

josette calais

éléments de théorie des groupes



MATHEMATIQUES

MATHÉMATIQUES

*Eléments
de théorie
des groupes*

JOSETTE GALAIS

Professeur à l'Université de Reims, Champagne-Ardenne



PRESSES UNIVERSITAIRES DE FRANCE

ISBN 2 13 038465 X

ISBN 0246-3822

Dépôt légal — 1^{re} édition : 1984, septembre

© Presses Universitaires de France, 1984
108, boulevard Saint-Germain, 75006 Paris

SOMMAIRE

PRÉFACE	11
INTRODUCTION	13
PRINCIPALES NOTATIONS	15
CHAPITRE PREMIER / <i>Structure de groupe</i>	17
1 / <i>Notion de groupe</i>	17
A / Loi de composition interne	17
B / Groupe	18
C / Règles de calcul dans un groupe	20
D / Premiers exemples de groupes	23
E / Table de Cayley d'un groupe fini	27
2 / <i>Sous-groupe</i>	29
A / Notion de sous-groupe. Propriétés élémentaires.....	29
B / Exemples de sous-groupes	31
C / Sous-groupe engendré par une partie non vide d'un groupe.....	34
D / Somme directe de sous-groupes d'un groupe abélien $(G, +)$	38
3 / <i>Morphismes de groupes</i>	41
A / Définitions. Propriétés générales	41
B / Isomorphismes. Théorème de Cayley	45
C / Monomorphismes et épimorphismes de groupes....	51

4 / Produit direct de groupes	54
A / Produit direct de deux groupes	54
B / Produit direct d'un nombre fini quelconque de groupes	58
C / Produit direct d'une famille quelconque de groupes	58
D / Propriété universelle du produit direct de groupes	60
Exercices chapitre I	61
CHAPITRE II / Classes modulo un sous-groupe	71
1 / Classes à droite, classes à gauche modulo un sous-groupe.....	71
A / Relations d'équivalence modulo un sous-groupe...	71
B / Théorème de Lagrange. Indice d'un sous-groupe...	74
C / Formule des indices	78
2 / Propriétés des relations d'équivalence modulo un sous-groupe...	79
A / Compatibilité d'une relation d'équivalence avec une loi de composition	79
B / Propriétés des relations du type \mathcal{R}_H et ${}_H\mathcal{R}$. 1 ^{er} théorème d'isomorphisme	81
Exercices chapitre II	84
CHAPITRE III / Groupes monogènes. Groupes symétriques S_n . Groupes diédraux	89
1 / Groupes monogènes.....	89
A / Caractérisation des groupes monogènes	89
B / Sous-groupes d'un groupe monogène	93
C / Générateurs d'un groupe monogène	97
D / Produits directs de groupes cycliques. Calcul de $\varphi(n)$	101
2 / Groupes symétriques S_n	105
A / Notion de σ -orbite (ou orbite suivant σ).....	106
B / Cycles dans S_n . Transpositions	108
C / Décomposition d'une permutation en un produit de cycles ou en un produit de transpositions.....	111
D / Signature d'une permutation	115
E / Groupe alterné A_n	120
3 / Groupes diédraux D_n	120
Exercices chapitre III	126

CHAPITRE IV / <i>Sous-groupes normaux</i>	136
1 / <i>Notion de sous-groupe normal (ou distingué). Groupe quotient</i>	136
2 / <i>Notion de groupe simple</i>	138
3 / <i>Etude des sous-groupes normaux</i>	140
A / <i>Caractérisations et propriétés</i>	140
B / <i>Classes de conjugaison. Normalisateur</i>	145
4 / <i>Etude des groupes quotients</i>	147
A / <i>Propriété universelle du groupe quotient</i>	147
B / <i>Sous-groupes d'un groupe quotient</i>	150
C / <i>2^e et 3^e théorèmes d'isomorphisme</i>	152
5 / <i>Groupe dérivé. Sous-groupe caractéristique</i>	156
A / <i>Groupe dérivé d'un groupe</i>	156
B / <i>Sous-groupe caractéristique</i>	157
6 / <i>Sous-groupe maximal. Sous-groupe normal maximal</i>	159
Exercices chapitre IV	163
CHAPITRE V / <i>Groupe opérant sur un ensemble</i>	175
1 / <i>Notion de groupe opérant sur un ensemble</i>	175
A / <i>Définitions. Généralités</i>	175
B / <i>Exemples classiques</i>	176
2 / <i>Sous-groupe d'isotropie ou stabilisateur. Orbite</i>	179
A / <i>Définitions. Exemples</i>	179
B / <i>Propriétés des stabilisateurs et des orbites</i>	182
3 / <i>Sous-groupe des points fixes d'un G-ensemble</i>	187
4 / <i>Produit semi-direct</i>	189
Exercices chapitre V	196
CHAPITRE VI / <i>Groupes finis. Théorèmes de Sylow</i>	207
1 / <i>Théorèmes de Sylow</i>	207
A / <i>Premier théorème de Sylow</i>	207
B / <i>Second théorème de Sylow</i>	210
2 / <i>Quelques applications des théorèmes de Sylow</i>	212
Exercices chapitre VI	216

CHAPITRE VII / <i>Suites de composition</i>	225
1 / <i>Théorème de Jordan-Hölder</i>	225
A / Suite de composition	225
B / Théorème de Jordan-Hölder	229
2 / <i>Groupes résolubles</i>	235
A / Définitions et propriétés générales	235
B / Groupes finis résolubles	241
3 / <i>Groupes nilpotents</i>	242
A / Suites centrales. Notion de groupe nilpotent	242
B / Propriétés générales des groupes nilpotents	250
C / Groupes nilpotents finis	254
Exercices chapitre VII	257
CHAPITRE VIII / <i>Groupes abéliens</i>	269
1 / <i>Somme directe de groupes abéliens</i>	270
A / Notion de somme directe de groupes abéliens	270
B / Propriété universelle de la somme directe de groupes abéliens	272
2 / <i>Groupes abéliens libres</i>	277
A / Caractérisation des groupes abéliens libres	277
B / Rang d'un groupe abélien libre	280
C / Propriété universelle d'un groupe abélien libre ...	284
D / Sous-groupe d'un groupe abélien libre	287
3 / <i>Groupes abéliens de torsion</i>	293
A / Groupes de torsion, sans torsion, mixtes	293
B / Composante p -primaire d'un groupe abélien de torsion	295
4 / <i>Groupes abéliens de type fini</i>	298
A / Sous-groupe d'un groupe abélien de type fini	298
B / Décomposition canonique d'un groupe abélien de type fini	306
Exercices chapitre VIII	322
CHAPITRE IX / <i>Groupes libres. Générateurs et relations. Produit libre de groupes</i>	329
1 / <i>Groupe libre</i>	329
A / Construction d'un groupe libre	329
B / Propriété universelle d'un groupe libre	338

2 / <i>Générateurs et relations</i>	341
A / Présentation	341
B / Rang d'un groupe libre	343
3 / <i>Sous-groupes d'un groupe libre</i>	345
A / Préliminaires	346
B / Transversales d'un sous-groupe dans un groupe ...	348
C / Preuve du théorème de Nielsen-Schreier.....	354
D / Rang d'un sous-groupe d'un groupe libre	355
4 / <i>Produit libre de groupes</i>	356
A / Construction d'un produit libre de groupes	357
B / Propriété universelle du produit libre de groupes...	360
Exercices chapitre IX	364
RÉFÉRENCES BIBLIOGRAPHIQUES	369
INDEX	373

Préface

La notion de groupe a été introduite explicitement en mathématiques, au début du dix-neuvième siècle. Elle intervient en effet à cette époque, pour la première fois, dans les travaux relatifs aux équations algébriques, sous forme de groupes de permutations des racines de ces équations ; il s'agissait donc de groupes finis. C'est en exploitant cette idée qu'Evariste Galois obtient en 1832 ses résultats définitifs sur la résolution « par radicaux » des équations polynomiales, qui constituent le fondement de ce qu'on développera plus tard sous le nom de théorie de Galois [44, 68] ⁽¹⁾.

A peu près au même moment, des groupes sont mis en évidence en géométrie, notamment, des groupes de symétries de polygones ou polyèdres réguliers (ce sont encore des groupes finis), puis des groupes (finis ou non) de transformations du plan ou de l'espace. Ces familles de groupes ainsi que leurs généralisations et leurs applications seront ultérieurement, à la base, d'une part, de la théorie de la représentation linéaire des groupes, en particulier des groupes finis [55, 66], et, d'autre part, de la définition et de l'étude des groupes classiques [19, 22].

Ainsi, c'est à partir de cette double origine, algébrique et géométrique, qu'a été conçue, vers la fin du dix-neuvième siècle, la notion abstraite de groupe et que, progressivement, a été construite la théorie des groupes, dont les applications et les prolongements dans le reste des mathématiques sont maintenant considérables.

Dans la théorie des groupes, une place importante a été accordée à l'analyse de la structure des groupes finis, compte tenu des nombreuses interprétations concrètes qui peuvent en être données. Au cours de ces dernières années, plusieurs problèmes relatifs aux groupes simples finis ont particulièrement animé

(1) Les chiffres entre crochets renvoient aux références bibliographiques, p. 369 et s.

le monde des chercheurs et les résultats décisifs les concernant ont été obtenus aux alentours de 1980 [3, 17] (v. infra, chap. IV).

D'une façon générale, l'« idée » de groupe s'est avérée extrêmement fructueuse pour l'ensemble des mathématiques, où elle se retrouve souvent intimement associée à des concepts très divers comme, par exemple, en topologie algébrique, dans les groupes topologiques, les groupes d'homologie et les groupes d'homotopie ⁽²⁾, et en géométrie différentielle dans les groupes de Lie ⁽³⁾.

Par ailleurs, on peut constater que le champ d'application des groupes a très largement dépassé le domaine des mathématiques au sens restreint, en permettant notamment l'interprétation et l'explication de nombreux phénomènes physiques. C'est ainsi que la théorie de la représentation linéaire des groupes finis est utilisée à propos de questions liées aux symétries des cristaux et des molécules, et que les groupes semi-simples (issus des groupes de Lie) ont été introduits en physique théorique (théorie de la relativité et mécanique quantique). De même, la théorie des groupes classiques [19] est à la base de l'étude des particules élémentaires.

Enfin, les applications des groupes à la théorie des plans d'expérience en statistique mathématique [20] montrent que, aujourd'hui, la notion de groupe intéresse toutes les sciences expérimentales ⁽⁴⁾.

⁽²⁾ M. Zisman, *Topologie algébrique élémentaire*, Armand Colin, coll. « U », 1972.

⁽³⁾ D. Leborgne, *Calcul différentiel et géométrie*, PUF, 1982.

⁽⁴⁾ S. Vajda, *The mathematics of experimental design*, Londres, Griffin, 1967.

Introduction

Ce livre est tout particulièrement destiné aux étudiants (1^{er} et 2^e cycle) et aux élèves des classes préparatoires. Il est conçu de manière à pouvoir être abordé à un niveau élémentaire et de façon à permettre ultérieurement d'entreprendre l'étude de tout domaine scientifique nécessitant des connaissances générales sur les groupes, et, plus précisément, dans le champ même de la théorie des groupes, à autoriser l'accès à des études plus approfondies et plus spécialisées.

Pour permettre à un étudiant de travailler éventuellement seul, les démonstrations ont été volontairement très détaillées. A la fin de chaque chapitre, de nombreux exercices doivent permettre le contrôle des connaissances acquises, et fournissent l'occasion d'une ouverture vers certaines applications de la théorie.

Ce volume comprend 9 chapitres qui correspondent, approximativement, aux niveaux d'études suivants :

Chapitres I à III : 1^{er} cycle des Universités et classe de Mathématiques supérieures;

Chapitres IV à VI : licence de Mathématiques et classe de Mathématiques spéciales;

Chapitres VII à IX : maîtrise de Mathématiques.

Nous serons éventuellement amenés à utiliser, dès les premiers chapitres, les structures d'anneau et de corps qui sont directement

liées à celle de groupe. Nous en rappelons donc, ci-dessous, les définitions (elles ne font appel qu'à des notions définies dans le 1^{er} paragraphe du Chapitre Premier).

Définition (0.1) : On appelle *anneau* tout ensemble non vide A , muni de deux lois de composition internes, en général notées l'une multiplicativement et l'autre additivement, vérifiant les conditions suivantes :

(A_1) : A est un groupe abélien par rapport à l'addition (dont l'élément neutre est noté 0).

(A_2) : La multiplication est associative.

(A_3) : La multiplication est distributive à droite et à gauche par rapport à l'addition.

— Un anneau A est dit *unitaire* s'il possède un élément neutre pour la multiplication (appelé élément unité et souvent noté 1_A).

— Un anneau est *commutatif*, si la multiplication est commutative.

Définition (0.2) : On appellera *corps* tout anneau commutatif et unitaire K , tel que $1_K \neq 0$ et dans lequel tout élément non nul est inversible.

Nous supposons connues les définitions et les propriétés algébriques élémentaires des nombres entiers, rationnels, réels et complexes (voir, par exemple, [11]).

PRINCIPALES NOTATIONS

A et B étant deux ensembles :

$$A \setminus B = \{x \in A; x \notin B\}$$

\emptyset ensemble vide

$f: A \rightarrow B$ application de A dans B

$$x \mapsto f(x)$$

$|A|$ ou $\text{card}(A)$: cardinal de A

$|A| < \infty$: A ensemble fini

$$A \times B = \{(x, y); x \in A, y \in B\}$$

N ($\text{resp}^t N^*$), 18

Z ($\text{resp}^t Z^*$), 18

Q ($\text{resp}^t Q^*$), 23

R ($\text{resp}^t R^*$), 23

C ($\text{resp}^t C^*$), 23

Q_+^* , 32

R_+^* , 32

$\frac{Z}{(n)}$, 24

S_E , 25

S_n , 25

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}, 26$$

Q_8 , 27

$\mathcal{J}(n)$, 33

G désigne un groupe quelconque :

$H \leq G$ ($\text{resp}^t H < G$), 30

(e) , 35

$\langle S \rangle$, 35

$\langle x \rangle$, 35

$o(G)$ ou $|G|$, 19

$o(x)$, 36

HK, 37

$Z(G)$, 34

Si G et G' sont deux groupes :

$\text{Hom}(G, G')$, 41

$\text{Im } f$, 43

$\text{Ker } f$, 43

$G \simeq G'$, 46

$\text{End}(G)$, 41

$\text{Aut}(G)$, 47

$\text{Int}(G)$, 48

$G_1 \times G_2$, 54

$\prod_{i \in I} G_i$, 59

Si H est un sous-groupe de G :

\mathcal{R}_H ($\text{resp}^t {}_H\mathcal{R}$), 71

Hx ($\text{resp}^t xH$), 71

$\left(\frac{G}{\overline{H}}\right)_a$ ($\text{resp}^t \left(\frac{G}{\overline{H}}\right)_o$), 73

$[G : H]$, 76

$H < G$, 137

$\frac{G}{\overline{H}}$, 82-137

$x \equiv y \pmod{H}$, 137

$GL(E)$, 27	$C_G(x)$, 64
$SL(E)$, 138	$[x, y]$, 156
$PSL(E)$, 139	$D(G)$, 156
$GO(E)$, 33	$D_i(G)$, 157
$O(E)$, 45	$H \sqsubset G$, 157
$O^+(E)$, 143	$\Phi(G)$, 162
$GL(n, K)$, 27	G_x ou $\text{Stab}_G(x)$, 179
$SL(n, K)$, 45	Ω_x , 179
$PSL(n, K)$, 139	E_G ou $\text{Fix}_E(G)$, 187
$\mathcal{D}(2)$, 87	$N \times_{\varphi} H$, 192
\mathbb{Z}	$\text{Hol}(N)$, 195
$\overline{n\mathbb{Z}}$ ou \mathbb{Z}_n , 74	$\text{long}(G)$, 233
C_n , 103	$[X, Y]$, 243
$(a, b) = 1$, 97	Γ_k , 244
$\varphi(n)$, 99	Z_i , 246
$\text{supp}(\sigma)$, 106	$\bigoplus_{i \in I} G_i$, 271
$\Omega_{\sigma}(i)$, 107	$\bigoplus_{i \in I} H_i$, 40
(j_1, j_2, \dots, j_r) , 108	G^I , 271
(j_1, j_2) , 109	$G^{(n)}$, 271
$\varepsilon(\sigma)$, 115	$F_{(X)}$, 278
A_n , 120	$T(G)$, 294
D_n , 121	F_X , 336
D_{∞} , 172	$(G \mid R)$, 342
$C_{p^{\infty}}$, 171	$\coprod_{i \in I} G_i$, 359
$N_G(S)$, 146	
$C_G(S)$, 64	
$N_G(x)$, 146	

CHAPITRE PREMIER

Structure de groupe

1 — Notion de groupe

A / Loi de composition interne

Définitions (1.1) : Etant donné un ensemble E , on appelle *loi de composition interne* sur E toute application de $E \times E$ dans E , où $E \times E = \{(x, y); x \in E \text{ et } y \in E\}$.

Supposons $E \neq \emptyset$ et désignons par (E, \cdot) l'ensemble E muni de la loi de composition définie par l'application :

$$(x, y) \mapsto x \cdot y.$$

a) Dans E , la loi \cdot est dite :

associative si, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, quels que soient x, y, z dans E ;

commutative si, $x \cdot y = y \cdot x$, quels que soient x, y dans E .

b) S'il existe $e \in E$ tel que, quel que soit $x \in E$,

$$x \cdot e = e \cdot x = x,$$

on dit que e est *élément neutre* dans (E, \cdot) .

c) Si (E, \cdot) possède un élément neutre e , alors un élément $x \in E$ est dit *symétrisable*, s'il existe $x' \in E$ tels que :

$$x' \cdot x = x \cdot x' = e;$$

x' est alors appelé *symétrique* de x dans (E, \cdot) .

