mathrm{I} \subset \mathrm{J}$, on a donc $ax = y + (ax - y) \in \mathrm{J}$. Par suite, J est un idéal à gauche de A.

Le cas des idéaux à droite se traite de même, et celui des idéaux bilatères s'en déduit.

b) Soit q la surjection canonique de A/I sur $(\mathrm{A}/\mathrm{I})/p(\mathrm{J})$. L'homomorphisme d'anneaux $q \circ p : \mathrm{A} \to (\mathrm{A}/\mathrm{I})/p(\mathrm{J})$ est surjectif. On a $\mathrm{Ker}(q \circ p) = (q \circ p)^{-1}(0) = p^{-1}(q^{-1}(0)) = p^{-1}(p(\mathrm{J})) = \mathrm{J}$. Ainsi, $q \circ p$ définit, par passage au quotient, un homomorphisme bijectif d'anneaux de A/J sur $(\mathrm{A}/\mathrm{I})/p(\mathrm{J})$. C'est un isomorphisme. □

Théorème **(3.6.19)** (Théorème chinois). — *Soit* A *un anneau, soit* I, J *des idéaux bilatères de* A *tels que* $\mathrm{I} + \mathrm{J} = \mathrm{A}$. *Notons* $p : \mathrm{A} \to \mathrm{A}/\mathrm{I}$ *et* $q : \mathrm{A} \to \mathrm{A}/\mathrm{J}$ *les surjections canoniques. Alors l'homomorphisme* $(p, q) : \mathrm{A} \to (\mathrm{A}/\mathrm{I}) \times (\mathrm{A}/\mathrm{J})$ *est surjectif et son noyau est égal à* $\mathrm{I} \cap \mathrm{J}$. *Il induit donc, par passage au quotient, un isomorphisme de* $\mathrm{A}/(\mathrm{I} \cap \mathrm{J})$ *sur* $(\mathrm{A}/\mathrm{I}) \times (\mathrm{A}/\mathrm{J})$.

On dit que I et J sont *comaximaux* si $\mathrm{I} + \mathrm{J} = \mathrm{A}$.

Démonstration. — Notons f l'homomorphisme (p, q). Puisque $\mathrm{I} + \mathrm{J} = \mathrm{A}$, il existe $u \in \mathrm{I}$ et $v \in \mathrm{J}$ tels que $u + v = 1$. Par suite, $u = 1 - v \equiv 1 \pmod{\mathrm{J}}$, de sorte que

c) Soit A un sous-groupe de $\mathfrak{S}_n$ tel que $(\mathfrak{S}_n : \mathrm{A}) = n$. Démontrer que l'homomorphisme de la question précédente induit un isomorphisme de groupes de A sur le fixateur de la classe A dans $\mathfrak{S}(\mathfrak{S}_n/\mathrm{A})$. En particulier, A est isomorphe à $\mathfrak{S}_{n-1}$.

Exercice **(2.12.29)**. — Soit n un entier tel que $n \geqslant 7$.

a) Soit τ une transposition. Quel est l'ordre de $\varphi(\tau)$? Quel est le cardinal du centralisateur de $\varphi(\tau)$? En utilisant alors la formule de l'exercice 2.12.26, démontrer que $\varphi(\tau)$ est une transposition.

b) (*suite*) Pour $i \in \{2, \ldots, n\}$, soit τ_i la transposition $(1\ i)$. Démontrer qu'il existe une suite $(a_1, \ldots, a_n)$ d'entiers deux à deux distincts tels que $\varphi(\tau_i) = (a_1\ a_i)$. En déduire que φ est un automorphisme intérieur.

c) (*suite*) Conclure que l'homomorphisme canonique $\mathrm{Int} : \mathfrak{S}_n \to \mathrm{Aut}(\mathfrak{S}_n)$ est un isomorphisme.

Exercice **(2.12.30)**. — Soit A un groupe fini et soit p un nombre premier. Soit $\sigma : \mathrm{A}^p \to \mathrm{A}^p$ l'application donnée par $\sigma(a_1, \ldots, a_p) = (a_2, \ldots, a_p, a_1)$.

a) Quels sont les points fixes de σ ? Démontrer que les orbites de σ ont pour cardinal 1 ou p.

b) On note X l'ensemble des $(a_1, \ldots, a_p) \in \mathrm{A}^p$ tels que $a_1 \ldots a_p = e$. Démontrer que σ induit par restriction une permutation de X.

c) Calculer $\mathrm{Card}(\mathrm{X})$. Si p divise $\mathrm{Card}(\mathrm{A})$, déduire des questions précédentes qu'il existe un élément $a \in \mathrm{A} - \{e\}$ tel que $a^p = e$.

d) Démontrer que pour tout élément $a \in \mathbf{N}$ qui n'est pas multiple de p, $a^{p-1} - 1$ est multiple de p.

Exercice **(2.12.31)**. — Soit p un nombre premier et soit n un entier naturel.

a) On suppose que que $n < 2p$; déterminer les p-sous-groupes de Sylow de $\mathfrak{S}_n$.

b) On suppose que p est impair et que $2p \leqslant n < p^2$. Décrire un p-sous-groupe de Sylow de $\mathfrak{S}_n$. Démontrer en particulier qu'ils sont commutatifs.

c) Décrire un p-sous-groupe de Sylow de $\mathfrak{S}_{p^2}$; observer qu'il n'est pas commutatif.

Exercice **(2.12.32)**. — Soit G un groupe fini de cardinal 60. Si p est un nombre premier, on note σ_p le nombre de p-sous-groupes de Sylow de G. On suppose

dans la suite que $\sigma_5 \neq 1$; le but de l'exercice est de prouver que G est simple. On raisonne par l'absurde en considérant un sous-groupe distingué H de G, distinct de $\{e\}$ et de G.

a) Quel peut être le cardinal de H ?

b) Démontrer que $\sigma_2 \in \{1,3,5,15\}$, $\sigma_3 \in \{1,4,10\}$ et $\sigma_5 = 6$. Combien G contient-il d'éléments d'ordre 5 ?

c) On suppose que $\mathrm{Card}(H)$ est multiple de 5. Démontrer que $\mathrm{Card}(H) = 30$. Observer que H possède 20 éléments d'ordre 3 et en déduire que H possède un unique 5-sous-groupe de Sylow. Pourquoi cette assertion est-elle absurde ?

d) On suppose que $\mathrm{Card}(H) \leqslant 4$. Prouver que G/H possède un unique sous-groupe d'ordre 5. En déduire que G possède un sous-groupe distingué H′, distinct de G mais dont le cardinal est multiple de 5. En déduire une contradiction.

e) On suppose que $\mathrm{Card}(H) = 6$ ou 12. Si H possède un unique 3-sous-groupe de Sylow, démontrer que c'est un sous-groupe distingué de G et en déduire une contradiction. Sinon, démontrer que H possède un unique 2-sous-groupe de Sylow et en déduire encore une contradiction.

Exercice **(2.12.33)**. — Soit G un groupe simple de cardinal 60.

a) Soit A un sous-groupe de G. Démontrer que $(G : A) \geqslant 5$. (Faire opérer G dans G/A.) Si $(G : A) = 5$, démontrer que G est isomorphe à $\mathfrak{A}_5$.

b) Si p est un nombre premier, on note σ_p le nombre de p-sous-groupes de Sylow de G. Démontrer que $\sigma_2 \in \{5,15\}$, $\sigma_3 = 10$ et $\sigma_5 = 6$.

c) Si $\sigma_2 = 5$, démontrer que G est isomorphe à $\mathfrak{A}_5$. (Faire opérer G dans l'ensemble de ses 5-sous-groupes de Sylow.)

d) On suppose que $\sigma_2 = 15$. Démontrer que G possède 24 éléments d'ordre 5. En déduire qu'il existe deux sous-groupes de 2-Sylow de G, P et Q, tels que $\mathrm{Card}(P \cap Q) = 2$. Soit $N = N_G(P \cap Q)$. Prouver que $(G : N) = 5$ puis que G est isomorphe à $\mathfrak{A}_5$, ce qui contredit l'hypothèse $\sigma_2 = 15$.

Exercice **(2.12.34)** (Argument de Frattini). — *a*) Soit A un groupe opérant dans un ensemble X. Soit B un sous-groupe de A tel que l'opération de B dans X déduite de celle de A soit transitive. Démontrer que pour tout $x \in X$, on a $A = B \cdot A_x$.

b) Soit A un groupe, soit G un sous-groupe fini de A et soit S un p-sous-groupe de Sylow de G. Démontrer que $A = G \cdot N_A(S)$.

(iv) *Il existe un anneau* B *et un homomorphisme de groupes surjectif* $f : A \to B$ *de noyau* I.

Démonstration. — (i)⇒(ii). Comme I est un sous-groupe du groupe abélien $(A, +)$, la relation définie est compatible avec l'addition de A. Soit en outre $a, b, a', b' \in A$ tels que $a \sim a'$ et $b \sim b'$; démontrons que $ab \sim a'b'$. En effet, par définition de la relation $\sim$, $a' - a \in I$ et $b' - b$; comme I est un idéal bilatère, $a'(b' - b) \in I$ et $(a' - a)b \in I$; comme c'est un sous-groupe du groupe additif de A, la relation $a'b' - ab = a'(b' - b) + (a' - a)b$ prouve que $ab \sim a'b'$.

L'implication (ii)⇒(iii) est évidente.

(iii)⇒(iv). Soit B l'anneau quotient de A par la relation d'équivalence $\sim$ et soit $c : A \to B$ l'homomorphisme canonique ; il est surjectif et son noyau est égal à I.

Enfin, l'implication (iv)⇒(i) résulte de ce que le noyau d'un homomorphisme d'anneaux est un idéal bilatère. □

3.6.16. — Soit A un anneau et soit I un idéal bilatère de A. L'anneau quotient de A par la relation d'équivalence associée à l'idéal bilatère I est noté A/I ; on dit que c'est le quotient de A par I.

Proposition **(3.6.17)** (Propriété universelle de l'anneau quotient)

Soit A *un anneau, soit* I *un idéal bilatère de* A *et soit* $p : A \to A/I$ *la surjection canonique. Soit* B *un anneau et soit* $f : A \to B$ *un homomorphisme d'anneaux tel que* $f(I) = \{0\}$. *Il existe un unique homomorphisme d'anneaux* $\tilde{f} : A/I \to B$ *tel que* $f = \tilde{f} \circ p$.

De plus, $\tilde{f}$ *est injectif si et seulement si* $\mathrm{Ker}(f) = I$.

Démonstration. — Notons $\sim$ la relation d'équivalence dans A associée à l'idéal bilatère I. Soit a et b des éléments de A tels que $a \sim b$; on a $f(b) - f(a) = f(b-a) = 0$ puisque $b - a \in I$, donc $f(b) = f(a)$. D'après la propriété universelle du groupe quotient, il existe un morphisme de groupes additifs $\tilde{f} : A/I \to B$, et un seul, tel que $f = \tilde{f} \circ p$. C'est aussi un morphisme de magmas pour la multiplication et il applique 1 sur 1. C'est ainsi un morphisme d'anneaux.

La dernière assertion résulte de la propriété analogue appliquée au groupe additif de A. □

Corollaire **(3.6.18)**. — *Soit* A *un anneau, soit* I *un idéal bilatère de* A, *notons* $p : A \to A/I$ *la surjection canonique.*

Soit m un entier tel que $J_n = J_m$ pour $n \geqslant m$; on a alors $I_n = p(J_n) = p(J_m) = I_m$, ce qui prouve que la suite (I_n) est stationnaire.

3.6.12. — Soit A un anneau et soit $(I_s)_{s\in S}$ une famille d'idéaux à gauche (*resp.* à droite, *resp.* bilatères). Le sous-groupe $\sum I_s$ de A engendré par la réunion des I_s est l'ensemble des sommes $\sum_{s\in S} a_s$, pour $(a_s) \in A^{(S)}$ tel que $a_s \in I_s$ pour tout $s \in S$. En effet, l'ensemble indiqué est un sous-groupe de A qui contient les I_s, et qui est contenu dans tout sous-groupe de A qui contient les I_s.

Observons alors que $\sum I_s$ est un idéal à gauche (*resp.* à droite, *resp.* bilatère) de A.

3.6.13. — Soit A un anneau, soit I un idéal à gauche de A, soit J un idéal à droite de A. On note IJ le sous-groupe de A engendré par les produits ab, pour $a \in I$ et $b \in J$. C'est l'ensemble des sommes $\sum_{s=1}^{n} a_s b_s$, pour $n \in \mathbf{N}$, $a_1, \ldots, a_n \in I$ et $b_1, \ldots, b_n \in J$. C'est un idéal bilatère de A.

3.6.14. — Soit A un anneau. Soit $\sim$ une relation d'équivalence dans A qui est compatible avec l'addition et avec la multiplication de A. Rappelons que cela signifie que les relations $a \sim b$ et $a' \sim b'$ entraînent $a + a' \sim b + b'$ et $aa' \sim bb'$. L'ensemble quotient $A/\!\sim$ de A par la relation d'équivalence $\sim$ est alors muni d'une addition et d'une multiplication telles que la surjection canonique $c : A \to A/\!\sim$ soit un morphisme de magmas pour chacune de ces lois. Par ailleurs, l'addition de $A/\!\sim$ est commutative et associative ; sa multiplication est associative, et est commutative si celle de A l'est ; de plus, $c(0)$ est élément neutre de A pour l'addition tandis que $c(1)$ est élément neutre pour la multiplication ; enfin, la multiplication est distributive par rapport à l'addition.

Ainsi, $A/\!\sim$ est un anneau qu'on appelle l'*anneau quotient* de A par la relation d'équivalence $\sim$, et l'application c est un homomorphisme d'anneaux dont le noyau est la classe de 0.