Remarque (1.2) : Si un élément neutre e existe dans (E, \cdot) , il est unique et il est son propre symétrique.

En effet, supposons e et e_1 éléments neutres dans (E, \cdot) , e élément neutre $\Rightarrow e_1 \cdot e = e_1$; e_1 élément neutre $\Rightarrow e_1 \cdot e = e$, d'où $e_1 = e$.

D'autre part, $e \cdot e = e$ implique e symétrique de e .

Exemples : Soit $N = \{0, 1, 2, \dots\}$ l'ensemble des entiers naturels et Z l'ensemble des entiers rationnels (entiers positifs, négatifs ou nul).

Dans N et dans Z les opérations habituelles d'addition et de multiplication sont des lois de composition internes associatives et commutatives; 0 et 1 sont, respectivement, élément neutre pour l'addition et pour la multiplication.

Dans $(N, +)$, aucun élément non nul n'est symétrisable.

Dans (N, \times) , aucun élément différent de 1 n'est symétrisable.

Dans $(Z, +)$, tout élément est symétrisable ($-x$ est symétrique de x).

Dans (Z, \times) , seuls 1 et -1 sont symétrisables.

B / Groupe

Définition (1.3) : Soit G un ensemble non vide, muni d'une loi de composition interne définie par : $(x, y) \mapsto x \cdot y$.

On dit que la loi \cdot définit sur G une *structure de groupe*, ou que G est un *groupe* relativement à cette loi, si les trois axiomes suivants sont vérifiés :

(G_1) : la loi \cdot est associative;

(G_2) : il existe dans (G, \cdot) un élément neutre e ;

(G_3) : tout élément de (G, \cdot) est symétrisable.

Remarques (1.4) :

1° D'après la remarque (1.2), un groupe G a un *unique élément neutre* e .

2° Dans un groupe G , tout élément x a un *unique symétrique* x' . Supposons x' et x'_1 symétriques de x dans le groupe (G, \cdot) .

$$x' \cdot x = e \Rightarrow (x' \cdot x) \cdot x'_1 = x'_1; \quad x \cdot x'_1 = e \Rightarrow x' \cdot (x \cdot x'_1) = x';$$

la loi \cdot étant associative (axiome (G_1)), on a $x'_1 = x'$.

Définition (1.5) : Un groupe G est dit *abélien* ⁽¹⁾ (ou *commutatif*) si la loi de composition interne de G est commutative.

Exemple : $(\mathbb{Z}, +)$ est un groupe abélien dont l'élément neutre est 0. Nous verrons plus loin d'autres exemples de groupes, dont certains ne sont pas abéliens.

Remarque (1.6) : Pour deux éléments x et y d'un groupe non abélien (G, \cdot) , on a en général $x \cdot y \neq y \cdot x$. Cependant, si $y = e$, on a $x \cdot e = e \cdot x$, quel que soit $x \in G$; la commutativité peut donc être vérifiée pour certains couples d'éléments.

Définition (1.7) : Dans un ensemble (E, \cdot) , on dit que deux éléments x et y *commutent* (ou sont *permutables*) si $x \cdot y = y \cdot x$.

Par exemple, dans un groupe quelconque (G, \cdot) , on a vu que l'élément neutre commute avec tout élément de G ; d'autre part, pour tout $x \in G$, x et son symétrique x' commutent.

Définition (1.8) : Un groupe G est dit *fini* s'il n'a qu'un nombre fini d'éléments. Dans ce cas, le cardinal de G s'appelle *l'ordre du groupe* G ; il est noté $o(G)$ (ou $|G|$).

Remarque (1.9) : Par analogie avec les notations utilisées dans les ensembles de nombres pour les opérations habituelles de multiplication et d'addition, la loi de composition interne d'un groupe G sera couramment notée

« multiplicativement » : $(x, y) \mapsto xy$

ou « additivement » : $(x, y) \mapsto x + y$.

Dans le premier cas, xy s'appelle le *produit* de x et y pris dans cet ordre; l'élément neutre se note, en général, e ou 1 et s'appelle *l'élément unité* du groupe; le symétrique d'un élément $x \in G$ s'écrit x^{-1} et est appelé *inverse* de x ; en abrégé, on dira que le groupe G est « *multiplicatif* ».

Dans le second cas, $x + y$ s'appelle la *somme* de x et y pris dans cet ordre; l'élément neutre est en général noté 0; le symétrique

(1) Du nom du mathématicien norvégien N. H. Abel (1802-1829).

de $x \in G$ s'écrit $-x$ et est appelé *opposé* de x ; en abrégé, on dira que le groupe G est « *additif* ».

C'est la notation multiplicative que nous adopterons pour énoncer et démontrer les propriétés générales des groupes.

Cependant, selon l'usage, c'est la notation additive qui sera employée pour l'étude des groupes abéliens (chap. VIII).

C / Règles de calcul dans un groupe

Ces règles sont la conséquence des axiomes (G_1) , (G_2) , (G_3) .

Dans tout ce paragraphe, G désigne un groupe multiplicatif, dont l'élément unité est noté e .

a) *Produit, dans G , de n éléments x_1, x_2, \dots, x_n pris dans cet ordre ($n \geq 2$ dans N).* Pour $n = 2$, $x_1 x_2$ est défini par la donnée de la multiplication du groupe G . Pour $n = 3$, l'axiome d'associativité (G_1) autorise à désigner $(x_1 x_2) x_3$ et $x_1 (x_2 x_3)$ par un unique symbole $x_1 x_2 x_3$ représentant par définition le produit, dans le groupe G , de x_1, x_2, x_3 pris dans cet ordre.

Pour $n > 3$, nous allons montrer par récurrence comment, grâce à l'axiome (G_1) , on peut « supprimer ou mettre des parenthèses » et par suite définir, sans ambiguïté, le produit de x_1, x_2, \dots, x_n .

Supposons donc $n > 3$; l'hypothèse de récurrence est la suivante : pour tout entier r ($2 \leq r < n$), on peut écrire

$$x_1 x_2 \dots x_r = (x_1 x_2 \dots x_s) (x_{s+1} x_{s+2} \dots x_r), \\ \forall s \ (1 \leq s < r).$$

Démontrons alors que, quels que soient les entiers r et s tels que $1 \leq s < r < n$, on a :

$$(x_1 x_2 \dots x_r) (x_{r+1} x_{r+2} \dots x_n) \\ = (x_1 x_2 \dots x_s) (x_{s+1} x_{s+2} \dots x_n) \quad (1)$$

Désignons par z le premier membre de (1); l'hypothèse de récurrence implique

$$z = [(x_1 x_2 \dots x_s) (x_{s+1} x_{s+2} \dots x_r)] (x_{r+1} x_{r+2} \dots x_n)$$

L'application de l'axiome (G_1) donne

$$z = (x_1 x_2 \dots x_s) [(x_{s+1} x_{s+2} \dots x_r) (x_{r+1} x_{r+2} \dots x_n)].$$

En réappliquant l'hypothèse de récurrence au produit entre crochets, on obtient

$$z = (x_1 x_2 \dots x_s) (x_{s+1} x_{s+2} \dots x_n),$$

d'où l'égalité (1).

Ce résultat autorise la « suppression des parenthèses » dans l'expression de z et $z = x_1 x_2 \dots x_n$ est par définition le produit, dans le groupe G , de x_1, x_2, \dots, x_n pris dans cet ordre.

b) Puissance n -ième d'un élément ($n \geq 1$ dans N). Soit $x \in G$; on pose

$$xx = x^2$$

$$(xx)x = x(xx) = x^3$$

et, d'une façon générale, pour tout $n \geq 1$ dans N , x^n est obtenu en remplaçant, pour tout i ($1 \leq i \leq n$), x_i par x dans $x_1 x_2 \dots x_n$.

On en déduit que, quels que soient les entiers positifs m et n ,

$$x^m x^n = x^{m+n} = x^n x^m \quad (2)$$

$$\text{et} \quad (x^m)^n = x^{mn} = (x^n)^m. \quad (3)$$

Remarques (1.9) :

1° Si le groupe G n'est pas abélien, pour x et y dans G , on a, en général

$$(xy)^n \neq x^n y^n.$$

Cependant, si x et y commutent, alors

$$(xy)^n = xy xy \dots xy = x^n y^n \quad (4)$$

$$\text{et} \quad x^m y^n = y^n x^m$$

2° Le calcul du produit d'un nombre quelconque d'éléments de G , ainsi que de la puissance n -ième d'un élément, résulte uniquement de l'application de l'axiome (G_1) ; ces règles de calcul sont donc valables dans tout ensemble non vide muni d'une loi de composition interne associative; un tel ensemble est appelé un *demi-groupe*.

Un demi-groupe avec élément neutre est un *monoïde* (ou demi-groupe unitaire). Par exemple, $(N, +)$ et (N, \times) sont des monoïdes; tout groupe est *a fortiori* un monoïde.

3° En notation additive, les formules (2) et (3) s'écrivent respectivement :

$$mx + nx = (m + n)x \quad (2')$$

$$n(mx) = nm x \quad (3')$$

c) *Règle de simplification.* Dans un groupe G tout élément a est *simplifiable à droite et à gauche*, c'est-à-dire que, pour x et y dans G ,

$$xa = ya \Rightarrow x = y \quad \text{et} \quad ax = ay \Rightarrow x = y.$$

En effet, si a^{-1} est l'inverse de a ,

$$xa = ya \Rightarrow (xa) a^{-1} = (ya) a^{-1}, \quad \text{d'où } x = y;$$

on justifie de même la règle de simplification à gauche.

On en déduit que, si a et b sont donnés dans G , les équations

$$ax = b \quad \text{et} \quad ya = b$$

ont chacune une solution *unique* dans G , respectivement,

$$x = a^{-1}b \quad \text{et} \quad y = ba^{-1}.$$

d) *Inverse d'un produit.*

Remarque (1.10) : Si, pour $x \in G$, il existe x' (resp^t x'') dans G tel que $xx' = e$ (resp. $x''x = e$), alors $x' = x^{-1}$ (resp^t $x'' = x^{-1}$).

En effet,

$$xx' = e \Rightarrow x^{-1}(xx') = x^{-1}e,$$

$$\text{mais} \quad x^{-1}(xx') = (x^{-1}x)x' = ex' = x'$$

(même raisonnement avec x'').

Compte tenu de la remarque ci-dessus, on a, quels que soient x et y dans G :

$$(xy)^{-1} = y^{-1}x^{-1} \quad (5)$$

puisque $(xy)y^{-1}x^{-1} = x(yy^{-1}x^{-1}) = xx^{-1} = e$.

Remarque (1.11) : Si x et y ne commutent pas, on a $x^{-1}y^{-1} \neq (xy)^{-1}$; par contre, si x et y commutent, alors x^{-1} et y^{-1} aussi, car, dans ce cas

$$x^{-1}y^{-1} = (yx)^{-1} = (xy)^{-1} = y^{-1}x^{-1}.$$

Par récurrence sur n , on vérifie facilement que pour tout $n \geq 2$ dans \mathbf{N} et x_i dans G ($1 \leq i \leq n$),

$$(x_1 x_2 \dots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \dots x_1^{-1} \quad (6)$$

En particulier, pour $x \in G$, $(x^n)^{-1} = (x^{-1})^n$ et on écrira :

$$(x^n)^{-1} = x^{-n} \quad (7)$$

D'autre part, pour tout $x \in G$, on pose

$$x^0 = e \quad (8)$$

On vérifie alors aisément que les formules (2) et (3) sont valables quels que soient m et n dans \mathbf{Z} .

D / Premiers exemples de groupes

Exemple (1.12) : Groupes de nombres.

Nous avons déjà signalé que $(\mathbf{Z}, +)$ était un groupe abélien.

\mathbf{Q} , \mathbf{R} et \mathbf{C} désignant respectivement l'ensemble des nombres rationnels, réels et complexes, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ et $(\mathbf{C}, +)$ sont des groupes abéliens d'élément neutre 0.

Posons $\mathbf{Q}^* = \mathbf{Q} - \{0\}$ et définissons de même \mathbf{R}^* et \mathbf{C}^* ; alors (\mathbf{Q}^*, \times) , (\mathbf{R}^*, \times) et (\mathbf{C}^*, \times) sont des groupes abéliens d'élément neutre 1. On remarque que (\mathbf{Q}, \times) , par exemple, n'est pas un groupe, car 0 n'a pas d'inverse dans \mathbf{Q} .

Exemple (1.13) : Groupe des classes de congruence de \mathbf{Z} , modulo n .

Rappelons tout d'abord qu'étant donné un ensemble non vide E et une relation binaire \mathcal{R} définie dans E on dit que \mathcal{R} est une *relation d'équivalence* si \mathcal{R} est :

réflexive : $x \mathcal{R} x$, quel que soit $x \in E$,

symétrique : $x \mathcal{R} y \Rightarrow y \mathcal{R} x$, quels que soient x, y dans E ,

transitive : $x \mathcal{R} y$ et $y \mathcal{R} z \Rightarrow x \mathcal{R} z$, quels que soient x, y, z dans E .

A tout $x \in E$, on associe alors sa *classe d'équivalence* modulo \mathcal{R} : $\text{cl}_{\mathcal{R}}(x)$, souvent notée \bar{x} , lorsqu'il n'y a pas d'ambiguïté possible; avec cette notation :

$$\bar{x} = \{y \in E; y \mathcal{R} x\} \quad \text{et} \quad y \in \bar{x} \Leftrightarrow \bar{y} = \bar{x}.$$

Les classes distinctes de E modulo \mathcal{R} forment une partition de E ; l'ensemble de ces classes s'appelle l'*ensemble quotient* de E par la relation d'équivalence \mathcal{R} , on le note $\frac{E}{\mathcal{R}}$.

Etant donné $C \in \frac{E}{\mathcal{R}}$, pour tout $x \in C$, on peut écrire $C = \bar{x}$; autrement dit, tout élément $x \in C$ peut être choisi comme *représentant* de la classe d'équivalence C .

Si $\{x_i\}_{i \in I}$ est une famille de représentants des classes distinctes de E modulo \mathcal{R} , on pourra écrire

$$\frac{E}{\mathcal{R}} = \{\bar{x}_i; i \in I\}.$$

Soit $n > 0$ dans \mathbf{Z} . Deux éléments x et y de \mathbf{Z} sont dits *congrus modulo n* si $x - y$ est un multiple de n dans \mathbf{Z} . Symboliquement, on écrit

$$x \equiv y \pmod{n}$$

$$\text{et} \quad x \equiv y \pmod{n} \Leftrightarrow \exists k \in \mathbf{Z}, \quad x - y = kn.$$

L'existence de la division euclidienne dans \mathbf{Z} implique que pour tout $x \in \mathbf{Z}$ il existe q et r dans \mathbf{Z} , tels que

$$x = nq + r \quad \text{avec } 0 \leq r < n;$$

$$\text{donc} \quad \bar{x} = \bar{r} \quad \text{où } 0 \leq r < n.$$

On en déduit que $\{0, 1, \dots, n-1\}$ forme une famille de représentants des classes distinctes modulo n .

L'ensemble quotient de \mathbf{Z} par la congruence modulo n est noté $\frac{\mathbf{Z}}{(n)}$, d'où :

$$\frac{\mathbf{Z}}{(n)} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}. \quad (9)$$

Montrons que la correspondance λ définie par

$$\begin{aligned} \lambda: \frac{\mathbf{Z}}{(n)} \times \frac{\mathbf{Z}}{(n)} &\rightarrow \frac{\mathbf{Z}}{(n)} \\ (\bar{x}, \bar{y}) &\mapsto \overline{x+y} \end{aligned}$$

est une *application*; il s'agit de prouver que

$$\bar{x}' = \bar{x} \text{ et } \bar{y}' = \bar{y} \Rightarrow \overline{x' + y'} = \overline{x + y}.$$

$$\bar{x}' = \bar{x} \Leftrightarrow \exists k \in \mathbf{Z}, \quad x' - x = kn,$$

$$\bar{y}' = \bar{y} \Leftrightarrow \exists l \in \mathbf{Z}, \quad y' - y = ln;$$

alors $(\bar{x}' = \bar{x} \text{ et } \bar{y}' = \bar{y}) \Rightarrow x' + y' - (x + y) = (k + l)n$,

donc $\overline{x' + y'} = \overline{x + y}$.

L'application $(\bar{x}, \bar{y}) \mapsto \overline{x + y}$ définit une loi de composition interne dans $\frac{\mathbf{Z}}{(n)}$, induite par l'addition du groupe \mathbf{Z} .

Cette loi est encore notée $+$ et quels que soient \bar{x}, \bar{y} dans $\frac{\mathbf{Z}}{(n)}$, on a :

$$\bar{x} + \bar{y} = \overline{x + y}$$

$(\mathbf{Z}, +)$ étant un groupe abélien, on vérifie facilement qu'il en est de même de $\left(\frac{\mathbf{Z}}{(n)}, +\right)$; $\bar{0}$ est l'élément neutre de ce groupe; l'opposé d'un élément \bar{x} est $-\bar{x} = \overline{-x}$.

En conclusion (compte tenu de (9)) : le groupe $\frac{\mathbf{Z}}{(n)}$ des classes de congruence de \mathbf{Z} modulo n est un groupe abélien fini d'ordre n .

Nous verrons plus loin (exemple (2.5)) une autre interprétation de ce groupe.

Exemple (1.14) : Groupes symétriques.

Soit E un ensemble non vide; notons S_E l'ensemble des *permutations* de E (c'est-à-dire des bijections de E dans lui-même). On sait que si f et g sont deux éléments de S_E , alors $f \circ g \in S_E$.

La composition des applications est donc une loi de composition interne dans S_E ; or cette loi est associative et si id_E désigne l'application « identité » de E , on a :

$$\text{id}_E \circ f = f \circ \text{id}_E = f, \quad \text{pour tout } f \in S_E;$$

de plus, toute permutation f de E admet une application réciproque f^{-1} qui est aussi une permutation de E et qui vérifie $f^{-1} \circ f = f \circ f^{-1} = \text{id}_E$.

On en déduit que (S_E, \circ) est un groupe.

Le groupe S_E est appelé *groupe symétrique de E* .

Si $E = \{1, 2, \dots, n\}$, le groupe symétrique S_E est noté S_n et s'appelle le *groupe symétrique de degré n* .

On sait, d'après un résultat d'analyse combinatoire (voir par

exemple [16]), que le nombre des permutations d'un ensemble de n éléments est $n!$; par suite :

S_n est un groupe fini d'ordre $n!$.

Notations (1.15) : Un élément $\sigma \in S_n$ s'écrit :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Ainsi, les 6 éléments de S_3 peuvent s'écrire :

$$\begin{aligned} e &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \sigma_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \tau_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & \tau_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, & \tau_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{aligned}$$

Pour σ et τ dans S_n , $\sigma \circ \tau$ est appelé produit de τ par σ dans S_n et

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma \circ \tau(1) & \sigma \circ \tau(2) & \dots & \sigma \circ \tau(n) \end{pmatrix},$$

où $\sigma \circ \tau(i) = \sigma(\tau(i))$.

Par exemple, dans S_3 :

$$\sigma_1 \circ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2, \quad \tau_3 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \tau_1.$$

On remarque que l'on a $\sigma_1 \circ \tau_3 \neq \tau_3 \circ \sigma_1$, donc le groupe S_3 est non abélien; on en déduit que, pour tout $n \geq 3$, le groupe symétrique S_n est non abélien. En effet, si $n > 3$, considérons σ et τ dans S_n tels que les restrictions de σ et τ à $\{1, 2, 3\}$ soient respectivement σ_1 et τ_3 et tels que $\sigma(i) = \tau(i) = i$, pour tout $i \in \{4, \dots, n\}$; on a alors $\sigma \circ \tau \neq \tau \circ \sigma$.

D'une façon générale, pour tout ensemble non vide E tel que $\text{card } E > 2$, le groupe symétrique S_E est non abélien.

Si $n = 2$, $S_2 = \{e, \tau\}$ où $e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

Le groupe S_2 est donc abélien et $\tau^2 = e \Rightarrow \tau^{-1} = \tau$.

Une étude détaillée des groupes symétriques S_n sera faite au chapitre III.

Exemple (1.16) : Le groupe des quaternions.

On vérifiera que l'ensemble des 8 matrices ci-dessous, dans lesquelles i est le nombre complexe tel que $i^2 = -1$, est un groupe par rapport à la multiplication des matrices carrées d'ordre 2 sur \mathbb{C} :

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\} \\ \left\{ \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\}.$$

Ce groupe est appelé *groupe des quaternions*, il se note en général Q_8 :

Q_8 est un groupe d'ordre 8, non abélien.

Exemple (1.17) : Groupes linéaires. Groupes de matrices.

E étant un espace vectoriel sur un corps commutatif K , on démontre en algèbre linéaire que l'ensemble des automorphismes K -linéaires de E est un groupe par rapport à la loi \circ de composition des applications.

Ce groupe est appelé *groupe linéaire général de E* et est noté $GL(E)$ [23].

Pour tout entier $n > 0$ et tout corps commutatif K , l'ensemble des matrices carrées d'ordre n inversibles est un groupe par rapport à la multiplication des matrices; ce groupe se note $GL(n, K)$ et est appelé *groupe linéaire général des matrices carrées inversibles d'ordre n sur K* [50]; il est non abélien pour $n \geq 2$.

E / Table de Cayley d'un groupe fini

Soit $E = \{x_1, x_2, \dots, x_n\}$ un ensemble fini de cardinal n . Si E est muni d'une loi de composition interne notée \cdot , il peut être commode, lorsque n n'est pas trop grand, d'écrire les éléments $x_i x_j$ dans un tableau carré à n lignes et n colonnes tel qu'à l'intersection de la i -ème ligne et de la j -ème colonne se trouve l'élément $x_i x_j$.

Ce tableau s'appelle la « table de Cayley » ⁽²⁾, de l'ensemble (E, \cdot) .

⁽²⁾ A. Cayley, mathématicien britannique (1821-1895), ayant le premier suggéré l'écriture de ces tables.

La méthode s'applique en particulier dans le cas des groupes finis; si le groupe est multiplicatif (resp^t additif), la table s'appelle table de multiplication (resp^t d'addition).

Exemple (1.18) :

Tables des groupes (additifs) $\frac{\mathbf{Z}}{(2)}$, $\frac{\mathbf{Z}}{(3)}$, $\frac{\mathbf{Z}}{(4)}$:

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Les trois groupes ci-dessus étant *abéliens*, chacune des tables est *symétrique par rapport à la diagonale principale* du carré (diagonale nord-ouest, sud-est). Cette symétrie n'existe plus dans le cas d'un groupe non abélien, tel qu'en particulier S_3 , dont la table est écrite ci-dessous en tenant compte des notations (1.15) :

0	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_3	τ_1	τ_2
σ_2	σ_2	e	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	e	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	e

(10)

Remarques (1.19) :

1° Un groupe fini peut éventuellement être défini par la donnée d'une table de multiplication. Considérons par exemple la table suivante :

\times	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(11)

L'examen de la 1^{re} ligne et de la 1^{re} colonne montre que e est élément unité; d'autre part, $a^2 = b^2 = c^2 = e$ implique que a, b, c sont inversibles et chacun d'eux est égal à son inverse. La table étant symétrique par rapport à la diagonale principale, la loi de composition considérée est commutative. Il reste à vérifier que la loi est associative, ce qui, ici, ne présente pas de difficultés; ainsi la table (11) définit un groupe abélien d'ordre 4.

2^o Une table de Cayley dont chaque ligne et chaque colonne est formée par les mêmes éléments dans un certain ordre est appelée un carré latin [20].

Dans un groupe, quels que soient a et b , on sait qu'il existe un unique x et un unique y tels que

$$ax = b \quad \text{et} \quad ya = b;$$

on en déduit que la table de multiplication d'un groupe fini est toujours un carré latin; mais la réciproque est fausse, car un carré latin ne vérifie pas toujours la règle d'associativité.

Considérons par exemple le carré latin :

\times	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

(12)

On a $(ab)c = dc = a$ et $a(bc) = ad = c$, la table (12) ne définit donc pas un groupe.

2 — Sous-groupe

Sauf mention contraire, G désigne toujours un groupe multiplicatif d'élément neutre e .

A / Notion de sous-groupe. Propriétés élémentaires

Définition (1.20) : G étant un groupe, une partie non vide H de G est un sous-groupe de G si

$$\begin{cases} (x, y) \in H \times H \Rightarrow xy \in H & (13) \\ x \in H \Rightarrow x^{-1} \in H & (14) \end{cases}$$

Remarques (1.21) :

1° Les conditions (13) et (14) impliquent $e \in H$.

2° Tout sous-groupe H d'un groupe G est un groupe relativement à la loi de composition induite dans H par celle de G .

3° Un groupe ayant plus d'un élément a au moins deux sous-groupes, G et le sous-groupe réduit à l'élément neutre, que l'on notera (e) .

Définition (1.22) : On appelle *sous-groupe propre* d'un groupe G tout sous-groupe de G *distinct* de G .

Dans tout groupe G ayant plus d'un élément, (e) est un sous-groupe propre.

Notations (1.23) : On écrira :

$H \leq G$ pour exprimer que H est un sous-groupe de G ,

$H < G$ si H est un sous-groupe *propre* de G .

THÉORÈME (1.24). *Soit H une partie non vide d'un groupe G , alors H est un sous-groupe de G si et seulement si*

$$\forall (x, y) [(x, y) \in H \times H \Rightarrow xy^{-1} \in H] \quad (15)$$

Preuve :

1° Supposons $H \leq G$; soit $(x, y) \in H \times H$, alors $y \in H \Rightarrow y^{-1} \in H$, d'après (14); par suite

$$(x, y^{-1}) \in H \times H \Rightarrow xy^{-1} \in H, \text{ d'après (13);}$$

on en déduit (15).

2° Supposons (15) vérifié; soit $(x, y) \in H \times H$.

$$x \in H \Rightarrow (x, x) \in H \times H, \quad \text{d'où } xx^{-1} = e \in H;$$

$$e \in H \text{ et } x \in H \Rightarrow (e, x) \in H \times H, \quad \text{d'où } ex^{-1} = x^{-1} \in H;$$

on en déduit que $(15) \Rightarrow (14)$. Par suite,

$$(x, y) \in H \times H \Rightarrow (x, y^{-1}) \in H \times H, \quad \text{d'où } xy \in H,$$

donc $(15) \Rightarrow (13)$.

Remarque : En notation additive, (15) s'écrit :

$$\forall (x, y) [(x, y) \in H \times H \Rightarrow (x - y) \in H] \quad (15')$$

PROPOSITION (1.25). *Soit G un groupe et $\{H_i\}_{i \in I}$ une famille de sous-groupes de G ; alors, quel que soit l'ensemble non vide I , $\bigcap_{i \in I} H_i$ est un sous-groupe de G .*

Démonstration laissée au lecteur.

Remarque (1.26) : En général, $\bigcup_{i \in I} H_i$ n'est pas un sous-groupe de G .

En effet, on peut vérifier, par exemple, que dans le groupe $(\mathbb{Z}, +)$, $3\mathbb{Z} = \{3x; x \in \mathbb{Z}\}$ et $8\mathbb{Z}$ sont des sous-groupes; or $3 + 8 = 11$ et $11 \notin 3\mathbb{Z} \cup 8\mathbb{Z}$, donc $3\mathbb{Z} \cup 8\mathbb{Z}$ n'est pas un sous-groupe de \mathbb{Z} .

On a cependant le résultat suivant :

PROPOSITION (1.27). *Si, dans un groupe G , $\{H_i\}_{i \in I}$ est une famille de sous-groupes totalement ordonnée par l'inclusion, alors $\bigcup_{i \in I} H_i$ est un sous-groupe de G .*

Preuve : Soient x et y dans $\bigcup_{i \in I} H_i$; il existe j et k dans I tels que $x \in H_j$ et $y \in H_k$. La famille des H_i étant totalement ordonnée par l'inclusion, on a $H_j \subseteq H_k$ ou $H_k \subseteq H_j$. Plaçons-nous, par exemple, dans le premier cas; on a alors x et y dans H_k , d'où xy^{-1} dans H_k et par suite $xy^{-1} \in \bigcup_{i \in I} H_i$. On en conclut, d'après le théorème (1.24), que $\bigcup_{i \in I} H_i$ est un sous-groupe de G .

B / Exemples de sous-groupes

Exemple (1.28) : Sous-groupe de $(\mathbb{Z}, +)$.

Pour tout entier $n \in \mathbb{N}$, $n\mathbb{Z} = \{nx; x \in \mathbb{Z}\}$ est un sous-groupe de \mathbb{Z} et tout sous-groupe de \mathbb{Z} est de cette forme.

On vérifie facilement que pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de \mathbb{Z} . Montrons que, quel que soit H sous-groupe de \mathbb{Z} , il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Si $H = (0)$, $H = 0\mathbb{Z}$; supposons $H \neq (0)$. Il existe $x \neq 0$ dans H ; $x \in H$ implique $-x \in H$; on en déduit qu'il existe au moins un entier strictement positif dans H . Posons

$E = \{x \in H; x > 0\}$; E est une partie non vide de N , donc il existe dans E un plus petit élément n ; on en déduit que $n\mathbb{Z} \subseteq H$.

D'autre part, soit $x \in H$; supposons $x > 0$, alors $x \in E$, donc $x \geq n$. La division euclidienne dans \mathbb{Z} permet d'écrire :

$$x = nq + r, \quad \text{avec } q \text{ et } r \text{ dans } \mathbb{Z} \quad \text{et} \quad 0 \leq r < n.$$

$$n \in H \Rightarrow nq \in H, \quad \text{par suite } x - nq = r \in H.$$

Or on a $0 \leq r < n$ et n est le plus petit entier positif contenu dans H , donc $r = 0$ et $x \in n\mathbb{Z}$; on en conclut que $H = n\mathbb{Z}$.

D'autre part, m et n entiers positifs et $m\mathbb{Z} = n\mathbb{Z}$ implique $m = n$, d'où l'unicité de l'entier n tel que $H = n\mathbb{Z}$.

Exemples (1.29) :

1° Les groupes additifs \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} sont tels que

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C} \quad (\text{notation (1.23)}).$$

2° Les groupes multiplicatifs \mathbb{Q}^* , \mathbb{R}^* , \mathbb{C}^* vérifient :

$$\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*.$$

3° Si $\mathbb{Q}_+^* = \{x \in \mathbb{Q}; x > 0\}$ et $\mathbb{R}_+^* = \{x \in \mathbb{R}; x > 0\}$, on a :

$$\mathbb{Q}_+^* < \mathbb{Q}^*, \quad \mathbb{R}_+^* < \mathbb{R}^* \quad \text{et} \quad \mathbb{Q}_+^* < \mathbb{R}_+^*.$$

Les exemples ci-dessus résultent des propriétés algébriques élémentaires de \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} .

Exemples (1.30): Soit U l'ensemble des *nombre complexes de module 1*; $|z|$ désignant le module de $z \in \mathbb{C}$, on sait que $|zz'| = |z||z'|$ quels que soient z et z' dans \mathbb{C} ; on vérifie alors facilement que U est un sous-groupe multiplicatif \mathbb{C}^* .

D'autre part, pour tout entier $n > 0$, désignons par U_n l'ensemble des *racines n -ième de l'unité dans \mathbb{C}* .

$$\text{On sait que } U_n = \{z_0, z_1, \dots, z_{n-1}\} \text{ où } z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}.$$

On a $z_0 = 1$, $U_n \subset U$ et $\text{card } U_n = n$; d'autre part, quels que soient z_k et $z_{k'}$ dans U_n :

$$(z_k^n = 1 \text{ et } z_{k'}^n = 1) \Rightarrow (z_k z_{k'})^n = 1$$

$$\text{et } z_k^n = 1 \Rightarrow (z_k^{-1})^n = 1;$$

par suite, U_n est un sous-groupe fini d'ordre n de U , donc de \mathbb{C}^* .

Exemple (1.31) : Le groupe linéaire général $GL(E)$ d'un espace vectoriel E [exemple (1.17)] est un *sous-groupe du groupe symétrique* S_E .

Exemple (1.32) : Considérons l'espace vectoriel euclidien \mathbf{R}^2 ; le produit scalaire de deux vecteurs x et y de \mathbf{R}^2 étant noté $(x|y)$, on appelle *similitude* de \mathbf{R}^2 tout élément $u \in GL(\mathbf{R}^2)$ tel qu'il existe $\lambda_u \in \mathbf{R}_+^*$ vérifiant :

$$(u(x)|u(y)) = \lambda_u(x|y), \quad \forall (x, y) \in \mathbf{R}^2 \times \mathbf{R}^2 \quad (16)$$

λ_u s'appelle le *rapport à la similitude* u .

On démontre [23] que l'ensemble des similitudes de \mathbf{R}^2 forme un *sous-groupe de* $GL(\mathbf{R}^2)$, noté $GO(\mathbf{R}^2)$ et appelé *groupe des similitudes linéaires de* \mathbf{R}^2 .

Remarque (1.33) :

1° La définition du groupe $GO(\mathbf{R}^2)$ se généralise à celle du groupe $GO(E)$ des similitudes d'un espace vectoriel euclidien E de dimension finie quelconque [23].

2° La notion de similitude peut aussi être envisagée dans le plan affine euclidien ([14] et [23]) et plus généralement dans un espace affine euclidien \mathcal{E} de dimension finie quelconque, d'où la notion de *groupe des similitudes affines* de \mathcal{E} [23].

Exemple (1.34) : Soit P le plan affine euclidien; on désigne par $d(x, y)$ la distance de deux points x et y du plan P . On appelle *isométrie* du plan P toute application $f: P \rightarrow P$ qui conserve les distances, c'est-à-dire telle que :

$$\forall (x, y) \in P \times P, \quad d(f(x), f(y)) = d(x, y).$$

On démontre ([1], exercice 26, chap. I^{er}) que toute isométrie est une bijection, donc appartient au groupe symétrique S_P et que l'ensemble $\mathcal{I}(2)$ de ces isométries est un *sous-groupe de* S_P , appelé *groupes des isométries du plan* P .

On définit de façon analogue le groupe $\mathcal{I}(3)$ des isométries de l'espace affine euclidien de dimension 3 ([1] et [23]), et plus généralement on peut considérer le groupe $\mathcal{I}(n)$ des isométries d'un espace affine euclidien de dimension $n \geq 1$ quelconque [23].

Exemple (1.35) : Centre d'un groupe.

Soit G un groupe quelconque, posons :

$$Z(G) = \{x \in G; xa = ax, \forall a \in G\};$$

$Z(G)$ est l'ensemble des éléments $x \in G$ qui commutent avec tout élément de G . $Z(G)$ est appelé le *centre du groupe G* et on vérifie facilement que *c'est un sous-groupe de G* . On remarque que $Z(G)$ est un sous-groupe *propre* de G si et seulement si G est *non abélien*.

C / Sous-groupe engendré par une partie non vide d'un groupe

Définition (1.36) : Soient G un groupe et S une partie non vide de G ; désignons par \mathcal{H}_S l'ensemble des sous-groupes de G contenant S et posons

$$\langle S \rangle = \bigcap_{H \in \mathcal{H}_S} H.$$

$\langle S \rangle$ est un sous-groupe de G (proposition (1.25)) appelé *sous-groupe de G engendré par S* .

Remarque (1.37) : Dans l'ensemble des sous-groupes de G ordonné par l'inclusion, $\langle S \rangle$ est le *plus petit sous-groupe de G contenant S* .