Lemme **(3.6.15)**. — *Soit* A *un anneau et soit* I *une partie de* A. *Les propriétés suivantes sont équivalentes :*

(i) *L'ensemble* I *est un idéal bilatère de* A ;

(ii) *La relation* $a \sim b$ *définie par* $b - a \in I$ *est une relation d'équivalence dans* A *qui est compatible avec son addition et avec sa multiplication ;*

(iii) *Il existe une relation d'équivalence dans* A *qui est compatible avec son addition et sa multiplication telle que* I *soit la classe de* 0 ;

c) Soit G un groupe fini, soit S un p-sous-groupe de Sylow de G et soit H un sous-groupe de G contenant $N_G(S)$. Démontrer que $H = N_G(H)$.

Exercice **(2.12.35)**. — *a*) Soit G un groupe fini, soit p un nombre premier ; on suppose que le nombre de p-sous-groupes de Sylow de G n'est pas congru à 1 modulo p^2. Démontrer qu'il existe deux p-sous-groupes de Sylow P et Q de G tels que $(P : P \cap Q) = (Q : P \cap Q) = p$.

b) Soit G un groupe fini d'ordre 1053. Démontrer qu'il existe deux 3-sous-groupes de Sylow de G, P et Q, tels que $\mathrm{Card}(P \cap Q) = 3^3$. Soit $N = N_G(P \cap Q)$. Démontrer que P et Q sont des sous-groupes de N. En déduire que $N = G$ et que G n'est pas simple.

Exercice **(2.12.36)** (Groupes nilpotents). — Soit A un groupe.

On définit par récurrence une suite (A_n) de sous-groupes distingués de A comme suit : $A_0 = \{e\}$ et, si A_n est défini, A_{n+1} est l'unique sous-groupe de A contenant A_n tel que A_{n+1}/A_n soit le centr de A/A_n.

On définit par récurrence une suite (A^n) de sous-groupes de A en posant $A^0 = A$ et, si A^n est défini, A^{n+1} est le sous-groupe de A engendré par $[A, A^n]$.

a) Démontrer que pour tout entier n, A_n et A^n sont des sous-groupes caractéristiques de A.

b) Démontrer que $A^m = \{e\}$ si et seulement si $A_m = A$. S'il existe un tel entier m, on dit que A est un groupe *nilpotent*.

c) On supose que $\{e\} = A^m \subsetneq A^{m-1}$. Démontrer que $A_{n-1} \subset A^{m-n} \subset A_n$ pour tout entier $n \in \{1, \ldots, m\}$.

d) On suppose que A est un p-groupe. Démontrer que A est nilpotent.

Exercice **(2.12.37)**. — Soit p et q des nombres premiers tels que $p < q$, soit G un groupe fini de cardinal pq. Soit P un p-sous-groupe de Sylow de G, soit Q un q-sous-groupe de Sylow de G.

a) Démontrer que P et Q sont des groupes cycliques, de même que le groupe $\mathrm{Aut}(Q)$ des automorphismes de Q.

b) Démontrer que Q est un sous-groupe distingué de G. En déduire que G est un produit semi-direct de P et Q.

c) On suppose que p ne divise pas $q - 1$. Démontrer que G est isomorphe à $\mathbf{Z}/pq\mathbf{Z}$.

d) On suppose que p divise $q - 1$. Démontrer qu'il existe un groupe non commutatif de cardinal pq, et que deux tels groupes sont isomorphes.

Exercice **(2.12.38)**. — *a*) Soit A un groupe et soit B une partie de A. Soit $\mathrm{M_A(B)}$ l'ensemble des $a \in \mathrm{A}$ tels que $\mathrm{Int}(a)(\mathrm{B}) \subset \mathrm{B}$. Démontrer que $\mathrm{M_A(B)}$ est un sous-monoïde de A.

b) On pose $\mathrm{A} = \mathrm{GL}(2, \mathbf{Q})$ et on prend pour B le sous-groupe des matrices de la forme $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, avec $a \in \mathbf{Z}$. Soit a la matrice $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Démontrer que a appartient à $\mathrm{M_A(B)}$ mais pas a^{-1}. En déduire que $\mathrm{M_A(B)}$ n'est pas un sous-groupe de A.

Lemme **(3.6.9)**. — *Soit* A *un anneau commutatif et soit* (I_j) *une famille non vide, totalement ordonnée, d'idéaux de* A. *Alors* $\mathrm{I} = \bigcup_j \mathrm{I}_j$ *est un idéal de* A. *Si, de plus,* I *possède une partie génératrice finie, il existe* j *tel que* $\mathrm{I} = \mathrm{I}_j$.

Démonstration. — Comme la famille n'est pas vide, $0 \in \mathrm{I}$. Soit $a, b \in \mathrm{I}$; soit j, k tels que $a \in \mathrm{I}_j$ et $b \in \mathrm{I}_k$. La famille (I_j) étant totalement ordonnée, on a $\mathrm{I}_j \subset \mathrm{I}_k$ ou $\mathrm{I}_k \subset \mathrm{I}_j$; dans le premier cas, on a $a, b \in \mathrm{I}_k$, donc $a + b \in \mathrm{I}_k$; dans le second, on a $a, b \in \mathrm{I}_j$, d'où $a + b \in \mathrm{I}_j$. Dans les deux cas, $a + b \in \mathrm{I}$. Soit $a \in \mathrm{I}$ et soit $b \in \mathrm{A}$; soit j tel que $a \in \mathrm{I}_j$; alors $ab \in \mathrm{I}_j$, car I_j est un idéal de A; par suite, $ab \in \mathrm{I}$. Cela démontre que I est un idéal de A.

Supposons que I possède une partie génératrice finie $\mathrm{S} = \{s_1, \ldots, s_n\}$. Pour tout $i \in \{1, \ldots, n\}$, soit j_i tel que $s_i \in \mathrm{I}_{j_i}$. La famille (I_j) étant totalement ordonnée, on démontre alors par récurrence sur n qu'il existe $j \in \{j_1, \ldots, j_n\}$ tel que l'idéal I_j contient $\mathrm{I}_{j_1}, \ldots, \mathrm{I}_{j_n}$. Ainsi, I_j contient $s_1, \ldots, s_n$, donc il contient l'idéal qu'ils engendre, à savoir I. Les inclusions $\mathrm{I} \subset \mathrm{I}_j \subset \mathrm{I}$ prouvent que $\mathrm{I} = \mathrm{I}_j$. □

Corollaire **(3.6.10)**. — *Pour qu'un anneau commutatif soit noethérien, il faut et il suffit que toute suite croissante d'idéaux soit stationnaire.*

Démonstration. — Soit A un anneau commutatif.

On suppose que toute suite croissante d'idéaux de A est stationnaire. Soit I un idéal de A; démontrons que I possède une partie génératrice finie. Sinon, pour toute partie finie S de I, l'idéal $\langle \mathrm{S} \rangle$ engendré par S est contenu dans I, mais distinct de I. On construit alors par récurrence une suite (s_n) d'éléments de I telle que, notant I_n l'idéal engendré par $\{s_1, \ldots, s_n\}$, s_{n+1} n'appartienne pas à I_n. La suite d'idéaux (I_n) est strictement croissante, ce qui contredit l'hypothèse faite sur A.