PROPOSITION (1.38). S étant une partie non vide d'un groupe G , on a :

$$\langle S \rangle = \{x_1 x_2 \dots x_n; n \in \mathbb{N}^*, x_i \in S \text{ ou } x_i^{-1} \in S, \forall i (1 \leq i \leq n)\} \quad (17)$$

Preuve : Désignons par H le second membre de (17) et démontrons que $H = \langle S \rangle$. On remarque que tout x de S appartient à H , d'où $S \subseteq H$.

Montrons que H est un sous-groupe de G . Considérons $x = x_1 x_2 \dots x_n$ et $y = y_1 y_2 \dots y_p$ dans H ; alors

$$xy^{-1} = x_1 x_2 \dots x_n y_p^{-1} y_{p-1}^{-1} \dots y_1^{-1}$$

appartient à H . On en déduit que H est un élément de l'ensemble \mathcal{H}_S , d'où $\langle S \rangle \subseteq H$.

D'autre part, tout sous-groupe de G contenant S contient nécessairement tous les éléments de H , par suite $H = \langle S \rangle$.

Cas particuliers :

1° $S = \bigcup_{i \in I} H_i$, où $\{H_i\}_{i \in I}$ est une famille de sous-groupes de G ; dans ce cas, $x \in S \Leftrightarrow x^{-1} \in S$; par suite

$$\langle S \rangle = \{x_1 x_2 \dots x_n; n \in \mathbf{N}^*, x_\alpha \in \bigcup_{i \in I} H_i, \forall \alpha (1 \leq \alpha \leq n)\} \quad (18)$$

2° $S = \{x\}$, $x \in G$; $\langle S \rangle$ s'écrit alors $\langle x \rangle$ et

$$\langle x \rangle = \{x^n; n \in \mathbf{Z}\} \quad (19)$$

Pour $x = e$, nous conserverons la notation $\langle e \rangle$, à la place de $\langle e \rangle$ (voir remarque (1.21)).

Remarque (1.39) : Si la loi de composition du groupe G est notée *additivement*, les formules (17) et (19) deviennent respectivement :

$$\langle S \rangle = \left\{ \sum_{i=1}^n x_i; n \in \mathbf{N}^*, x_i \in S \text{ ou } -x_i \in S, \forall i (1 \leq i \leq n) \right\} \quad (17')$$

$$\langle x \rangle = \{nx; n \in \mathbf{Z}\} \quad (19')$$

Définitions (1.40) : Soit G un groupe.

1° Si S est une partie non vide de G telle que $\langle S \rangle = G$, on dit que S est une *partie génératrice* du groupe G , ou que S est un *ensemble de générateurs* de G , ou encore que S engendre G .

2° S'il existe $x \in G$ tel que $\langle x \rangle = G$, le groupe G est dit *monogène*.

Plus généralement, s'il existe une partie non vide et finie de G , $S = \{x_1, x_2, \dots, x_n\}$, telle que $\langle S \rangle = G$, on dit que le groupe G est de *type fini*. Un groupe fini est nécessairement de type fini, mais la réciproque est fautive (voir exemple (1.42) 1°).

Exemple (1.41) : Considérons le groupe symétrique S_3 .

$$S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\} \quad (\text{notations (1.15)}).$$

La table (10) montre que $\sigma_1^2 = \sigma_2$ et $\sigma_1^3 = e$, d'où

$$\langle \sigma_1 \rangle = \{ \sigma_1, \sigma_2, e \}.$$

D'autre part, $\sigma_1 \circ \tau_3 = \tau_2$, $\tau_3 \circ \sigma_1 = \tau_1$, par suite

$$\langle \sigma_1, \tau_3 \rangle = \{ \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3, e \} = S_3;$$

donc $\{ \sigma_1, \tau_3 \}$ est une partie génératrice de S_3 .

Exemples (1.42) :

1° Puisque tout $n \in \mathbf{Z}$ s'écrit $1 + 1 + \dots + 1$ si $n > 0$, $(-1) + (-1) + \dots + (-1)$ si $n < 0$ et $0 = 1 + (-1)$, \mathbf{Z} est un groupe monogène engendré par 1.

On remarque que \mathbf{Z} peut aussi être considéré comme engendré par -1 .

2° Considérons le groupe $\frac{\mathbf{Z}}{(4)}$ dont la table d'addition est explicitée dans l'exemple (1.18); celle-ci permet de montrer que le groupe $\frac{\mathbf{Z}}{(4)}$ est monogène engendré par $\bar{1}$ et que $\frac{\mathbf{Z}}{(4)}$ peut aussi être considéré comme engendré par $\bar{3}$; donc $\frac{\mathbf{Z}}{(4)}$ est un groupe monogène fini.

Définition (1.43) : On appellera *groupe cyclique* tout groupe monogène fini.

Les groupes monogènes et en particulier les groupes cycliques seront étudiés en détail au chapitre III.

Définitions (1.44) : Soit G un groupe quelconque et x un élément de G .

a) Si le sous-groupe de G engendré par x est de cardinal infini, on dit que x est d'ordre infini dans G .

b) Si le sous-groupe de G engendré par x est fini, on dit que x est d'ordre fini dans G et le cardinal du sous-groupe $\langle x \rangle$ s'appelle l'ordre de x dans G ; on le note $o(x)$.

Exemples (1.45) :

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

2° Dans \mathbf{Z} , tout élément $x \neq 0$ est d'ordre infini.

3° Dans le groupe symétrique S_3 , τ_1, τ_2, τ_3 sont d'ordre 2 et σ_1, σ_2 sont d'ordre 3 (voir la table (10)).

Remarque (1.46) : Etant donné deux parties non vides X et Y d'un groupe G , on pose :

$$XY = \{xy; (x, y) \in X \times Y\} \quad (20)$$

si $Y = X$, on écrit $X^2 = \{xy; (x, y) \in X \times X\}$.

Si le groupe G est noté additivement, XY est remplacé par

$$X + Y = \{x + y; (x, y) \in X \times Y\} \quad (20')$$

Cas particuliers :

a) $X = \{x\}$, $x \in G$ et $Y = G$; on a alors $XY = xG = G$, car x est inversible et on a aussi $YX = Gx = G$.

b) $X = G = Y$; alors $G^2 = G$.

c) $X < G$ et $Y < G$; l'exemple ci-dessous montre qu'en général on a $XY \neq YX$ et ni XY , ni YX ne sont des sous-groupes de G .

En effet, dans le groupe symétrique S_3 , posons

$$H = \langle \tau_1 \rangle = \{e, \tau_1\} \quad \text{et} \quad K = \langle \tau_2 \rangle = \{e, \tau_2\};$$

alors :

$$HK = \{e, \tau_1, \tau_2, \tau_1 \circ \tau_2 = \sigma_1\}$$

$$\text{et} \quad KH = \{e, \tau_1, \tau_2, \tau_2 \circ \tau_1 = \sigma_2\}.$$

$$\sigma_1 \neq \sigma_2 \Rightarrow HK \neq KH.$$

$$\sigma_1^{-1} = \sigma_2 \quad \text{et} \quad \sigma_2 \notin HK; \quad \sigma_2^{-1} = \sigma_1 \quad \text{et} \quad \sigma_1 \notin KH,$$

par suite ni HK , ni KH ne sont des sous-groupes de G .

Cette remarque justifie l'intérêt du résultat suivant :

PROPOSITION (1.47). *H et K étant deux sous-groupes d'un groupe G , alors HK est un sous-groupe de G si et seulement si $HK = KH$.*

Preuve :

1° Supposons $HK \leq G$. Soit $x \in H$ et $y \in K$, on peut écrire

$$yx = (x^{-1}y^{-1})^{-1}$$

yx est l'inverse d'un élément du sous-groupe HK , donc $yx \in HK$, d'où $KH \subseteq HK$.

Soit $z \in HK$, alors $z^{-1} \in HK$, donc il existe $x' \in H$ et $y' \in K$ tels que $z^{-1} = x'y'$; par suite $z = y'^{-1}x'^{-1} \in KH$, d'où $HK \subseteq KH$.

On en conclut que HK sous-groupe de G implique $HK = KH$.

2° Réciproquement, supposons $HK = KH$; on remarque que $e \in HK$ implique $HK \neq \emptyset$. Soient x et x_1 dans H , y et y_1 dans K ;

$$(xy)(x_1y_1)^{-1} = x(yy_1^{-1}x_1^{-1}),$$

$$(yy_1^{-1}x_1^{-1} \in KH \text{ et } HK = KH) \Rightarrow \exists (x_2, y_2) \in H \times K,$$

$$yy_1^{-1}x_1^{-1} = x_2y_2;$$

alors, $(xy)(x_1y_1)^{-1} = xx_2y_2 \in HK$ et d'après le théorème (1.24), HK est un sous-groupe de G .

Remarques (1.48) :

1° Si HK est un sous-groupe de G , alors HK est le sous-groupe de G engendré par $H \cup K$.

2° Si G est abélien, quels que soient les sous-groupes H et K de G , HK est un sous-groupe de G .

COROLLAIRE (1.49). Soit $\{H_i\}_{1 \leq i \leq n}$ une famille finie de sous-groupes de G . Si, quel que soit (i, j) tel que $1 \leq i < j \leq n$, $H_i H_j$ est un sous-groupe de G , alors

$$H_1 H_2 \dots H_n = \{x_1 x_2 \dots x_n; x_i \in H_i, \forall i (1 \leq i \leq n)\}$$

est un sous-groupe de G .

Démonstration laissée au lecteur (exercice 28, chap. Ier).

D / Somme directe de sous-groupes d'un groupe abélien $(G, +)$

a) *Somme directe de deux sous-groupes.* Soient H et K deux sous-groupes d'un groupe abélien $(G, +)$; d'après les remarques (1.48)

le sous-groupe de G engendré par $H \cup K$ est $G' = H + K$, qui est appelé *somme des sous-groupes* H et K .

Définition (1.50) : Compte tenu des notations ci-dessus, le sous-groupe $G' = H + K$ est dit *somme directe* des sous-groupes H et K , si $H \cap K = (0)$.

Dans ce cas, on écrit $G' = H \oplus K$.

PROPOSITION (1.51). $(G, +)$ étant un groupe abélien, la somme des deux sous-groupes H et K est directe, si et seulement si tout élément de $H + K$ s'écrit de façon unique : $x + y$, où $x \in H$ et $y \in K$.

Preuve :

1° Supposons la somme $H + K$ directe, c'est-à-dire que l'on a $H \cap K = (0)$. Soit $z \in H \oplus K$ tel que $z = x + y = x' + y'$, où x et x' sont dans H et y, y' dans K ; alors

$$x - x' = y' - y \text{ est dans } H \cap K = (0),$$

par suite $x = x'$ et $y = y'$.

2° Réciproquement, on suppose que tout $z \in H + K$ s'écrit de façon unique $z = x + y$ où $x \in H, y \in K$.

Soit $z \in H \cap K$, alors $z \in H + K$ et on peut écrire :

$$z = z + 0, \quad \text{avec } z \in H \text{ et } 0 \in K$$

$$\text{ou } z = 0 + z, \quad \text{avec } 0 \in H \text{ et } z \in K.$$

L'hypothèse implique alors $z = 0$, d'où $H \cap K = (0)$.

b) Somme directe d'une famille quelconque de sous-groupes. Soient I un ensemble non vide et $\{H_i\}_{i \in I}$ une famille de sous-groupes d'un groupe abélien $(G, +)$.

Le sous-groupe de $(G, +)$ engendré par $\bigcup_{i \in I} H_i$ se note $\sum_{i \in I} H_i$ et s'appelle la somme des sous-groupes de $H_i, i \in I$.

Si I est fini et $I = \{1, 2, \dots, n\}$, d'après les remarques (1.48) et le corollaire (1.49), on a :

$$\sum_{1 \leq i \leq n} H_i = H_1 + H_2 + \dots + H_n$$

$$\sum_{1 \leq i \leq n} H_i = \{x_1 + x_2 + \dots + x_n; x_i \in H_i, \forall i (1 \leq i \leq n)\}.$$

Si I est infini, d'après la relation (18), $x \in \sum_{i \in I} H_i$ si et seulement si $x = x_{i_1} + x_{i_2} + \dots + x_{i_n}$, où $n \in \mathbf{N}^*$,

$$\{i_1, i_2, \dots, i_n\} \subseteq I \quad \text{et} \quad x_{i_k} \in H_{i_k}, \quad \forall k (1 \leq k \leq n).$$

Autrement dit, $x \in \sum_{i \in I} H_i$ si et seulement s'il existe une partie finie et non vide de $I : \{i_1, i_2, \dots, i_n\}$ telle que $x \in \sum_{1 \leq k \leq n} H_{i_k}$.

Notation : Pour un élément $x \in \sum_{i \in I} H_i$ (I infini), on pourra écrire :

$$x = \sum_{i \in I} x_i, \quad \text{où } x_i = 0, \quad \text{sauf pour un nombre fini d'indices } i;$$

cette condition s'exprime aussi par la formule : « les x_i étant presque tous nuls ».

Définition (1.52) : $(G, +)$ étant un groupe abélien et $\{H_i\}_{i \in I}$ une famille quelconque de sous-groupes de G , le sous-groupe $\sum_{i \in I} H_i$ est dit *somme directe* des sous-groupes H_i , si :

$$\forall j \in I, \quad H_j \cap \sum_{\substack{i \in I \\ i \neq j}} H_i = (0) \quad (21)$$

La somme directe des H_i , $i \in I$, est notée : $\bigoplus_{i \in I} H_i$.

PROPOSITION (1.53). I étant un ensemble non vide et $\{H_i\}_{i \in I}$ une famille de sous-groupes d'un groupe abélien $(G, +)$, le sous-groupe $G' = \sum_{i \in I} H_i$ est somme directe des H_i , si et seulement si tout $x \in G'$ s'écrit de façon unique :

$$x = \sum_{1 \leq k \leq n} x_{i_k},$$

où $n \in \mathbf{N}^*$, $\{i_1, \dots, i_n\} \subseteq I$ et $x_{i_k} \in H_{i_k}$, $\forall k (1 \leq k \leq n)$.

Démonstration laissée au lecteur (exercice 28, chap. I^{er}).

3 — Morphismes de groupes

A / Définitions. Propriétés générales

Définition (1.54) : Etant donné deux groupes (G, \cdot) et $(G', *)$, un *morphisme de groupes* de G dans G' est une application $f: G \rightarrow G'$ telle que, quels que soient x et y dans G , on ait :

$$f(x \cdot y) = f(x) * f(y) \quad (22)$$

Un morphisme de groupes est aussi appelé *homomorphisme* de groupes.

L'ensemble des morphismes d'un groupe G dans un groupe G' sera noté $\text{Hom}(G, G')$.

Un morphisme d'un groupe G dans lui-même est appelé *endomorphisme* de groupe.

L'ensemble des endomorphismes d'un groupe G sera noté $\text{End}(G)$.

Selon nos conventions générales, dans la suite, les groupes G et G' seront notés multiplicativement, leurs éléments unités étant respectivement e et e' .

PROPOSITION (1.55). *Tout $f \in \text{Hom}(G, G')$ vérifie les propriétés suivantes :*

$$1^\circ f(e) = e'.$$

$$2^\circ f(x^{-1}) = (f(x))^{-1}, \text{ quel que soit } x \text{ dans } G.$$

$$3^\circ f(x^n) = (f(x))^n, \text{ quels que soient } x \text{ dans } G \text{ et } n \text{ dans } \mathbb{Z}.$$

$$4^\circ H \leq G \Rightarrow f(H) \leq G'.$$

$$5^\circ H' \leq G' \Rightarrow f^{-1}(H') \leq G, \text{ où } f^{-1}(H') = \{x \in G; f(x) \in H'\}.$$

Preuve :

$$1^\circ \text{ Pour tout } x \in G, \text{ on a } f(x) = f(xe) = f(x)f(e); \text{ or,}$$

$$f(x) \in G' \Rightarrow f(x) = f(x)e'.$$

La règle de simplification dans G' implique alors :

$$f(e) = e'.$$

2° Quel que soit $x \in G$, $f(xx^{-1}) = f(x)f(x^{-1}) = f(e)$; or,

$$f(e) = e' = f(x)(f(x))^{-1},$$

d'où $(f(x))^{-1} = f(x^{-1})$.

3° Pour $n = 0$, $x^0 = e$ et $(f(x))^0 = e'$; on est ramené au 1°. Pour $n > 0$, $x^n = xx \dots x$ (n fois), d'où

$$f(x^n) = f(x)f(x) \dots f(x) \quad (n \text{ fois}),$$

donc $f(x^n) = (f(x))^n$.

Pour $n < 0$, on pose $n = -n'$, $n' > 0$;

$$\begin{aligned} x^n &= (x^{-1})^{n'} \Rightarrow f(x^n) = (f(x^{-1}))^{n'} \\ &= ((f(x))^{-1})^{n'} = (f(x))^{-n'} \end{aligned}$$

d'où $f(x^n) = f(x)^n$.

4° $f(H) = \{f(x); x \in H\}$. Soient y_1 et y_2 dans $f(H)$; il existe x_1 et x_2 dans H tels que $y_1 = f(x_1)$, $y_2 = f(x_2)$.

$$y_1 y_2^{-1} = f(x_1)(f(x_2))^{-1} = f(x_1)f(x_2^{-1}),$$

d'où $y_1 y_2^{-1} = f(x_1 x_2^{-1})$.

$$(x_1 \in H, x_2 \in H \text{ et } H \leq G) \Rightarrow x_1 x_2^{-1} \in H;$$

par suite $y_1 y_2^{-1} \in f(H)$, donc $f(H) \leq G'$.