Inversement, une suite croissante (I_n) d'idéaux est une famille totalement ordonnée; si sa réunion I possède une partie génératrice finie, il existe d'après le lemme un entier n tel que $\mathrm{I} = \mathrm{I}_n$. On a alors $\mathrm{I} = \mathrm{I}_n \subset \mathrm{I}_m \subset \mathrm{I}$ pour tout entier $m \geqslant n$, donc $\mathrm{I}_m = \mathrm{I}_n$ pour $m \geqslant n$. Cela prouve que la suite (I_n) est stationnaire. □

Remarque **(3.6.11)**. — Soit A un anneau noethérien et soit I un idéal de A; alors A/I est un anneau noethérien.

Notons $p : \mathrm{A} \to \mathrm{A/I}$ la surjection canonique. Soit une suite croissante (I_n) d'idéaux de A/I; pour tout entier n, posons $\mathrm{J}_n = p^{-1}(\mathrm{I}_n)$. La suite (J_n) est une suite croissante d'idéaux de A; comme A est noethérien, elle est stationnaire.

proposition 2.4.6, on a donc $\mathrm{Ker}(f) = \{0\}$ si et seulement si l'homomorphisme f est injectif.

Exemple **(3.6.5)**. — Soit A un anneau commutatif et soit I un idéal de A. On note $\sqrt{\mathrm{I}}$ l'ensemble des éléments $a \in \mathrm{A}$ pour lesquels il existe $n \geqslant 1$ tel que $a^n \in \mathrm{I}$ (*radical de* I).

On a $\mathrm{I} \subset \sqrt{\mathrm{I}}$. Soit ensuite $a, b \in \sqrt{\mathrm{I}}$, soit $m, n \in \mathbf{N}$ tels que $a^m \in \mathrm{I}$ et $b^n \in \mathrm{I}$. Pour $p \geqslant m + n - 1$, on a $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i = 0$ car si $i < n$, alors $p - i \geqslant m$ et $a^i = 0$, et si $i \geqslant n$, alors $b^i = 0$. Enfin, si $a \in \sqrt{\mathrm{I}}$ et $b \in \mathrm{A}$, soit $n \in \mathbf{N}$ tel que $a^n = 0$; comme A est commutatif, il vient $(ba)^n = b^n a^n = 0$. Il en résulte que $\sqrt{\mathrm{I}}$ est un idéal de A qui contient I.

En particulier, si l'on prend $\mathrm{I} = \{0\}$, l'ensemble N des éléments de A qui sont nilpotents est un idéal de A, qu'on appelle le *nilradical* de A.

Lemme **(3.6.6)**. — *Soit* A *un anneau. L'intersection* $\bigcap_{s \in \mathrm{S}} \mathrm{I}_s$ *d'une famille* $(\mathrm{I}_s)_{s \in \mathrm{S}}$ *d'idéaux à gauche (*resp. *à droite,* resp. *bilatères) de* A *est un idéal à gauche (*resp. *à droite,* resp. *bilatère) de* A.

Démonstration. — Traitons le cas d'une famille d'idéaux à gauche. Notons I cette intersection ; c'est un sous-groupe du groupe additif de A. Soit $a \in \mathrm{A}$ et $x \in \mathrm{I}$; pour tout $s \in \mathrm{S}$, on a $x \in \mathrm{I}_s$, donc $ax \in \mathrm{I}_s$, car I_s est un idéal à gauche de A ; par suite, $ax \in \mathrm{I}$. Cela prouve que I est un idéal à gauche de A. □

Corollaire **(3.6.7)**. — *Soit* A *un anneau et soit* S *une partie de* A. *Il existe un plus petit idéal à gauche (*resp. *à droite,* resp. *bilatère) de* A *qui contient* S.

C'est l'intersection de la famille de tous les idéaux à gauche (*resp.* à droite, *resp.* bilatères) de A qui contiennent S. On dit que c'est l'idéal à gauche (*resp.* à droite, *resp.* bilatère) de A engendré par S.

L'idéal à gauche engendré par S est l'ensemble des sommes de la forme $\sum_{s \in \mathrm{S}} a_s s$, pour $(a_s) \in \mathrm{A}^{(\mathrm{S})}$. En effet, l'ensemble indiqué est un idéal à gauche de A qui contient S et qui est contenu dans tout idéal à gauche qui contient S. On démontre de même que l'idéal à droite engendré par S est l'ensemble des sommes de la forme $\sum_{s \in \mathrm{S}} s b_s$, pour $(b_s) \in \mathrm{A}^{(\mathrm{S})}$, et que l'idéal bilatère engendré par S est l'ensemble des sommes $\sum_{s \in \mathrm{S}} a_s s b_s$, pour $(a_s), (b_s) \in \mathrm{A}^{(\mathrm{S})}$.

Définition **(3.6.8)**. — *Soit* A *un anneau commutatif. On dit que* A *est un anneau* noethérien *si tout idéal de* A *possède une partie génératrice finie.*

CHAPITRE 3

ANNEAUX

3.1. Définitions

Définition **(3.1.1)**. — *Un anneau est un ensemble* A *muni de deux lois,* $+$ *et* $\cdot$, *appelées addition et multiplication, vérifiant les propriétés suivantes :*

a) *Pour l'addition,* A *est un groupe commutatif ;*
b) *Pour la multiplication,* A *est un monoïde ;*
c) *La multiplication est distributive par rapport à l'addition.*

On note 0 l'élément neutre de l'addition, 1 l'élément neutre de la multiplication.

3.1.2. — Soit A un anneau. On dit que A est un *anneau commutatif* si la multiplication de A est commutative.

On dit que des éléments a et b de A commutent si l'on a $ab = ba$.

Proposition **(3.1.3)** (Formule du binôme). — *Soit* A *un anneau, soit* a *et* b *des éléments de* A *tels que* $ab = ba$. *Pour tout entier* $n \geqslant 0$, *on a*

$$(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^{n-p} b^p.$$

Démonstration. — La preuve est classique et se fait par récurrence sur n. Lorsque $n = 0$, les deux membres valent 1. Supposons la formule vraie pour n, alors

$$\begin{aligned}(a+b)^{n+1} = (a+b)(a+b)^n &= (a+b)\left(\sum_{p=0}^{n} \binom{n}{p} a^{n-p} b^p\right) \\ &= a \sum_{p=0}^{n} \binom{n}{p} a^{n-p} b^p + b \sum_{p=0}^{n} \binom{n}{p} a^{n-p} b^p\end{aligned}$$

$$
\begin{aligned}
&= \sum_{p=0}^{n} \binom{n}{p} a^{n+1-p} b^p + \sum_{p=0}^{n} \binom{n}{p} a^{n-p} b^{p+1} \\
&= \binom{n}{0} a^{n+1} + \sum_{p=1}^{n} \binom{n}{p} a^{n+1-p} b^p + \sum_{p=1}^{n} \binom{n}{p-1} a^{n+1-p} b^p + \binom{n}{0} b^{n+1} \\
&= a^{n+1} + \sum_{p=1}^{n} \left(\binom{n}{p} + \binom{n}{p-1} \right) a^{n+1-p} b^p + b^{n+1} \\
&= \sum_{p=0}^{n+1} \binom{n+1}{p} a^{n+1-p} b^p,
\end{aligned}
$$

comme il fallait démontrer. □

Définition **(3.1.4)**. — *Soit* A *un anneau et soit a un élément de* A.

a) *On dit que a est* simplifiable *(ou* régulier*) s'il l'est pour la multiplication, c'est-à-dire si pour tout élément non nul* $x \in A$*, on a* $ax \neq 0$ *et* $xa \neq 0$.

b) *On dit que a est* inversible *s'il l'est pour la multiplication, c'est-à-dire s'il existe* $b \in A$ *tel que* $ab = ba = 1$.

c) *On dit que a est* nilpotent *s'il existe un entier* $n \geqslant 1$ *tel que* $a^n = 0$.