5° Soient x_1 et x_2 dans $f^{-1}(H')$; alors $f(x_1) \in H'$ et $f(x_2) \in H'$; H' étant un sous-groupe de G' , on a

$$f(x_1)(f(x_2))^{-1} = f(x_1)f(x_2^{-1}) = f(x_1 x_2^{-1}) \text{ dans } H',$$

d'où $x_1 x_2^{-1} \in f^{-1}(H')$ et par suite $f^{-1}(H')$ est un sous-groupe de G .

COROLLAIRE (1.56). Soit $f \in \text{Hom}(G, G')$, alors :

1° $f(G)$ est un sous-groupe de G' .

2° $f^{-1}(e') = \{x \in G; f(x) = e'\}$ est un sous-groupe de G .

Ces propriétés découlent de l'application de la proposition (1.55) aux cas particuliers : $H = G$ et $H' = (e')$.

Définition (1.57) : Soit $f \in \text{Hom}(G, G')$.

$f(G)$ est appelé *image de f* et est noté $\text{Im } f$.

$f^{-1}(e')$ est appelé *noyau de f* et est noté $\text{Ker } f$.

PROPOSITION (1.58). Pour $f \in \text{Hom}(G, G')$, on a :

$$1^\circ f \text{ surjectif} \Leftrightarrow \text{Im } f = G'.$$

$$2^\circ f \text{ injectif} \Leftrightarrow \text{Ker } f = (e).$$

Preuve : La première propriété est immédiate puisque, par définition, f est surjectif si $f(G) = G'$.

Démontrons la seconde propriété; rappelons que f est injectif si et seulement si, quels que soient x et x' dans G , $f(x) = f(x')$ implique $x = x'$.

— Supposons f injectif; soit $x \in \text{Ker } f$, alors $f(x) = e' = f(e)$, d'où $x = e$ et par suite $\text{Ker } f = (e)$;

— Supposons $\text{Ker } f = (e)$; soient x et x' dans G tels que $f(x) = f(x')$; on en déduit :

$$e' = (f(x))^{-1} f(x') = f(x^{-1}) f(x'), \quad \text{d'où } e = f(x^{-1} x'),$$

ce qui implique $x^{-1} x' \in \text{Ker } f$;

$$\text{Ker } f = (e) \Rightarrow x^{-1} x' = e, \quad \text{d'où } x' = x;$$

f est donc injectif.

PROPOSITION (1.59). Soient G , G' , G'' trois groupes, alors $f \in \text{Hom}(G, G')$ et $g \in \text{Hom}(G', G'')$ implique $g \circ f \in \text{Hom}(G, G'')$.

Preuve : Soient x et y dans G ;

$$g \circ f(xy) = g(f(xy))$$

$$g \circ f(xy) = g(f(x)f(y)), \quad \text{car } f \in \text{Hom}(G, G');$$

$$g \circ f(xy) = g(f(x)) g(f(y)), \quad \text{car } g \in \text{Hom}(G', G'')$$

$$\text{d'où } g \circ f(xy) = (g \circ f(x)) (g \circ f(y)).$$

Définition (1.60) : Un groupe G' est dit *image homomorphe* d'un groupe G , s'il existe un morphisme surjectif $f \in \text{Hom}(G, G')$.

*Premiers exemples de morphismes de groupes.**Exemples (1.61) :*1° Soient G un groupe et H un sous-groupe de G .*L'injection canonique $i : H \rightarrow G$*

$$x \mapsto x$$

est un *morphisme injectif* de groupes.2° Soient deux groupes G et G' ; l'application $h : G \rightarrow G'$

$$x \mapsto e'$$

est un morphisme de groupes tel que $\text{Ker } h = G$.Lorsque le groupe G' est additif et que e' est noté 0, h est appelé : *morphisme nul* de G dans G' .*Exemple (1.62) :* Soit $n > 0$ dans \mathbf{Z} ; la *surjection canonique* de \mathbf{Z} dans $\frac{\mathbf{Z}}{(n)}$, c'est-à-dire l'application :

$$\pi : \mathbf{Z} \rightarrow \frac{\mathbf{Z}}{(n)}$$

$$x \mapsto \bar{x} \text{ (classe de } x \text{ modulo } n),$$

est un *morphisme surjectif* de groupes.En effet, compte tenu de la définition de l'addition dans $\frac{\mathbf{Z}}{(n)}$ (exemple (1.13), formule 10), on a, quels que soient x et y dans \mathbf{Z} , $\pi(x + y) = \pi(x) + \pi(y)$.*Exemple (1.63) :* Soit $n > 1$ dans \mathbf{N} ; en associant à toute matrice A du groupe $\text{GL}(n, \mathbf{R})$ son *déterminant* : $\det A$, on définit une application, que nous noterons d , de $\text{GL}(n, \mathbf{R})$ dans le groupe multiplicatif \mathbf{R}^* , car toute matrice de $\text{GL}(n, \mathbf{R})$ est inversible, donc de déterminant non nul; de plus, quels que soient A et B dans $\text{GL}(n, \mathbf{R})$, on a $\det AB = \det A \det B$ (voir [31] ou [50]); par suite, l'application $d : \text{GL}(n, \mathbf{R}) \rightarrow \mathbf{R}^*$ est un morphisme de groupes.

$$A \mapsto \det A$$

$$\text{Ker } d = \{A \in \text{GL}(n, \mathbf{R}); \det A = 1\}.$$

 $\text{Ker } d$ est un sous-groupe de $\text{GL}(n, \mathbf{R})$ appelé : *groupe linéaire spécial* des matrices carrées d'ordre n sur \mathbf{R} et noté $SL(n, \mathbf{R})$;

plus généralement, on peut définir $SL(n, K)$, où K est un corps commutatif quelconque [51].

Exemple (1.64) : Soit $GO(\mathbb{R}^2)$ le groupe des similitudes de l'espace vectoriel euclidien \mathbb{R}^2 (exemple (1.32)).

$$\begin{aligned} \text{L'application } \lambda : GO(\mathbb{R}^2) &\rightarrow \mathbb{R}_+^* \\ u &\mapsto \lambda_u \end{aligned}$$

où λ_u est le rapport de la similitude u est un *morphisme de groupes* (le vérifier à partir de la relation (16)).

$$\text{Ker } \lambda = \{u \in GO(\mathbb{R}^2); \lambda_u = 1\}$$

$\text{Ker } \lambda$ est un sous-groupe de $GO(\mathbb{R}^2)$, appelé *groupe orthogonal de \mathbb{R}^2* et noté $O(\mathbb{R}^2)$.

Pour tout espace vectoriel euclidien de dimension finie E , on peut définir de même le groupe orthogonal $O(E)$ ([23], [51]).

B / Isomorphismes. Théorème de Cayley

Définition (1.65) : Une application f d'un groupe G dans un groupe G' est un *isomorphisme de groupe* si $f \in \text{Hom}(G, G')$ et s'il existe $g \in \text{Hom}(G', G)$ tel que

$$g \circ f = \text{id}_G \quad \text{et} \quad f \circ g = \text{id}_{G'} \quad (23)$$

PROPOSITION (1.66). *Soient deux groupes G et G' :*

- 1° Si f est une application de G dans G' , alors : f est un isomorphisme de groupes $\Leftrightarrow f \in \text{Hom}(G, G')$ et f bijectif.
- 2° f isomorphisme de G sur $G' \Rightarrow f^{-1}$ isomorphisme de G' sur G .

Preuve :

1° a) Supposons f isomorphisme de groupes; d'après la définition (1.65), $f \in \text{Hom}(G, G')$ et il existe $g \in \text{Hom}(G', G)$ vérifiant les relations (23).

Montrons que f est surjectif; soit $y \in G'$, on a

$$y = \text{id}_{G'}(y) = f \circ g(y) = f(g(y)),$$

donc $G' = \text{Im } f$.

Montrons que f est injectif; supposons x et x' dans G tels que $f(x) = f(x')$; on a alors : $g \circ f(x) = g \circ f(x')$, c'est-à-dire $\text{id}_G(x) = \text{id}_G(x')$, donc $x = x'$.

On en conclut que f est *bijectif*.

b) Supposons $f \in \text{Hom}(G, G')$ et f *bijectif*. f admet une application réciproque f^{-1} qui est une bijection de G' sur G et qui vérifie

$$f^{-1} \circ f = f \circ f^{-1} = \text{id}_G.$$

Montrons que f^{-1} est un morphisme de groupes.

Soient y_1 et y_2 dans G' , posons $x = f^{-1}(y_1 y_2)$; on a $f(x) = y_1 y_2$; d'autre part, il existe x_1 et x_2 uniques dans G tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$, d'où

$$f(x) = f(x_1) f(x_2) = f(x_1 x_2), \quad \text{car } f \in \text{Hom}(G, G').$$

f *bijectif* implique f *injectif*, par suite $x = x_1 x_2$; or, $x_1 = f^{-1}(y_1)$, $x_2 = f^{-1}(y_2)$, on en déduit :

$$f^{-1}(y_1 y_2) = f^{-1}(y_1) f^{-1}(y_2);$$

alors, $g = f^{-1}$ satisfait aux conditions (23), donc f est *isomorphisme*.

Le 2° de la proposition (1.66) résulte directement de la démonstration précédente.

Définition (1.67) : S'il existe un isomorphisme d'un groupe G sur un groupe G' , on dit que G et G' sont des groupes *isomorphes*; dans ce cas on écrit : $G \simeq G'$.

Remarques (1.68) :

1° Un isomorphisme étant une bijection, deux groupes isomorphes sont équipotents, c'est-à-dire sont de même cardinal [28]. En particulier, *deux groupes finis isomorphes sont de même ordre*; la réciproque de cette propriété est fausse.

Considérons par exemple le groupe $\frac{\mathbb{Z}}{(4)}$ et le groupe V défini par la table (11); ils sont de même ordre 4.

Supposons qu'une bijection f de V sur $\frac{\mathbb{Z}}{(4)}$ soit un isomorphisme; on aurait :

$$\frac{\mathbb{Z}}{(4)} = \{f(e) = \bar{0}, f(a), f(b), f(c)\};$$

mais la table (11) montre que dans V tout élément $x \neq e$ est d'ordre 2; par suite, dans $\frac{\mathbb{Z}}{(4)}$ tout élément, autre que $\bar{0}$, devrait être d'ordre 2; or nous savons que $\bar{1}$ et $\bar{3}$ sont d'ordre 4; on en conclut que les groupes $\frac{\mathbb{Z}}{(4)}$ et V ne sont pas isomorphes et, en particulier, le groupe V n'est pas cyclique. (La notation V vient du nom allemand : *Viererguppe*.)

2° Même si deux groupes G et G' sont isomorphes, une bijection de G sur G' n'est pas nécessairement un isomorphisme (voir remarque (1.76) 1°).

3° ($f \in \text{Hom}(G, G')$ et f injectif) $\Rightarrow G \simeq \text{Im } f$.

En effet, la restriction surjective de f , c'est-à-dire l'application

$$\begin{aligned} f_1 : G &\rightarrow \text{Im } f \\ x &\mapsto f_1(x) = f(x) \end{aligned}$$

est un isomorphisme de groupes d'après la proposition (1.62) 1°.

Définition (1.69) : G étant un groupe, un isomorphisme de G sur lui-même est appelé un *automorphisme* du groupe G .

L'ensemble des automorphismes d'un groupe G est noté $\text{Aut}(G)$.

PROPOSITION (1.70). *Pour tout groupe G , $\text{Aut}(G)$ est un sous-groupe du groupe symétrique S_G .*

Ce résultat se déduit des propositions (1.59) et (1.66).

Remarque (1.71) : G, G', G'' désignant des groupes, les propositions (1.59) et (1.66) impliquent :

- a) $G \simeq G$;
- b) $G \simeq G' \Rightarrow G' \simeq G$;
- c) $(G \simeq G' \text{ et } G' \simeq G'') \Rightarrow G \simeq G''$.

Exemples d'isomorphismes.

Exemple (1.72) :

On a défini (exemple (1.17)) les groupes linéaires $\text{GL}(E)$ et les groupes de matrices $\text{GL}(n, K)$. On démontre en algèbre

linéaire (voir par exemple [49]) que si E est un espace vectoriel de dimension finie n sur un corps K , alors les groupes $GL(E)$ et $GL(n, K)$ sont isomorphes et toute base $b = \{e_1, e_2, \dots, e_n\}$ de E sur K permet de définir un isomorphisme $M_b : GL(E) \rightarrow GL(n, K)$

$$u \mapsto M_b(u)$$

où $M_b(u)$ est la matrice de u dans la base b , c'est-à-dire la matrice carrée d'ordre n dont les colonnes sont respectivement formées par les composantes dans la base b des vecteurs $u(e_1), u(e_2), \dots, u(e_n)$.

Exemples (1.73) : Automorphismes intérieurs d'un groupe G .

A tout $g \in G$, associons l'application :

$$\begin{aligned} \sigma_g : G &\rightarrow G \\ x &\mapsto gxg^{-1}. \end{aligned}$$

$$\begin{aligned} \text{Pour } x \text{ et } y \text{ dans } G, \quad \sigma_g(xy) &= gxyg^{-1} = (gxg^{-1})(gyg^{-1}), \\ \sigma_g(xy) &= \sigma_g(x) \sigma_g(y), \end{aligned}$$

donc $\sigma_g \in \text{End}(G)$.

D'autre part, la règle de simplification à droite et à gauche implique l'injectivité de σ_g .

Enfin, quel que soit $y \in G$, on peut écrire :

$$y = g(g^{-1}yg)g^{-1} = \sigma_g(g^{-1}yg),$$

donc σ_g est surjectif.

On en conclut que $\sigma_g \in \text{Aut}(G)$.

σ_g est appelé : *automorphisme intérieur* de G défini par g .

Posons $\text{Int}(G) = \{\sigma_g; g \in G\}$ et montrons que

$\text{Int}(G)$ est un sous-groupe de $\text{Aut}(G)$.

$$\sigma_e = \text{id}_G \Rightarrow \text{Int}(G) \neq \emptyset.$$

Soient g_1 et g_2 dans G ; pour tout $x \in G$, on a

$$\sigma_{g_1} \circ \sigma_{g_2}(x) = g_1(g_2 x g_2^{-1}) g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1},$$

d'où $\sigma_{g_1} \circ \sigma_{g_2} = \sigma_{g_1 g_2}$, donc $\sigma_{g_1} \circ \sigma_{g_2} \in \text{Int}(G)$.

De plus, pour tout $g \in G$,

$$(\sigma_g \circ \sigma_{g^{-1}} = \sigma_e = \text{id}_G) \Rightarrow (\sigma_g)^{-1} = \sigma_{g^{-1}};$$

par suite, $(\sigma_g)^{-1} \in \text{Int}(G)$, d'où $\text{Int } G \leq \text{Aut}(G)$.

Théorème de Cayley.

LEMME (1.74). Soient E et E' deux ensembles non vides ; S_E et $S_{E'}$ étant leurs groupes symétriques, on a :

$$E \text{ équipotent à } E' \Rightarrow S_E \simeq S_{E'};$$

en particulier :

$$(E \text{ fini et } \text{card } E = n) \Rightarrow S_E \simeq S_n.$$

Preuve : Dire que E est équipotent à E' , c'est-à-dire qu'il existe une bijection f de E sur E' .

Soit $\sigma \in S_E$, le diagramme :

$$E' \xrightarrow{f^{-1}} E \xrightarrow{\sigma} E \xrightarrow{f} E'$$

montre que $f \circ \sigma \circ f^{-1} \in S_{E'}$.

Considérons alors l'application $\varphi : S_E \rightarrow S_{E'}$
 $\sigma \mapsto f \circ \sigma \circ f^{-1}$.

φ est injective, car $\varphi(\sigma) = \varphi(\sigma')$ implique

$$f \circ \sigma \circ f^{-1}(x') = f \circ \sigma' \circ f^{-1}(x'), \quad \forall x' \in E';$$

f étant injective, on en déduit que

$$\sigma \circ f^{-1}(x') = \sigma' \circ f^{-1}(x'), \quad \forall x' \in E',$$

donc $\sigma \circ f^{-1} = \sigma' \circ f^{-1}$;

par suite, $\sigma \circ f^{-1} \circ f = \sigma' \circ f^{-1} \circ f$, d'où $\sigma = \sigma'$.

φ est surjective ; en effet, étant donné $\tau \in S_{E'}$, si l'on pose $\sigma = f^{-1} \circ \tau \circ f$, on a $\sigma \in S_E$ et $\tau = \varphi(\sigma)$.

Enfin, φ est un *morphisme* de groupes, car, quels que soient σ et σ' dans S_E , on a :

$$\varphi(\sigma \circ \sigma') = f \circ \sigma \circ \sigma' \circ f^{-1}$$

$$\varphi(\sigma \circ \sigma') = (f \circ \sigma \circ f^{-1}) \circ (f \circ \sigma' \circ f^{-1})$$

$$\varphi(\sigma \circ \sigma') = \varphi(\sigma) \circ \varphi(\sigma');$$

on en conclut que φ est un *isomorphisme* de groupes.

Dans le cas particulier où E est fini et $\text{card } E = n$, posons $E = \{x_1, x_2, \dots, x_n\}$. La bijection $f : i \mapsto x_i$ de $\{1, 2, \dots, n\}$

sur E induit, comme plus haut, l'isomorphisme φ de S_n sur S_E tel que pour tout $\sigma \in S_n$,

$$\varphi(\sigma)(x_i) = x_{\sigma(i)}, \quad \forall x_i \in E.$$

On peut alors identifier S_E à S_n , en notant σ l'élément de S_E égal à $\varphi(\sigma)$.

Compte tenu de cette identification, quel que soit l'entier $n \geq 1$, nous considérons le groupe S_n comme étant le groupe symétrique de tout ensemble de cardinal n .

Définition (1.75) : G étant un groupe, à tout $g \in G$, on associe l'application $\tau_g : G \rightarrow G$

$$x \mapsto gx.$$

τ_g s'appelle la *translation à gauche* de G , définie par g .

On remarque que $\tau_e = \text{id}_G$.

Posons $T_G = \{\tau_g; g \in G\}$; on a $T_G \neq \emptyset$; montrons que T_G est un sous-ensemble du groupe symétrique S_G .

Pour tout $g \in G$, l'injectivité de τ_g résulte de la règle de simplification à gauche; d'autre part, quels que soient g et y dans G , il existe $x \in G$ tel que $y = gx$, d'où la surjectivité de τ_g . On a donc $T_G \subseteq S_G$.

Remarques (1.76) :

1° Pour $g \neq e$, τ_g n'est pas un automorphisme de G , car pour x et y quelconques dans G , on a, en général, $gxy \neq xgy$.

2° Si G est noté additivement, τ_g est telle que, pour tout $x \in G$, $\tau_g(x) = g + x$.

3° On peut définir de façon analogue la notion de translation à droite δ_g , telle que pour tout $x \in G$, $\delta_g(x) = xg$.

L'ensemble T'_G des translations à droite de G est aussi une partie non vide de S_G .

LEMME (1.77). *Pour tout groupe G , on a*

$$T_G \leq S_G \quad \text{et} \quad G \simeq T_G.$$

Preuve : On a montré précédemment que T_G est une partie non vide de S_G . Soient τ_{g_1} et τ_{g_2} dans T_G .

Pour tout $x \in G$, $\tau_{g_1} \circ \tau_{g_2}(x) = g_1 g_2 x = \tau_{g_1 g_2}(x)$, donc

$$\tau_{g_1} \circ \tau_{g_2} \in T_G.$$

D'autre part, pour tout g et tout x dans G , on a :

$$\tau_g \circ \tau_{g^{-1}}(x) = \tau_e(x) = x,$$

d'où $(\tau_g)^{-1} = \tau_{g^{-1}} \in T_G$;

on en conclut que T_G est un sous-groupe de S_G .

Considérons l'application $\tau : G \rightarrow T_G$
 $g \mapsto \tau_g$

τ est surjective, par définition, et

$$\tau_g = \tau_{g'} \Leftrightarrow gx = g'x, \quad \forall x \in G,$$

d'où $\tau_g = \tau_{g'} \Rightarrow g = g'$;

τ est donc injective, par suite τ est une bijection.

On a vu plus haut que $\tau_{g_1 g_2} = \tau_{g_1} \circ \tau_{g_2}$, quels que soient g_1 et g_2 dans G , donc τ est un morphisme de groupes.

D'après la proposition (1.66) τ est un isomorphisme de groupes.

Ce résultat s'énonce généralement sous la forme du théorème suivant, connu sous le nom de *Théorème de Cayley* :

THÉORÈME (1.78). *Tout groupe est isomorphe à un sous-groupe du groupe de ses permutations.*

En particulier, tout groupe fini d'ordre n est isomorphe à un sous-groupe du groupe symétrique S_n .

Dans le cas particulier où le groupe est fini, la propriété résulte à la fois des lemmes (1.74) et (1.77).

C / Monomorphismes et épimorphismes de groupes

Définitions (1.79) : Soient deux groupes G et G' .

1° Une application $f : G \rightarrow G'$ est appelée *monomorphisme de groupes*, si :

a) $f \in \text{Hom}(G, G')$ et

b) quel que soit le groupe Γ , la propriété suivante est vérifiée :

$$(u \text{ et } v \text{ dans } \text{Hom}(\Gamma, G) \text{ et } f \circ u = f \circ v) \Rightarrow u = v.$$

2° Une application $f: G \rightarrow G'$ est appelée *épimorphisme de groupes*, si :

a) $f \in \text{Hom}(G, G')$ et

b) quel que soit le groupe Γ , on a la propriété :

$$(u \text{ et } v \text{ dans } \text{Hom}(G', \Gamma) \text{ et } u \circ f = v \circ f) \Rightarrow u = v.$$

PROPOSITION (1.80). Pour une application f d'un groupe G dans un groupe G' , on a :

1° f morphisme injectif $\Leftrightarrow f$ monomorphisme

2° f morphisme surjectif $\Leftrightarrow f$ épimorphisme.

Preuve :

1° Supposons $f \in \text{Hom}(G, G')$ et f injectif; soient Γ un groupe et u, v dans $\text{Hom}(\Gamma, G)$ tels que $f \circ u = f \circ v$.

Pour tout $x \in \Gamma$, on a $f(u(x)) = f(v(x))$; l'injectivité de f implique alors $u = v$, d'où f monomorphisme.

Réciproquement, supposons f monomorphisme et x, x' dans G tels que $f(x) = f(x')$. Considérons le groupe \mathbf{Z} et les applications u et v de \mathbf{Z} dans G telles que :

$$\begin{array}{ll} u: \mathbf{Z} \rightarrow G, & v: \mathbf{Z} \rightarrow G \\ n \mapsto x^n & n \mapsto x'^n. \end{array}$$

On sait que pour n et m dans \mathbf{Z} on a $x^{m+n} = x^m x^n$; u et v sont donc des morphismes de groupes. D'autre part,

$$f \circ u(n) = f(x^n) = (f(x))^n \text{ et } f \circ v(n) = f(x'^n) = (f(x'))^n;$$

alors $f(x) = f(x') \Rightarrow f \circ u = f \circ v$

et f monomorphisme implique $u = v$, d'où :

$$x^n = x'^n, \text{ quel que soit } n \in \mathbf{Z};$$

pour $n = 1$, on obtient $x = x'$, par suite, f est un morphisme injectif.

2° On suppose que f est un morphisme surjectif de G sur G' . Soient Γ un groupe et u, v dans $\text{Hom}(G', \Gamma)$ tels que

$$u \circ f = v \circ f.$$

Soit $y \in G'$, f étant surjectif, il existe $x \in G$ tel que $y = f(x)$, par suite :

$$u(y) = u(f(x)) = v(f(x)) = v(y), \quad \text{d'où } u = v;$$

f est donc un épimorphisme.

Réciproquement, supposons f épimorphisme de G dans G' .

Posons $H = \text{Im } f$ et supposons $H \neq G'$.

Soit $Q_H = \{x'H; x' \in G'\}$, où $x'H = \{x'h; h \in H\}$.

Considérons l'ensemble $E = Q_H \cup \{\infty\}$, où ∞ désigne un élément arbitraire n'appartenant pas à G' .

$$H = e'H \Rightarrow H \in Q_H.$$

Soit τ la permutation de E qui échange H et ∞ et qui laisse fixes tous les autres éléments de E .

D'autre part, pour tout $g \in G'$, notons σ_g l'application de E dans E définie par :

$$\begin{cases} \sigma_g(x'H) = gx'H, & \forall x'H \in Q_H \\ \sigma_g(\infty) = \infty. \end{cases}$$

On vérifie facilement que σ_g est une permutation de E , c'est-à-dire un élément du groupe symétrique S_E .

Considérons alors les applications :

$$\begin{aligned} \sigma : G' &\rightarrow S_E & \text{et} & & \gamma : G' &\rightarrow S_E \\ g &\mapsto \sigma_g & & & g &\mapsto \tau \circ \sigma_g \circ \tau. \end{aligned}$$

Des définitions de τ et σ_g , on déduit aisément que σ et γ sont des morphismes de groupes.

Montrons que l'on a $\sigma \circ f = \gamma \circ f$.

Soit x dans G ; $f(x) \in H$, posons $f(x) = h$; on a $hH = H$ et

$$\begin{aligned} \sigma \circ f(x) &= \sigma_h, & \gamma \circ f(x) &= \tau \circ \sigma_h \circ \tau \\ \sigma_h(\infty) &= \infty; & \tau \circ \sigma_h \circ \tau(\infty) &= \tau \circ \sigma_h(H) = \tau(H) = \infty. \\ \sigma_h(H) &= H; & \tau \circ \sigma_h \circ \tau(H) &= \tau \circ \sigma_h(\infty) = \tau(\infty) = H. \end{aligned}$$

$$x'H \neq H \Rightarrow \sigma_h(x'H) = hx'H \quad \text{et} \quad \tau \circ \sigma_h \circ \tau(x'H) = \tau \circ \sigma_h(x'H) = hx'H,$$

f étant un épimorphisme,

$$\sigma \circ f = \gamma \circ f \Rightarrow \sigma = \gamma,$$

par suite, par tout $g \in G'$, $\sigma_g = \tau \circ \sigma_g \circ \tau$.

Soit $g \notin H$ dans G' ; on a alors :

$$\sigma_g(H) = gH \neq H$$

et $\tau \circ \sigma_g \circ \tau(H) = \tau \circ \sigma_g(\infty) = \tau(\infty) = H,$

d'où une contradiction; par suite $\text{Im } f = H = G'$, donc f est surjectif.

Remarque (1.81) : Les résultats de la proposition (1.80) autorisent, dans le cas des groupes, à appeler :

monomorphisme, tout morphisme injectif
 et *épimorphisme, tout morphisme surjectif.*

Compte tenu de la proposition (1.66), la proposition (1.80) admet le corollaire suivant :

COROLLAIRE (1.82). *Une application f d'un groupe G dans un groupe G' est un isomorphisme de groupes si et seulement si c'est à la fois un monomorphisme et un épimorphisme.*

4 — Produit direct de groupes

A / Produit direct de deux groupes

Soient deux groupes G_1 et G_2 d'éléments unités e_1 et e_2 .

Posons $G = G_1 \times G_2 = \{(x_1, x_2); x_1 \in G_1, x_2 \in G_2\}$.

On vérifie facilement que l'ensemble non vide G muni de la loi de composition interne définie par :

$$\begin{aligned} G \times G &\rightarrow G \\ ((x_1, x_2), (y_1, y_2)) &\mapsto (x_1 y_1, x_2 y_2) \end{aligned}$$

est un groupe dont l'élément unité est (e_1, e_2) et quel que soit $(x_1, x_2) \in G$, $(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1})$.

Définition (1.83) : Le groupe $G_1 \times G_2$ est appelé *groupe produit direct* des groupes G_1 et G_2 .

Au produit direct $G_1 \times G_2$ on associe deux couples d'applications :

a) les *projections canoniques* p_1 et p_2 telles que :

$$\begin{aligned} p_1 : G_1 \times G_2 &\rightarrow G_1, & p_2 : G_1 \times G_2 &\rightarrow G_2 \\ (x_1, x_2) &\mapsto x_1 & (x_1, x_2) &\mapsto x_2. \end{aligned}$$

b) les *injections canoniques* q_1 et q_2 définies par :

$$\begin{aligned} q_1 : G_1 &\rightarrow G_1 \times G_2, & q_2 : G_2 &\rightarrow G_1 \times G_2 \\ x_1 &\mapsto (x_1, e_2) & x_2 &\mapsto (e_1, x_2). \end{aligned}$$

Il est alors facile de montrer que :

p_1 et p_2 sont des *épimorphismes de groupes*
et que q_1 et q_2 sont des *monomorphismes de groupes*.

Remarques (1.84) :

1° Le groupe $G_1 \times G_2$ est abélien si et seulement si G_1 et G_2 sont abéliens.

2° Les applications :

$$\begin{aligned} G_1 &\rightarrow G_1 \times (e_2) = \text{Im } q_1 & \text{et} & & G_2 &\rightarrow (e_1) \times G_2 = \text{Im } q_2 \\ x_1 &\mapsto (x_1, e_2) & & & x_2 &\mapsto (e_1, x_2) \end{aligned}$$

sont des isomorphismes de groupes; on en déduit que *le groupe $G_1 \times G_2$ contient au moins un sous-groupe isomorphe à G_1 et un sous-groupe isomorphe à G_2 .*

$$3^\circ \quad p_1 \circ q_1 = \text{id}_{G_1} \quad \text{et} \quad p_2 \circ q_2 = \text{id}_{G_2}, \quad (24)$$

4° Pour $x = (x_1, x_2)$ dans $G_1 \times G_2$, on peut écrire :

$$x = (p_1(x), p_2(x)) \quad (25)$$

$$x = q_1(x_1) q_2(x_2) = q_2(x_2) q_1(x_1) \quad (26)$$

5° Si G_1 et G_2 sont des groupes finis, compte tenu des propriétés générales des cardinaux [28], on a :

$$o(G_1 \times G_2) = o(G_1) o(G_2) \quad (27)$$

PROPOSITION (1.85). *Soient deux groupes G_1 et G_2 ; un groupe G est isomorphe au produit direct $G_1 \times G_2$, si et seulement s'il contient deux sous-groupes H_1 et H_2 tels que :*

1) $H_i \simeq G_i$, pour $i = 1, 2$.

2) $\forall h_1 \in H_1, \forall h_2 \in H_2, h_1 h_2 = h_2 h_1$.

$$3) \quad G = H_1 H_2.$$

$$4) \quad H_1 \cap H_2 = (e), \quad e \text{ étant l'élément neutre de } G.$$

Preuve :

1° Supposons G isomorphe à $G_1 \times G_2$; sans restreindre la généralité du résultat, on peut supposer $G = G_1 \times G_2$.

q_1 et q_2 étant les injections canoniques associées à $G_1 \times G_2$, posons :

$$H_1 = \text{Im } q_1, \quad H_2 = \text{Im } q_2.$$

D'après la remarque (1.84) 2°, on a

$$H_1 \simeq G_1 \quad \text{et} \quad H_2 \simeq G_2.$$

D'autre part, quels que soient $h_1 \in H_1$ et $h_2 \in H_2$, il existe $x_1 \in G_1$ et $x_2 \in G_2$ tels que

$$h_1 = (x_1, e_2), \quad h_2 = (e_1, x_2);$$

d'où $(x_1, x_2) = h_1 h_2 = h_2 h_1$.

Le résultat ci-dessus implique que $H_1 H_2$ est un sous-groupe de G (Proposition (1.47)). De plus, d'après la remarque (1.84) 4°, tout élément de G appartient à $H_1 H_2$, d'où $G = H_1 H_2$.

Enfin, compte tenu de la définition de H_1 et de H_2 , on a $H_1 \cap H_2 = (e_1, e_2)$, élément neutre de G .

2° On suppose que G contient deux sous-groupes H_1, H_2 satisfaisant aux quatre conditions énoncées.

Soit $g \in G$; les hypothèses impliquent qu'il existe $h_1 \in H_1$ et $h_2 \in H_2$ tels que :

$$g = h_1 h_2 = h_2 h_1.$$

Montrons que g s'écrit sous cette forme, de façon unique; supposons qu'il existe $h'_1 \in H_1, h'_2 \in H_2$ tels que

$$g = h'_1 h'_2 = h'_2 h'_1$$

$$h_1 h_2 = h'_1 h'_2 \Rightarrow h_1^{-1} h_1 = h'_2 h_2^{-1},$$

La condition 4) implique alors $e = h_1^{-1} h_1 = h'_2 h_2^{-1}$, d'où

$$h'_1 = h_1, \quad h'_2 = h_2.$$

D'après la condition 1), pour $i = 1, 2$, il existe un isomorphisme $\varphi_i : H_i \rightarrow G_i$. Considérons alors l'application φ suivante :

$$\begin{aligned}\varphi : G &\rightarrow G_1 \times G_2 \\ g = h_1 h_2 &\mapsto (\varphi_1(h_1), \varphi_2(h_2)).\end{aligned}$$

Pour $g = h_1 h_2$ et $g' = h'_1 h'_2$ dans G , on a

$$gg' = h_1 h_2 h'_1 h'_2 = h_1 h'_1 h_2 h'_2 \quad (\text{d'après la condition 2});$$

on en déduit facilement que φ est un morphisme de groupes.

D'autre part, $\varphi(h_1 h_2) = (e_1, e_2) \Rightarrow \varphi_1(h_1) = e_1$ et $\varphi_2(h_2) = e_2$; or φ_1 et φ_2 sont des isomorphismes, par suite,

$$\varphi(h_1 h_2) = (e_1, e_2) \Rightarrow h_1 = h_2 = e;$$

on en déduit que $\text{Ker } \varphi = (e)$, donc φ est injectif.

De plus, si $x = (x_1, x_2) \in G_1 \times G_2$, il existe un unique $h_1 \in H_1$ et un unique $h_2 \in H_2$ tels que : $x_1 = \varphi_1(h_1)$ et $x_2 = \varphi_2(h_2)$; par suite, $x = \varphi(h_1 h_2)$, donc φ est surjectif.

En conclusion : φ est un isomorphisme de G sur $G_1 \times G_2$.

Exemple (1.86) :

Le groupe produit direct $\frac{\mathbf{Z}}{(2)} \times \frac{\mathbf{Z}}{(2)}$ est généralement appelé *groupe de Klein* ⁽³⁾; d'après les propriétés vues plus haut, c'est un groupe abélien fini d'ordre 4. Considérons alors le groupe V défini par la table (11). Dans V , posons $H_1 = \langle a \rangle = \{e, a\}$ et $H_2 = \langle b \rangle = \{e, b\}$. On remarque que H_1 et H_2 sont isomorphes à $\frac{\mathbf{Z}}{(2)}$. D'autre part, $ab = ba = c$, d'où $V = H_1 H_2$; de plus $H_1 \cap H_2 = (e)$; compte tenu de la proposition (1.85), on a :

$$V \simeq \frac{\mathbf{Z}}{(2)} \times \frac{\mathbf{Z}}{(2)}$$

D'après la remarque (1.68) 1°, V est non cyclique, donc le *groupe de Klein est non cyclique*.

⁽³⁾ Félix Klein, mathématicien allemand (1849-1925).

B / Produit direct d'un nombre fini quelconque de groupes

La notion de produit direct de deux groupes se généralise de façon naturelle au produit direct de n groupes G_i ($1 \leq i \leq n$), quel que soit $n > 2$ dans \mathbb{N} . Le groupe produit direct est alors noté $G_1 \times G_2 \times \dots \times G_n$ ou $\prod_{1 \leq i \leq n} G_i$.