On définit plus généralement la notion d'élément simplifiable à droite ou à gauche, et la notion d'élément inversible à droite ou à gauche.

L'ensemble des éléments simplifiables de A est un sous-monoïde de $(A, \times)$. L'ensemble des éléments inversibles de A est un groupe pour la multiplication qu'on note $A^\times$.

Définition **(3.1.5)**. — *Soit* A *un anneau non nul.*

On dit que A *est un* corps *si tout élément non nul est inversible.*

On dit que A *est* intègre *s'il est commutatif et si tout élément non nul de* A *est simplifiable.*

3.2. Sous-anneaux, sous-corps

3.2.1. — Soit A un anneau et soit B une partie de A. On dit que B est un sous-anneau de A si c'est un sous-groupe de A pour l'addition et un sous-monoïde de A pour la multiplication. Cela signifie que $0, 1 \in B$, que la somme et le produit de deux éléments de B appartiennent à B, de même que l'opposé d'un élément de B.

Enfin, si $\varphi' : A^{(M)} \to B$ est un morphisme de A-algères tel que $\varphi'(\delta_m) = f(m)$ pour tout $m \in M$, les calculs ci-dessus montrent que $\varphi'(u) = \varphi(u)$ pour tout $u \in A^{(M)}$, donc $\varphi' = \varphi$. □

Exemple **(3.5.4)**. — Soit K un corps commutatif et soit G un groupe. L'algèbre $K^{(G)}$ est appelée l'algèbre du groupe G. Soit V un espace vectoriel et prenons pour K-algèbre B l'algèbre $\mathrm{End}_K(V)$ des endomorphismes de V. L'ensemble de ses éléments inversibles est le groupe $\mathrm{GL}(V)$ des automorphismes de V. D'après la propriété universelle, les homomorphismes de groupes de G dans $\mathrm{GL}(V)$ correspondent aux homomorphismes d'algèbres de $K^{(G)}$ dans $\mathrm{End}_K(V)$.

3.6. Idéaux, anneaux quotients

Définition **(3.6.1)**. — *Soit* A *un anneau et soit* I *un sous-groupe du groupe additif de* A*. On dit que* I *est un* idéal à gauche (resp. *à droite) si pour tout* $a \in A$ *et tout* $x \in I$*, on a* $ax \in I$ (resp. $xa \in I$)*. On dit que c'est un idéal* bilatère *si c'est à la fois un idéal à droite et à gauche.*

Dans un anneau commutatif, les notions d'idéal à gauche, à droite et bilatère coïncident ; on dit alors plus simplement *idéal.*

Exemple **(3.6.2)**. — Les sous-groupes $\{0\}$ et A sont des idéaux bilatères de A.

Exemple **(3.6.3)**. — Soit A un anneau et soit a un élément de A. L'ensemble des éléments de A de la forme xa, pour $x \in A$, est un idéal à gauche de A ; on dit que c'est l'idéal principal à gauche engendré par A. De même, l'ensemble des éléments de A de la forme ax, pour $x \in A$ est un idéal à droite de A.

Exemple **(3.6.4)**. — Soit $f : A \to B$ un homomorphisme d'anneaux, soit J un idéal à gauche (*resp.* à droite, *resp.* bilatère) de B et notons $I = f^{-1}(J)$. Alors I est un idéal à gauche (*resp.* à droite, *resp.* bilatère) de A.

C'est en effet un sous-groupe du groupe additif de A. De plus, pour $a \in A$ et $x \in I$, on a $f(ax) = f(a)f(x) \in J$ si J est un idéal à gauche de B, ce qui prouve que I est, dans ce cas, un idéal à gauche de A. Le cas d'un idéal à droite se traite de façon analogue et celui d'un idéal bilatère s'en déduit.

En particulier, le *noyau* de f, $\mathrm{Ker}(f) = f^{-1}(\{0\})$, est un idéal bilatère de A ; c'est en fait le noyau de f en tant qu'homomorphisme de groupes. D'après la

3.5.2. — Si le monoïde M est commutatif, cet anneau est commutatif. En effet, pour $f, g \in A^{(M)}$ et $m \in M$, on a alors

$$f * g(m) = \sum_{xy=m} f(x)g(y) = \sum_{yx=m} g(y)f(x) = g * f(m).$$

Lemme **(3.5.3)** (Propriété universelle de l'algèbre d'un monoïde)

Soit M *un monoïde et soit* A *un anneau commutatif. Soit* B *une* A*-algèbre (commutative ou non) et soit* $f : M \to B$ *un morphisme de* M *dans le monoïde multiplicatif de* B*. Il existe un unique homomorphisme de* A*-algèbres,* $\varphi : A^{(M)} \to B$*, tel que* $\varphi(\delta_m) = f(m)$ *pour tout* $m \in M$*.*

Démonstration. — Soit u un élément de $A^{(M)}$; c'est une fonction de M dans A, à support fini, et l'on peut écrire $u = \sum_{m\in M} u(m)\delta_m$ (somme éventuellement infinie mais dont seulement un nombre fini de termes ne sont pas nuls). Posons alors $\varphi(u) = \sum_{m\in M} u(m)f(m)$. Démontrons que l'application $\varphi : A^{(M)} \to B$ ainsi définie est un homomorphisme de A-algèbres. Il applique 0 sur 0 et respecte l'addition : pour $u, v \in A^{(M)}$, on a en effet :

$$\varphi(u+v) = \sum_{m\in M} (u+v)(m)f(m) = \sum_{m\in M} u(m)f(m) + \sum_{m\in M} v(m)f(m).$$

Ensuite, l'élément unité de $A^{(M)}$ est la fonction δ_e, où e est l'élément neutre de M, de sorte que $\varphi(\delta_e) = u(e) = 1$. De plus, si $u, v \in A^{(M)}$, on a

$$\begin{aligned}
\varphi(u * v) &= \sum_{m\in M} u * v(m)f(m) \\
&= \sum_{x,y\in M} u(x)v(y)f(xy) \\
&= \sum_{x,y\in M} u(x)v(y)f(x)f(y) \\
&= \sum_{x\in M} u(x)f(x) \sum_{y\in M} v(y)f(y) \\
&= \varphi(u)\varphi(v).
\end{aligned}$$

Cela prouve que φ est un homomorphisme d'anneaux. Enfin, pour $a \in A$ et $u \in A^{(M)}$, la fonction au applique m sur $au(m)$, de sorte que

$$\varphi(au) = \sum_{m\in M} (au)(m) = \sum_{m\in M} au(m) = a \sum_{m\in M} u(m) = a\varphi(u),$$

ce qui prouve que φ est un morphisme de A-algèbres.

Alors, l'addition et la multiplication de A définissent des lois de composition sur B qui en font un anneau.

Lemme **(3.2.2)**. — *Soit* A *un anneau, soit* $(B_i)_{i\in I}$ *une famille de sous-anneaux de* A *et soit* $B = \bigcap_{i\in I} B_i$ *son intersection. Alors,* B *est un sous-anneau de* A*.*

Démonstration. — Cela découle immédiatement du résultat correspondant pour les monoïdes et les groupes (lemme 2.3.5). □

Corollaire **(3.2.3)**. — *Soit* A *un anneau et soit* S *une partie de* A*. Il existe un plus petit sous-anneau* B *de* A *qui contient* S*.*

C'est l'intersection de la famille de tous les sous-anneaux de A qui contiennent S. On l'appelle le sous-anneau de A engendré par S.

Un cas particulier de cette construction est important, où S est de la forme $B \cup T$, B étant un sous-anneau de A. Dans ce cas, on note $B[T]$ le sous-anneau de A engendré par $B \cup T$, et on dit que c'est le sous-anneau de A engendré par T sur B.

3.2.4. — Soit F un corps et soit E une partie de F. On dit que E est un sous-corps de F si c'est un sous-anneau de F et si c'est un corps.

Cela signifie que $0, 1 \in E$, que la somme et le produit de deux éléments de E appartiennent à E, de même que l'opposé d'un élément de E et l'inverse d'un élément non nul de E.

Alors, l'addition et la multiplication de F définissent des lois de composition sur E qui en font un anneau.

Lemme **(3.2.5)**. — *Soit* F *un corps, soit* $(E_i)_{i\in I}$ *une famille de sous-corps de* A *et soit* $E = \bigcap_{i\in I} E_i$ *son intersection. Alors,* E *est un sous-corps de* F*.*

Démonstration. — Il résulte du résultat correspondant pour les anneaux que E est un sous-anneau de F. De plus, $E \neq \{0\}$ car $1 \in E$. Soit enfin x un élément non nul de E ; pour tout i, on a $x \in E_i$, donc $x^{-1} \in E_i$; par suite, $x^{-1} \in E$. □

Corollaire **(3.2.6)**. — *Soit* F *un corps et soit* S *une partie de* F*. Il existe un plus petit sous-corps de* F *qui contient* S*.*

C'est l'intersection de la famille de tous les sous-corps de F qui contiennent S ; on l'appelle le sous-corps de F engendré par S.

Un cas particulier de cette construction est important, où S est de la forme $E \cup T$, E étant un sous-corps de F. Dans ce cas, on note $E(T)$ le sous-corps de F engendré par $E \cup T$, et on dit que c'est le sous-corps de F engendré par T sur E.

3.2.7. — Soit A un anneau et soit a un élément de A. Le *commutant* de a est l'ensemble $Z_a(A)$ des éléments b de A qui commutent avec a, c'est-à-dire tels que $ab = ba$. C'est un sous-anneau de A. Si A est un corps, le commutant de a est un sous-corps de A.

Le *centre* de A, noté $Z(A)$, est l'ensemble des éléments $a \in A$ tels que $ab = ba$ pour tout $b \in A$. C'est l'intersection des commutants de tous les éléments de a ; c'est un sous-anneau de A. Si A est un corps, le centre de A est un sous-corps de A.

Exemple **(3.2.8)**. — Soit F un corps. On appelle *sous-corps premier* de F le plus petit sous-corps de F, c'est-à-dire le sous-corps de F engendré par $\varnothing$. Notons-le E.

On a $1_F \in E$, donc $n \cdot 1_F \in E$ pour tout entier $n \in \mathbf{Z}$. On voit alors deux possibilités pour ce sous-corps :

a) Supposons que pour tout entier $n \geqslant 1$, on ait $n \cdot 1_F \neq 0$. Alors, pour m et $n \in \mathbf{Z}$ tels que $m \neq n$, on a $n \cdot 1_F \neq m \cdot 1_F$ puisque, par hypothèse, $(n-m) \cdot 1_F \neq 0$ si $n > m$, et $(m-n) \cdot 1_F \neq 0$ sinon. Ainsi, l'ensemble des éléments de F de la forme $n \cdot 1_F$, pour $n \in \mathbf{Z}$, est un sous-anneau de E que l'on peut identifier à $\mathbf{Z}$. De plus, E contient aussi l'inverse de $n1_F$, si $n \neq 0$, et toute fraction m/n, pour $m \in \mathbf{Z}$ et $n \in \mathbf{Z} - \{0\}$, de sorte que E « contient » tous les nombres rationnels. Ils forment un sous-corps de E, de sorte que E s'identifie au corps $\mathbf{Q}$ des nombres rationnels. On dit que F est de *caractéristique* 0.

b) Supposons qu'il existe un entier $n \geqslant 1$ tel que $n \cdot 1_F = 0$, et soit p le plus petit de ces entiers. Démontrons que p est un nombre premier. On a $p \neq 1$ puisque $1 \cdot 1_F = 1_F \neq 0$. Si p n'était pas premier, il existerait des entiers $m, n \geqslant 2$ tels que $p = mn$, d'où $p \cdot 1_F = (m \cdot 1_F)(n \cdot 1_F) = 0$ puis $m \cdot 1_F = 0$ ou $n \cdot 1_F = 0$. Comme $m, n < p$, cela contredit la minimalité de p.

Dans ce cas, l'ensemble $\{0, 1_F, \ldots, (p-1) \cdot 1_F\}$ est un sous-anneau de E, qu'on identifie à l'anneau $\mathbf{Z}/p\mathbf{Z}$. Cet anneau est un corps, donc $E = \mathbf{Z}/p\mathbf{Z}$; on dit que F est de caractéristique p.

Bien que ces deux expressions soient tout à fait impropres, surtout en français, on dit souvent que F est de caractéristique positive, ou de caractéristique finie, pour dire qu'il n'est pas de caractéristique 0.

Pour $f, g \in A^{(M)}$, l'ensemble P des couples (x, y) tels que $f(x) \neq 0$ et $g(y) \neq 0$ est fini, ce qui entraîne d'une part que $f * g(m)$ est bien défini (la somme est finie) et d'autre part que $f * g(m) \neq 0$ si m n'est pas égal à l'un des produits xy, pour $(x, y) \in P$.