On généralise sans peine les définitions de projection et injection canoniques pour $n > 2$ dans \mathbb{N} , ainsi que les remarques (1.81) et la proposition (1.85) s'énonce alors sous la forme suivante :

PROPOSITION (1.88). *Soit $\{G_i\}_{1 \leq i \leq n}$ une famille finie de n groupes; un groupe G est isomorphe au groupe produit direct $\prod_{1 \leq i \leq n} G_i$, si et seulement s'il contient une famille de n sous-groupes H_i ($1 \leq i \leq n$) tels que :*

- 1) $H_i \simeq G_i, \forall i$ ($1 \leq i \leq n$).
- 2) $\forall (i, j)$ ($1 \leq i < j \leq n$), $\forall h_i \in H_i, \forall h_j \in H_j, h_i h_j = h_j h_i$.
- 3) $G = H_1 H_2 \dots H_n$.
- 4) $H_i \cap H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n = (e), \forall i$ ($1 \leq i \leq n$), e étant l'élément unité de G .

Démonstration laissée au lecteur.

COROLLAIRE (1.89). *Si $(G, +)$ est un groupe abélien et si $\{G_i\}_{1 \leq i \leq n}$ est une famille finie de n groupes abéliens, alors G est isomorphe au produit direct $\prod_{1 \leq i \leq n} G_i$, si et seulement s'il existe une famille de sous-groupes $\{H_i\}_{1 \leq i \leq n}$ tels que $H_i \simeq G_i$, pour tout i ($1 \leq i \leq n$), et $G = \bigoplus_{1 \leq i \leq n} H_i$.*

Ce résultat est une conséquence de la proposition (1.88) et de la définition (1.52).

C / Produit direct d'une famille quelconque de groupes

Soit I un ensemble non vide quelconque, donc éventuellement infini, et soit $\{G_i\}_{i \in I}$ une famille de groupes indexée par I .

L'ensemble produit cartésien

$$\prod_{i \in I} G_i = \{(x_i)_{i \in I}; x_i \in G_i, \forall i \in I\}$$

muni de la loi de composition définie par :

$$((x_i)_{i \in I}, (y_i)_{i \in I}) \mapsto (x_i y_i)_{i \in I}$$

est un groupe, dont l'élément neutre est $(e_i)_{i \in I}$, où e_i désigne l'élément neutre du groupe G_i ; ce groupe noté $\prod_{i \in I} G_i$ est, par définition, le *groupe produit direct des G_i , $i \in I$* .

Quel que soit l'ensemble non vide I , pour tout $k \in I$, on définit :

$$\begin{aligned} \text{la projection canonique } p_k : \prod_{i \in I} G_i &\rightarrow G_k \\ (x_i)_{i \in I} &\mapsto x_k \end{aligned}$$

$$\begin{aligned} \text{et l'injection canonique } q_k : G_k &\rightarrow \prod_{i \in I} G_i \\ x_k &\mapsto (x_i)_{i \in I} \end{aligned}$$

où $x_i = e_i$ si $i \neq k$ et $x_i = x_k$ si $i = k$.

Les projections et les injections canoniques sont, respectivement, des épimorphismes et monomorphismes de groupes.

Remarque (1.90) : Les remarques (1.84) 1° 2° 3° se généralisent au cas d'une famille quelconque $\{G_i\}_{i \in I}$ de groupes; en particulier, pour tout $i \in I$, on a :

$$p_i \circ q_i = \text{id}_{G_i} \quad (28)$$

et quel que soit $x \in \prod_{i \in I} G_i$, on peut écrire

$$x = (p_i(x))_{i \in I} \quad (29)$$

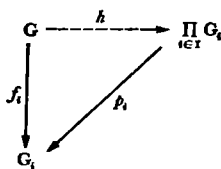
Par contre, si I est infini, la formule (26) et la proposition (1.88) ne peuvent pas être généralisées, puisque, dans un groupe, seul le produit d'un nombre fini d'éléments a un sens.

D / Propriété universelle du produit direct de groupes

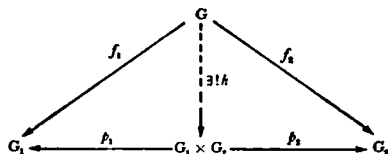
THÉORÈME (1.91). Soient I un ensemble non vide, $\{G_i\}_{i \in I}$ une famille de groupes et $\{p_i\}_{i \in I}$ la famille des projections canoniques associées au groupe produit direct $\prod_{i \in I} G_i$.

Etant donné un groupe G , quelle que soit la famille $\{f_i\}_{i \in I}$ de morphismes de groupes telle que, pour tout $i \in I$, $f_i \in \text{Hom}(G, G_i)$, il existe un unique morphisme $h \in \text{Hom}(G, \prod_{i \in I} G_i)$ tel que, quel que soit $i \in I$, $p_i \circ h = f_i$.

Compte tenu des hypothèses, le théorème (1.91) exprime que, pour tout $i \in I$, le diagramme suivant commute :



Preuve : Nous ferons la démonstration dans le cas où $I = \{1, 2\}$; la méthode se généralise sans peine au cas où I est un ensemble non vide quelconque. Le problème peut être schématisé par le diagramme ci-dessous :



$\{p_1, p_2\}, \{f_1, f_2\}$ sont connus, il s'agit de prouver l'existence et l'unicité du morphisme h .

a) *Existence de h :* Considérons l'application

$$h : G \rightarrow G_1 \times G_2$$

définie par :

$$x \mapsto (f_1(x), f_2(x))$$

f_1 et f_2 étant des morphismes de groupes, on en déduit facilement que $h \in \text{Hom}(G, G_1 \times G_2)$.

D'autre part, $p_1 \circ h(x) = f_1(x)$ et $p_2 \circ h(x) = f_2(x)$, quel que soit $x \in G$, impliquent :

$$p_1 \circ h = f_1 \quad \text{et} \quad p_2 \circ h = f_2.$$

b) *Unicité de h* : Supposons qu'il existe $h' \in \text{Hom}(G, G_1 \times G_2)$ tel que $p_1' \circ h' = f_1$ et $p_2' \circ h' = f_2$; ces conditions impliquent que pour tout $x \in G$ on a (formules 24) :

$$h'(x) = (f_1(x), f_2(x)) = h(x),$$

d'où $h' = h$.

Remarque (1.92) : La propriété du produit direct d'une famille de groupes énoncée dans le théorème (1.91) est dite « *universelle* » ; le lecteur pourra trouver dans [54], par exemple, la justification de ce qualificatif, issu de la théorie des catégories, et que nous retrouverons plusieurs fois au cours de cet ouvrage.

Exercices Chapitre Premier

- 1) Soit \mathbf{Z} l'ensemble des entiers rationnels, muni de la loi de composition interne notée $*$, définie par :

$$\mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}$$

$$(a, b) \mapsto a * b = a - b.$$

a) La loi $*$ est-elle associative ? commutative ?

b) Vérifier qu'il existe dans $(\mathbf{Z}, *)$ un élément neutre à droite, c'est-à-dire un élément e tel que

$$\forall a \in \mathbf{Z}, \quad a * e = a.$$

e est-il élément neutre dans $(\mathbf{Z}, *)$?

c) Existe-t-il, pour tout $a \in \mathbf{Z}$, un *symétrique à droite* relativement à e , c'est-à-dire un élément $a' \in \mathbf{Z}$ tel que $a * a' = e$?

- 2) Soit \mathbf{Q} l'ensemble des nombres rationnels muni de la loi de composition interne notée $*$, définie par :

$$\mathbf{Q} \times \mathbf{Q} \rightarrow \mathbf{Q}$$

$$(a, b) \mapsto a * b = a + b + ab$$

$(\mathbf{Q}, *)$ est-il un groupe ?

- 3) Soit G un ensemble non vide muni d'une loi de composition interne *associative* notée \cdot ; on suppose que dans (G, \cdot) les deux conditions suivantes sont vérifiées :

- 1° il existe un élément *neutre à droite* e (voir exercice 1) ;
 2° tout élément $x \in G$ admet un *symétrique à droite*, x' (voir exercice 1).

Démontrer que (G, \cdot) est un groupe ; vérifier, par un contre-exemple, que, sans l'associativité de la loi \cdot , ce résultat n'est plus vrai.

- 4) Soit G un ensemble *fini*, non vide, muni d'une loi de composition interne notée \cdot ; on suppose que la loi \cdot est associative et que dans (G, \cdot) tout élément est simplifiable à droite et à gauche.

Démontrer que (G, \cdot) est un groupe.

- 5) Soit G un groupe d'élément unité e , vérifiant la condition (\mathcal{C}) :

$$\forall x \in G, x^2 = e.$$

a) Donner au moins un exemple de groupe, non réduit à un seul élément, vérifiant (\mathcal{C}) .

b) Démontrer que tout groupe G vérifiant (\mathcal{C}) est abélien.

- 6) G étant un groupe, prouver que l'application $f: G \rightarrow G$
 $x \mapsto x^{-1}$

est une permutation de G et que f est un automorphisme si et seulement si le groupe G est abélien.

- 7) Montrer que si G est un groupe *fini d'ordre pair*, il existe au moins un élément $x \neq e$, dans G , tel que $x^2 = e$.

- 8) Dans l'ensemble des entiers \mathbf{Z} , on pose $U = \{-1, 1\}$.

a) Vérifier que U est un groupe relativement à la multiplication des entiers, donc un sous-groupe de (\mathbf{Q}^*, \times) .

b) Montrer que le groupe U est isomorphe au groupe $\left(\frac{\mathbf{Z}}{(2)}, +\right)$.

- 9) Soit \mathbf{D} le sous-ensemble de \mathbf{Q} formé par les nombres décimaux :

$$\mathbf{D} = \left\{ \frac{a}{10^n} ; a \in \mathbf{Z}, n \in \mathbf{N} \right\}.$$

Prouver que \mathbf{D} est un sous-groupe de $(\mathbf{Q}, +)$.

10) Soit, dans \mathbf{N} , un nombre premier p . On pose :

$$\mathbf{Q}_p = \left\{ \frac{a}{p^n} ; a \in \mathbf{Z}, n \in \mathbf{N} \right\}.$$

a) Vérifier que \mathbf{Q}_p est un sous-groupe de $(\mathbf{Q}, +)$ et que

$$\mathbf{Q}_p = \bigcup_{n \in \mathbf{N}} \left\langle \frac{1}{p^n} \right\rangle.$$

b) Montrer que l'application $\varphi : \mathbf{Q}_p \rightarrow \mathbf{Q}_p$ est une permutation de \mathbf{Q}_p .

$$x \mapsto px$$

L'application φ est-elle un automorphisme du groupe $(\mathbf{Q}_p, +)$?

11) Soit p un nombre premier dans \mathbf{N} . Vérifier les propriétés suivantes :

$$\{a + b\sqrt{p} ; (a, b) \in \mathbf{Z} \times \mathbf{Z}\} < (\mathbf{R}, +).$$

$$\{a + b\sqrt{p} ; a \text{ et } b \text{ dans } \mathbf{Q} \text{ et non simultanément nuls}\} < (\mathbf{R}^*, \times).$$

$$\{a + ib\sqrt{p} ; (a, b) \in \mathbf{Z} \times \mathbf{Z}\} < (\mathbf{C}, +).$$

$$\{a + ib\sqrt{p} ; a \text{ et } b \text{ dans } \mathbf{Q} \text{ et non simultanément nuls}\} < (\mathbf{C}^*, \times).$$

12) Etant donné un nombre premier $p \in \mathbf{N}$, on pose :

$$\Gamma_\infty = \{z \in \mathbf{C} ; \exists n \in \mathbf{N}, z^n = 1\}.$$

Vérifier que Γ_∞ est un sous-groupe de (\mathbf{C}^*, \times) .

13) A tout nombre réel a on associe l'application :

$$\begin{aligned} \tau_a : \mathbf{R} &\rightarrow \mathbf{R} \\ x &\mapsto a + x. \end{aligned}$$

Justifier la propriété :

$T = \{\tau_a ; a \in \mathbf{R}\}$ est un sous-groupe du groupe symétrique $S_{\mathbf{R}}$ et le groupe T est isomorphe au groupe $(\mathbf{R}, +)$.

14) On considère les groupes multiplicatifs \mathbf{R}^* , \mathbf{R}_+^* et \mathbf{C}^* (voir exemples (1.29)) et les applications :

$$\begin{aligned} f : \mathbf{R}^* &\rightarrow \mathbf{R}_+^* \\ x &\mapsto |x|, \quad \text{où } |x| \text{ est la valeur absolue de } x \end{aligned}$$

$$\begin{aligned} \text{et } g : \mathbf{C}^* &\rightarrow \mathbf{R}_+^* \\ z &\mapsto |z|, \quad \text{où } |z| \text{ est le module de } z. \end{aligned}$$

Vérifier que f et g sont les épimorphismes de groupes.
Déterminer les noyaux de f et g .

- 15) Démontrer que l'application $\lambda: \mathbf{R} \rightarrow \mathbf{R}_+^*$ est un isomorphisme
 $x \mapsto 10^x$
 du groupe $(\mathbf{R}, +)$ sur le groupe (\mathbf{R}_+^*, \times) .

- 16) a) Le centre d'un groupe G étant désigné par $Z(G)$, démontrer la propriété :

$$H \leq G \Rightarrow Z(G) \cap H \leq Z(H).$$

b) G et G' étant deux groupes, si f est un épimorphisme de G sur G' , prouver que l'on a : $f(Z(G)) \leq Z(G')$.

- 17) Soit S une partie non vide d'un groupe G ; on pose :

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

a) Vérifier que $C_G(S)$ est un sous-groupe de G .

$C_G(S)$ est appelé le *centralisateur de S dans G* .

Si $S = \{x\}$, avec $x \in G$, $C_G(S)$ se note $C_G(x)$;

$$C_G(x) = \{g \in G; gx = xg\}$$

est appelé *centralisateur de x dans G* .

b) $Z(G)$ étant le centre du groupe G , démontrer en relation :

$$\bigcap_{x \in G} C_G(x) = Z(G).$$

c) Pour $x \in G$, posons $H = C_G(x)$; vérifier que $x \in Z(H)$.

- 18) Soient A, B, C trois parties non vides d'un groupe G .

Soit $H = \langle A, B \rangle$ le sous-groupe de G engendré par $A \cup B$.

Si $K = \langle A, B, C \rangle$ est le sous-groupe de G engendré par $A \cup B \cup C$, démontrer que $K = \langle H, C \rangle$.

- 19) Démontrer que le groupe des quaternions (exemple (1.16)) est engendré par les matrices :

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

- 20) Dans l'ensemble $M_2(\mathbf{R})$ des matrices carrées d'ordre 2 sur \mathbf{R} , on considère le sous-ensemble Γ tel que :

$$\Gamma = \left\{ \begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix}; x \in \mathbf{R}^* \right\}.$$

Démontrer que Γ est un groupe par rapport à la multiplication des matrices, mais que ce groupe n'est pas un sous-groupe de $GL(2, \mathbb{R})$.

Vérifier que le groupe Γ est isomorphe au groupe (\mathbb{R}^*, \times) .

21) Soit $n > 1$ dans \mathbb{N} et $\left(\frac{\mathbb{Z}}{(n)}, +\right)$ le groupe des classes de congruences modulo n . On considère la correspondance μ définie par :

$$\mu : \frac{\mathbb{Z}}{(n)} \times \frac{\mathbb{Z}}{(n)} \rightarrow \frac{\mathbb{Z}}{(n)} \\ (\bar{x}, \bar{y}) \mapsto \overline{xy}.$$

a) Prouver que la correspondance μ est une application [c'est-à-dire que : $(\bar{x}' = \bar{x} \text{ et } \bar{y}' = \bar{y}) \Rightarrow \overline{x'y'} = \overline{xy}$].

En déduire que l'on peut définir dans $\frac{\mathbb{Z}}{(n)}$ une « multiplication » telle que $\bar{x}\bar{y} = \overline{xy}$.

Montrer alors que $\frac{\mathbb{Z}}{(n)}$ est un anneau unitaire et commutatif (voir : définition (0.1) de l'Introduction).

b) Soit, dans \mathbb{N} , un nombre premier p . On désigne par G_p l'ensemble des éléments non nuls de $\frac{\mathbb{Z}}{(p)}$.

Prouver, en utilisant le résultat de l'exercice 4, que G_p est un groupe par rapport à la multiplication définie dans $\frac{\mathbb{Z}}{(p)}$.

En conclure que $\frac{\mathbb{Z}}{(p)}$ est un corps (voir définition (0.2) de l'Introduction).

c) Vérifier que si n n'est pas premier $\frac{\mathbb{Z}}{(n)}$ n'est pas un corps.

22) Vérifier que

$$\Gamma = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \right\}$$

est un sous-groupe de $GL(2, \mathbb{R})$ isomorphe au groupe $GL\left(2, \frac{\mathbb{Z}}{(2)}\right)$.

Ecrire la table de multiplication du groupe Γ ; en déduire que Γ est isomorphe au groupe symétrique S_3 .

23) a) Démontrer les résultats suivants :

$$\Gamma_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

est un sous-groupe de $\text{GL}(2, \mathbf{R})$.

$$\Gamma_2 = \{1, i, -1, -i\}$$

où $i^2 = -1$ est un sous-groupe de (\mathbf{C}^*, \times) .

$$\Gamma_3 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\},$$

sous-ensemble de $\frac{\mathbf{Z}}{(5)}$, est un groupe par rapport à la multiplication définie dans $\frac{\mathbf{Z}}{(5)}$ (exercice 21).

b) Prouver que Γ_1 , Γ_2 , Γ_3 sont trois groupes isomorphes. Sont-ils cycliques?

24) a) Montrer que :

$$K_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

est un sous-groupe de $\text{GL}(2, \mathbf{R})$ et que $K_2 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, sous-ensemble de $\frac{\mathbf{Z}}{(8)}$ est un groupe par rapport à la multiplication définie dans $\frac{\mathbf{Z}}{(8)}$ (exercice 21).

b) Vérifier que les groupes K_1 et K_2 sont isomorphes.