Soit $f, g, h \in A^{(M)}$. Pour $m \in M$, on a

$$(f * g) * h)(m) = \sum_{\substack{p,z \in M \\ pz=m}} (f * g)(p)h(z) = \sum_{\substack{x,y,z \in M \\ xyz=m}} f(x)g(y)h(z).$$

De même,

$$f * (g * h)(m) = \sum_{\substack{x,q \in M \\ xq=m}} f(x)(g * h)(q) = \sum_{\substack{x,y,z \in M \\ xyz=m}} f(x)g(y)h(z).$$

On a donc $(f * g) * h = f * (g * h)$: le produit de convolution est associatif.

Pour tout élément $m \in M$, soit δ_m la fonction de M dans A telle que $\delta_m(x) = 1$ si $x = m$ et $\delta_m(x) = 0$ sinon (« fonction de Dirac »). Soit e l'élément neutre de M. Alors, pour tout $f \in A^{(M)}$ et tout $m \in M$, on a $\delta_e * f(m) = \sum_{xy=m} \delta_e(x) f(y) = f(m)$ et $f * \delta_e(m) = \sum_{xy=m} f(x)\delta_e(y) = f(m)$. Ainsi, δ_e est l'élément neutre du produit de convolution.

Plus généralement, pour tout couple (m, n) d'éléments de M, on a $\delta_m * \delta_n = \delta_{mn}$, de sorte que l'application $m \mapsto \delta_m$ est un homomorphisme de monoïdes de M dans le monoïde multiplicatif de $A^{(M)}$. On remarque aussi que pour tout $f \in A^{(M)}$, on a $f = \sum_{m \in M} f(m)\delta_m$; plus précisément, la famille $(f(m))_{m \in M}$ est l'unique famille (a_m) telle que $f = \sum_{m \in M} a_m \delta_m$.

Enfin, le produit de convolution est distributif sur l'addition : pour $f, g, h \in A^{(M)}$ et $m \in M$, on a

$$\begin{aligned} f * (g + h)(m) &= \sum_{xy=m} f(x)(g + h)(y) \\ &= \sum_{xy=m} f(x)g(y) + \sum_{xy=m} f(x)h(y) \\ &= f * g(m) + f * h(m), \end{aligned}$$

et, de façon analogue, $(f + g) * h = f * h + g * h$.

Ainsi, l'addition et le produit de convolution font de $A^{(M)}$ un anneau. L'application $a \mapsto a\delta_e$ de A dans $A^{(M)}$ est un homomorphisme d'anneaux, et tout élément de son image est central. Ainsi, $A^{(M)}$ est une A-algèbre qu'on appelle l'*algèbre du monoïde* M sur A.

Par les mêmes calculs qu'en licence, on vérifie que c'est un anneau. Son élément 0 est la matrice dont tous les coefficients sont nuls ; son élément 1 est la matrice I_n dont le coefficient (i, j) est égal à 1 si $i = j$, et à 0 sinon.

Cet anneau n'est pas commutatif lorsque $n \geqslant 2$ ou lorsque A n'est pas commutatif.

Son centre est égal à $A \cdot I_n$, et est isomorphe à A. Lorsque A est commutatif, l'homomorphisme $a \mapsto aI_n$ de A dans $M_n(A)$ fait de $M_n(A)$ une A-algèbre.

3.4.5. — Soit G un groupe abélien. L'ensemble $\mathrm{End}(G)$ des endomorphismes de G est un sous-groupe du groupe abélien des applications de G dans G. C'est aussi un sous-monoïde pour la composition des applications. Enfin, la composition est distributive sur l'addition, puisque pour $f, g, h \in \mathrm{End}(G)$ et $x \in G$, on a $f \circ (g+h)(x) = f(g(x)+h(x)) = f \circ g(x) + f \circ h(x)$. Ginsi, $\mathrm{End}(G)$ possède une structure naturelle d'anneau.

Soit F un corps et soit V un F-espace vectoriel. L'ensemble $\mathrm{End}_F(V)$ est un sous-anneau de l'anneau des endomorphismes du groupe abélien V.

3.4.6. — Soit A un anneau ; l'anneau opposé A^o a même sous-groupe additif, mais le monoïde multiplicatif est le monoïde opposé du monoïde multiplicatif de A.

Si A est un anneau commutatif, l'application $M \mapsto {}^tM$ est un isomorphisme de l'anneau des matrices $M_n(A)$ sur son anneau opposé.

3.5. Algèbres de monoïdes, de groupes

3.5.1. — Soit M un monoïde et soit A un anneau ; pour simplifier certains énoncés, on suppose que A est commutatif. Soit $A^{(M)}$ l'ensemble des fonctions f de M dans A de support fini, c'est-à-dire telles que l'ensemble des $m \in M$ tels que $f(m) \neq 0$ soit fini. C'est un sous-groupe du groupe additif A^M des applications de M dans A, mais ce n'est pas un sous-anneau lorsque M est infini, puisque la fonction constante de valeur 1 n'appartient pas à $A^{(M)}$. On le munit du *produit de convolution* défini par

$$f * g(m) = \sum_{\substack{x,y \in M \\ xy=m}} f(x)g(y).$$

3.3. Morphismes

Définition **(3.3.1)**. — *Soit* A *et* B *des anneaux. On dit qu'une application* $f : A \to B$ *est un* homomorphisme *d'anneaux si c'est à la fois un morphisme de groupes pour l'addition et un morphismes de monoïdes pour la multiplication.*

Autrement dit, on demande que soient vérifiées les relations : $f(0) = 0$, $f(1) = 1$, $f(a+b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$ pour tous $a, b \in A$.

Un homomorphisme d'anneaux $f : A \to B$ induit par restriction un homomorphisme du groupe $A^\times$ des éléments inversibles de A dans le groupe $B^\times$ des éléments inversibles de B.

3.3.2. — Soit A un anneau ; l'application identique id_A est un homomorphisme d'anneaux. Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux, leur composée $g \circ f$ est un morphisme d'anneaux.

Les anneaux et leurs morphismes constituent ainsi une catégorie.

On dit qu'un homomorphisme d'anneaux $f : A \to B$ est un *isomorphisme* s'il existe un homomorphisme d'anneaux $g : B \to A$ tel que $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$.

Un homomorphisme de A dans A est appelé endomorphisme de A ; si c'est un isomorphisme, on dit que c'est un automorphisme. L'ensemble $\mathrm{End}(A)$ des endomorphismes de A est un monoïde pour la composition des applications ; le groupe de ses éléments inversibles est l'ensemble $\mathrm{Aut}(A)$ des automorphismes de A.

Lemme **(3.3.3)**. — *Pour qu'un homomorphisme d'anneaux* $f : A \to B$ *soit un isomorphisme, il faut et il suffit qu'il soit bijectif, sa bijection réciproque est alors un homomorphisme d'anneaux.*

Démonstration. — Si f est un isomorphisme, il est bijectif. Supposons inversement que f soit bijectif et soit g sa bijection réciproque. Comme la bijection réciproque d'un homomorphisme bijectif de monoïdes est un homomorphisme de monoïdes, g est un homomorphisme de monoïdes à la fois pour l'addition et pour la multiplication, donc c'est un homomorphisme d'anneaux. □

Exemple **(3.3.4)**. — Soit p un nombre premier et soit A un anneau commutatif tel que $p \cdot 1 = 0$ dans A.[(1)] Démontrons que l'application $\varphi : A \to A$ définie par $\varphi(x) = x^p$ est un homomorphisme d'anneaux.

[(1)] On dit parfois que A est un anneau de caractéristique p.

On a bien sûr $\varphi(0) = 0$ et $\varphi(1) = 1$. On a aussi $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$ pour tous $x, y \in A$, car x et y commutent. Enfin, pour tous $x, y \in A$, la formule du binôme entraîne que $\varphi(x+y) = \varphi(x) + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + \varphi(y)$. Soit $k \in \{1, \ldots, p-1\}$; démontrons que $\binom{p}{k}$ est un entier divisible par p. Par définition, on a $\binom{p}{k} = p!/k!(p-k)!$, de sorte que $k!(p-k)!\binom{p}{k} = p!$ est multiple de p. Comme p est un nombre premier, p ne divise aucun entier k tel que $1 \leqslant k \leqslant p-1$, de sorte que p ne divise pas $k!(p-k)!$ de $\binom{p}{k}$. Par suite, il divise $\binom{p}{k}$. On a donc $\binom{p}{k} x^{p-k} y^k$ et $\varphi(x+y) = \varphi(x) + \varphi(y)$. Enfin, $\varphi(-x) = (-x)^p = (-1)^p \varphi(x)$; si $p = 2$, on a $\varphi(-x) = \varphi(x) = -\varphi(x)$ puisque $1 = -1$ dans A ; sinon, $(-1)^p = -1$ et $\varphi(-x) = -\varphi(x)$.

Cet homomorphisme est appelé homomorphisme de Frobenius de A.

Un cas particulier très important est obtenu lorsque A est un corps de caractéristique p.

Exemple **(3.3.5)**. — Soit A un anneau. Pour tout $a \in A^\times$, l'application $\mathrm{Int}(a) : x \mapsto axa^{-1}$ est un automorphisme de A (appelé *automorphisme intérieur*). On a $\mathrm{Int}(a) \circ \mathrm{Int}(b) = \mathrm{Int}(ab)$; si $a \in Z(A)$, on a $\mathrm{Int}(a) = \mathrm{id}_A$. L'application $\mathrm{Int} : A^\times \to \mathrm{Aut}(A)$ est donc un homorphisme de groupes.

3.3.6. — Soit A un anneau commutatif. On appelle A-*algèbre* la donnée d'un anneau B et d'un homomorphisme u de A dans B tel que $u(A)$ soit contenu dans le centre de B. Alors, pour tout élément $a \in A$ et tout élément $b \in B$, on pose $ab = u(a)b$. On a les relations $a(b+c) = ab + ac$, $(aa')b = a(a'b)$ et $(ab)(a'c) = aa'(bc)$ pour $a, a' \in A$ et $b, c \in B$.

Cette convention permet de sous-entendre l'homomorphisme u, en écrivant par exemple « Soit B une A-algèbre. »

Si B et C sont des A-algèbres, un homomorphisme de A-algèbres de B dans C est un homomorphisme d'anneaux $f : B \to C$ tel que $f(ab) = af(b)$ pour tout $a \in A$ et tout $b \in B$.

3.4. Exemples

3.4.1. — Citons sans commentaires l'anneau $\mathbf{Z}$ des entiers relatifs, les anneaux finis $\mathbf{Z}/n\mathbf{Z}$, pour $n \geqslant 1$, les corps $\mathbf{Q}$ des nombres rationnels, $\mathbf{R}$ des nombres réels, $\mathbf{C}$ des nombres complexes. Mentionnons aussi, si F est un corps commutatif, l'anneau $F[T]$ des polynômes en une indéterminée T à coefficients dans F.

3.4.2. Produit d'une famille d'anneaux. — Soit I un ensemble et soit $(A_i)_{i \in I}$ une famille d'anneaux ; soit $A = \prod_{i \in I} A_i$ le produit de cette famille. On le munit de l'addition et de la multiplication terme à terme : pour $a = (a_i)$ et $b = (b_i)$ dans A, on pose $a + b = (a_i + b_i)$ et $ab = (a_i b_i)$; on note aussi 0 (*resp.* 1) la famille dont le terme d'indice i est l'élément 0 (*resp.* l'élément 1) de A_i. Alors A un un groupe abélien pour l'addition (produit de groupes abélien), un monoïde pour la multiplication (produit de monoïdes) et on vérifie immédiatement la distributivité de la multiplication sur l'addition ; c'est donc un anneau qu'on appelle le *produit* de la famille $(A_i)_{i \in I}$.

Pour tout $i \in I$, soit $p_i : A \to A_i$ la projection d'indice i ; c'est un homomorphisme d'anneaux.

Lorsque les anneaux A_i sont égaux à un même anneau A, on note A^I l'anneau produit ; c'est aussi l'ensemble des fonctions de I dans A avec la l'addition et la multiplication point par point. Lorsque X est un espace topologique, l'ensemble $\mathscr{C}(X, \mathbf{R})$ des applications continues de X dans $\mathbf{R}$ est un sous-anneau de $\mathbf{R}^X$. Lorsque X est un ouvert de $\mathbf{R}$ (ou de $\mathbf{R}^n$), l'ensemble $\mathscr{C}^k(X, \mathbf{R})$ des fonctions de classe $\mathscr{C}^k$ de X dans $\mathbf{R}$ est un sous-anneau de $\mathbf{R}^X$. (Ici, k est un élément de $\mathbf{N} \cup \{\infty\}$.)

L'anneau A et la famille (p_i) vérifient la propriété universelle suivante.

Lemme **(3.4.3)**. — *Soit (A_i) une famille d'anneaux et soit $A = \prod_{i \in I} A_i$ l'anneau produit ; pour tout i, soit $p_i : A \to A_i$ la projection d'indice i. Pour tout anneau B et toute famille (f_i), où $f_i : B \to A_i$ est un homomorphisme d'anneaux, il existe un unique homomorphisme d'anneaux $f : B \to A$ tel que $f_i = p_i \circ f$ pour tout i.*

Démonstration. — Soit $f : B \to A$ l'application donnée par $f(b) = (f_i(b))_{i \in I}$; c'est la seule application de B dans A dont la composée avec p_i est égale à f_i, pour tout $i \in I$. C'est un homomorphisme d'anneaux, d'où le lemme. □

3.4.4. — Soit A un anneau et soit n un entier $\geqslant 0$. Soit $M_n(A)$ l'ensemble des matrices $n \times n$ à coefficients dans A. On le munit des règles de calcul usuelles : la somme de deux matrices $P = (p_{i,j})$ et $Q = (q_{i,j})$ est la matrice $R = (r_{i,j})$ donnée par $r_{i,j} = p_{i,j} + q_{i,j}$ pour tout couple (i, j) d'éléments de $\{1, \ldots, n\}$; le produit de ces matrices P et Q est la matrice S donnée par $s_{i,j} = \sum_{k=1}^{n} p_{i,k} q_{k,j}$, pour tout couple (i, j).