Ces groupes sont-ils isomorphes au groupe de Klein (exemple (1.83))?

25) Définition : étant donné un groupe G , on appelle *représentation matricielle* de G , de degré n ($n \in \mathbf{N}$) sur un corps K , tout morphisme $\rho \in \text{Hom}(G, \text{GL}(n, K))$.

Si ρ est *injectif*, on dit que la représentation matricielle est *fidèle*.

a) Montrer que le groupe symétrique S_3 (exercice 22), les groupes Γ_2 et Γ_3 de l'exercice 23 et le groupe K_2 de l'exercice 24 admettent chacun une représentation matricielle fidèle de degré 2 sur \mathbf{R} .

b) En associant à tout nombre complexe non nul $a + ib$ la matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, vérifier que le groupe multiplicatif \mathbf{C}^* admet aussi une représentation fidèle de degré 2 sur \mathbf{R} .

26) [1] Soit P le plan affine euclidien. Si f est une isométrie du plan P (exemple (1.34)), on dit qu'un point A est *fixe* pour f , si $f(A) = A$.

On désigne par $\mathcal{J}(2)$ l'ensemble des isométries du plan P .

Si Δ est une droite de P , on note s_Δ la symétrie du plan par rapport à Δ ; $s_\Delta: P \rightarrow P$, $A' \mapsto A'$ est tel que Δ est médiatrice de AA' .

a) Vérifier les propriétés suivantes :

- l'identité de P , notée id_P , appartient à $\mathcal{J}(2)$;
- quelle que soit la droite Δ , $s_\Delta \in \mathcal{J}(2)$ et $s_\Delta^2 = s_\Delta \circ s_\Delta = \text{id}_P$;
- si f_1 et f_2 sont dans $\mathcal{J}(2)$, alors $f_2 \circ f_1 \in \mathcal{J}(2)$; $f_2 \circ f_1$ sera appelé « produit » de f_1 et f_2 dans $\mathcal{J}(2)$.

b) Soit $f \in \mathcal{J}(2)$; montrer que :

- si f a deux points fixes distincts A et B , alors tout point de la droite AB est fixe pour f ;
- si f a trois points fixes, A , B , C , non alignés, alors $f = \text{id}_P$.

c) Démontrer que toute isométrie $f \in \mathcal{J}(2)$ est le produit de 0, 1, 2 ou 3 symétries (par convention, quel que soit la droite Δ , $s_\Delta^0 = \text{id}_P$).

d) Prouver que $\mathcal{J}(2)$ est un sous-groupe du groupe symétrique S_P et que $\mathcal{J}(2)$ est non abélien.

e) A tout vecteur v de l'espace vectoriel \mathbf{R}^2 , on associe la translation de vecteur v du plan affine P , notée t_v .

Montrer à l'aide de c) que $t_v \in \mathcal{J}(2)$ et que $\mathcal{E}(P) = \{t_v; v \in \mathbf{R}^2\}$ est un sous-groupe abélien de $\mathcal{J}(2)$, isomorphe à $(\mathbf{R}^2, +)$.

f) Soit O un point du plan P , pour $\alpha \in \mathbf{R}$, on note $r_{0,\alpha}$ la rotation du plan P de centre O et d'angle α .

Montrer à l'aide de c) que $r_{0,\alpha} \in \mathcal{J}(2)$. $\mathcal{R}(P, O)$ désignant l'ensemble de toutes les rotations $r_{0,\alpha}$ pour $\alpha \in \mathbf{R}$, vérifier que $\mathcal{R}(P, O) = \{r_{0,\alpha}; 0 \leq \alpha < 2\pi\}$ et que $\mathcal{R}(P, O)$ est un sous-groupe abélien de $\mathcal{J}(2)$.

27) Notons \mathbf{C} le plan complexe, c'est-à-dire le plan affine euclidien \mathbf{R}^2 rapporté à un système d'axes orthonormé Oxy et dont tout point $M(x, y)$ est considéré comme l'image du nombre complexe $z = x + iy$.

A toute famille de 4 nombres complexes (a, b, c, d) telle que $ad - bc \neq 0$, on associe l'application

$$f: z \mapsto \frac{az + b}{cz + d}, \quad \text{où } z \in \mathbf{C}.$$

On remarque que si $c \neq 0$, le point $-\frac{d}{c}$ n'a aucune image par f ; d'autre part, le point $\frac{a}{c}$ n'est l'image d'aucun point de \mathbf{C} .

Pour remédier à ces difficultés, on rajoute au plan complexe un point dit point à l'infini et noté ∞ .

On pose $\tilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, pour $c \neq 0$, $f\left(-\frac{d}{c}\right) = \infty$ et $f(\infty) = \frac{a}{c}$.

Une application telle que f est appelée *homographie* du plan complexe.

(Compte tenu de l'interprétation géométrique des homographies à l'aide de la projection stéréographique de la sphère, $\tilde{\mathbb{C}}$ est appelé sphère de Riemann [1].)

a) Montrer que toute homographie f est une permutation de $\tilde{\mathbb{C}}$.

b) Démontrer que l'ensemble \mathcal{H} des homographies du plan complexe est un sous-groupe du groupe symétrique $S_{\tilde{\mathbb{C}}}$.

c) En considérant le cas où $c = 0$, prouver que \mathcal{H} contient comme sous-groupe le groupe des similitudes et translations du plan complexe.

d) Vérifier que l'homographie $z \mapsto \frac{1}{z}$ est le produit (commutatif) de l'inversion de centre O et de puissance 1, et de la symétrie par rapport à l'axe Ox .

e) Démontrer que toute homographie f du plan complexe conserve les angles et leur orientation, ce que l'on exprime en disant que f est une transformation *conforme* du plan; la réciproque étant vraie [1], le groupe \mathcal{H} des homographies du plan complexe est aussi appelé *groupe des transformations conformes* du plan.

f) Prouver que les homographies :

$$f_1: z \mapsto z, \quad f_2: z \mapsto -z, \quad f_3: z \mapsto \frac{1}{z}, \quad f_4: z \mapsto -\frac{1}{z}$$

forment un sous-groupe de \mathcal{H} isomorphe au groupe de Klein.

g) Prouver que les homographies :

$$g_1: z \mapsto z, \quad g_2: z \mapsto \frac{1}{1-z}, \quad g_3: z \mapsto \frac{z-1}{z},$$

$$g_4: z \mapsto \frac{1}{z}, \quad g_5: z \mapsto 1-z, \quad g_6: z \mapsto \frac{z}{z-1},$$

forment un sous-groupe de \mathcal{H} isomorphe au groupe symétrique S_3 .

28) a) Démontrer le corollaire (1.49).

b) Démontrer la proposition (1.53).

- 29) Soient E un ensemble non vide et G un groupe d'élément unité e . On désigne par G^E l'ensemble des applications f de E dans G . On considère la loi de composition définie dans G^E par :

$$G^E \times G^E \rightarrow G^E$$

$$(f, g) \mapsto fg,$$

où fg est telle que, pour tout $x \in E$, $fg(x) = f(x)g(x)$.

Prouver que G^E est ainsi muni d'une structure de groupe.

Vérifier que G^E est un groupe abélien si et seulement si G est abélien.

- 30) \mathbf{R} désignant le groupe additif des nombres réels, on pose

$$J = \{x \in \mathbf{R}; 0 \leq x \leq 1\}.$$

L'addition de \mathbf{R} induit dans l'ensemble \mathbf{R}^J une structure de *groupe additif abélien* (voir exercice 29).

a) Vérifier les propriétés suivantes :

- l'ensemble des fonctions $f \in \mathbf{R}^J$, continues sur J , est un sous-groupe de $(\mathbf{R}^J, +)$, que l'on notera $\mathcal{C}(J)$;
- si, pour tout $a \in \mathbf{R}$, on note c_a la fonction constante de J dans \mathbf{R} telle que $c_a(x) = a$ pour tout $x \in J$, alors $\Gamma = \{c_a; a \in \mathbf{R}\}$ est un sous-groupe de $(\mathcal{C}(J), +)$.

b) On considère les applications F_i de $\mathcal{C}(J)$ dans \mathbf{R} telles que :

$$F_1: f \mapsto f(1), \quad F_2: f \mapsto |f(0)|, \quad F_3: f \mapsto \int_0^1 f(x) dx$$

$$F_4: f \mapsto \frac{\pi}{3} \int_0^1 f(x) \cos \frac{\pi x}{6} dx, \quad F_5: f \mapsto \int_0^1 \cos \frac{\pi(f(x))}{6} dx.$$

Déterminer les F_i qui sont des morphismes de groupes de $(\mathcal{C}(J), +)$ dans $(\mathbf{R}, +)$. Pour chacun des morphismes de groupes F_i , prouver que, quel que soit $a \in \mathbf{R}$, $F_i(c_a) = a$ et montrer qu'il existe un unique $m_i \in \mathbf{R}$ tel que $F_i(\text{id}_J - c_{m_i}) = 0$. En déduire que les $\text{Ker } F_i$ sont deux à deux distincts.

c) Démontrer que pour tout $F \in \text{Hom}(\mathcal{C}(J), \mathbf{R})$, tel que $F(c_a) = a$, quel que soit $a \in \mathbf{R}$, on a

$$\mathcal{C}(J) = \text{Ker } F \oplus \Gamma.$$

En conclure qu'il existe de nombreux sous-groupes H de $\mathcal{C}(J)$ tels que $\mathcal{C}(J) = H \oplus \Gamma$.

- 31) *a)* Soient deux groupes G_1 et G_2 ; prouver que les groupes $G_1 \times G_2$ et $G_2 \times G_1$ sont isomorphes.
b) Γ_1 et Γ_2 étant aussi deux groupes, démontrer la propriété :
 $(\Gamma_1 \simeq G_1 \text{ et } \Gamma_2 \simeq G_2) \Rightarrow \Gamma_1 \times \Gamma_2 \simeq G_1 \times G_2$.
c) Montrer que tout sous-groupe de $G_1 \times G_2$ est de la forme $H_1 \times H_2$ où H_1 et H_2 sont respectivement des sous-groupes de G_1 et G_2 .
- 32) Pour deux groupes G_1 et G_2 , démontrer les propriétés :
a) $G_1 \simeq G_2 \Rightarrow \text{Aut}(G_1) \simeq \text{Aut}(G_2)$
b) $G_1 \simeq G_2 \Rightarrow \text{Int}(G_1) \simeq \text{Int}(G_2)$.
- 33) Soit $\{G_i\}_{i \in I}$ une famille de groupes; montrer que, pour tout groupe G , l'ensemble $\text{Hom}(G, \prod_{i \in I} G_i)$ est équipotent à l'ensemble $\prod_{i \in I} (\text{Hom}(G, G_i))$. [Voir le théorème (1.91).]

CHAPITRE II

Classes modulo un sous-groupe

Sauf indication contraire, un groupe G quelconque est noté multiplicativement et e désigne son élément unité.

1 — Classes à droite, classes à gauche modulo un sous-groupe

A / Relations d'équivalence modulo un sous-groupe

A tout sous-groupe H d'un groupe G , on peut associer deux relations binaires \mathcal{R}_H et ${}_H\mathcal{R}$ définies dans G par :

$$x \mathcal{R}_H y \Leftrightarrow xy^{-1} \in H \quad \text{et} \quad x {}_H\mathcal{R} y \Leftrightarrow x^{-1}y \in H.$$

PROPOSITION (2.1). G étant un groupe :

- 1) Pour tout sous-groupe H de G , les relations \mathcal{R}_H et ${}_H\mathcal{R}$ sont des relations d'équivalence.
- 2) $y \equiv x(\mathcal{R}_H) \Leftrightarrow y \in Hx$, où $Hx = \{hx; h \in H\}$;
 $y \equiv x({}_H\mathcal{R}) \Leftrightarrow y \in xH$, où $xH = \{xh; h \in H\}$.

Preuve : Démontrons la propriété pour \mathcal{R}_H .

1) Pour tout $x \in G$, on a $xx^{-1} = e \in H$, donc $x \mathcal{R}_H x$.

Si $xy^{-1} \in H$, alors $(xy^{-1})^{-1} = yx^{-1} \in H$, donc $x \mathcal{R}_H y \Rightarrow y \mathcal{R}_H x$.

Enfin, si $xy^{-1} \in H$ et $yz^{-1} \in H$, alors $xy^{-1}yz^{-1} = xz^{-1} \in H$,

d'où $x \mathcal{R}_H y$ et $y \mathcal{R}_H z \Rightarrow x \mathcal{R}_H z$.

$$2) \quad y \equiv x(\mathcal{R}_H) \Leftrightarrow yx^{-1} \in H$$

$$yx^{-1} \in H \Leftrightarrow \exists h \in H, y = hx,$$

$$\text{d'où} \quad y \equiv x(\mathcal{R}_H) \Leftrightarrow y \in Hx.$$

Définitions (2.2) : H étant un sous-groupe d'un groupe G , les relations \mathcal{R}_H et ${}_H\mathcal{R}$ sont respectivement appelées : *relation d'équivalence à droite* et *à gauche, modulo H* dans G .

Pour $x \in G$, les ensembles Hx et xH sont appelés *classes à droite* et *classes à gauche de x modulo H* .

Remarques (2.3) :

1° Les conventions « à droite » et « à gauche » adoptées ici sont les plus couramment utilisées par les algébristes, cependant, certains auteurs préfèrent les conventions opposées, c'est en particulier le cas de S. Mac Lane et G. Birkhoff dans [54].

2° Si le groupe G est noté additivement, \mathcal{R}_H et ${}_H\mathcal{R}$ sont définies par :

$$x \mathcal{R}_H y \Leftrightarrow (x - y) \in H \quad \text{et} \quad x {}_H\mathcal{R} y \Leftrightarrow (-x + y) \in H.$$

Les classes à droite et à gauche modulo H d'un élément $x \in G$ sont respectivement :

$$H + x = \{h + x; h \in H\} \quad \text{et} \quad x + H = \{x + h; h \in H\}.$$

3° Les classes à droite modulo H étant des classes d'équivalence, on a :

$$Hx \neq Hy \Rightarrow Hx \cap Hy = \emptyset$$

et si $\{x_i\}_{i \in I}$ est une famille de représentants des classes à droite modulo H , *distinctes*, alors la famille $\{Hx_i\}_{i \in I}$ forme une *partition* de G :

$$G = \bigcup_{i \in I} Hx_i \quad \text{et} \quad Hx_i \neq Hx_j \Leftrightarrow i \neq j.$$

La même remarque est valable pour les classes à gauche modulo H .

4° Si $H = G$, pour tout $x \in G$, on a $Gx = xG = G$, donc $\mathcal{R}_G = {}_G\mathcal{R}$ est l'équivalence universelle dans G .

Si $H = (e)$, pour tout $x \in G$, $\{x\}$ est à la fois classe à droite et classe à gauche de x modulo (e) , donc $\mathcal{R}_{(e)} = {}_{(e)}\mathcal{R}$ est l'égalité dans G .

5° Quel que soit $H \leq G$ et quel que soit $h \in H$, on a $Hh = hH = H$, donc H est à la fois classe à droite et classe à gauche de h modulo H ; en particulier, H est classe à droite et à gauche de e modulo H .

6° Si le groupe G est abélien, quel que soit $H \leq G$, et quel que soit $x \in G$, on a $Hx = xH$, donc $\mathcal{R}_H = {}_H\mathcal{R}$.

Dans ce cas, deux éléments x et y de G , équivalents modulo $\mathcal{R}_H (= {}_H\mathcal{R})$, seront dits *équivalents modulo H* ; on écrira : $x \equiv y \pmod{H}$.

L'ensemble quotient de G par $\mathcal{R}_H (= {}_H\mathcal{R})$ sera noté $\frac{G}{H}$ et appelé *quotient* de G par H .

7° Si le groupe G est non abélien, alors, pour $H \neq (e)$, $H \neq G$ et $x \notin H$, on a, en général, $Hx \neq xH$, donc $\mathcal{R}_H \neq {}_H\mathcal{R}$.

Les ensembles quotients $\frac{G}{\mathcal{R}_H}$ et $\frac{G}{{}_H\mathcal{R}}$ seront respectivement notés $\left(\frac{G}{H}\right)_d$ et $\left(\frac{G}{H}\right)_g$.

Exemple (2.4) : Considérons le groupe symétrique S_3 qui est engendré par :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{et} \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

(voir exemple (1.41)).

Pour simplifier l'écriture, posons ici : $\sigma = \sigma_1$ et $\tau = \tau_3$; on a alors $S_3 = \{e, \tau, \sigma, \sigma^2, \tau \circ \sigma, \sigma \circ \tau\}$.

Soit $H = \langle \tau \rangle = \{e, \tau\}$. Les classes à droite et à gauche de S_3 modulo H sont respectivement :

$$\left\{ \begin{array}{l} H = \{e, \tau\} \\ H\sigma = \{\sigma, \tau \circ \sigma\} \\ H\sigma^2 = \{\sigma^2, \tau \circ \sigma^2 = \sigma \circ \tau\} \end{array} \right\} \quad \left\{ \begin{array}{l} H = \{e, \tau\} \\ \sigma H = \{\sigma, \sigma \circ \tau\} \\ \sigma^2 H = \{\sigma^2, \sigma^2 \circ \tau = \tau \circ \sigma\} \end{array} \right\}$$

$$\tau \circ \sigma \neq \sigma \circ \tau \Rightarrow H\sigma \neq \sigma H, \quad \text{d'où } \mathcal{R}_H \neq {}_H\mathcal{R}.$$

Exemple (2.5) : Soit $H = n\mathbf{Z}$ un sous-groupe de $(\mathbf{Z}, +)$. Le groupe $(\mathbf{Z}, +)$ étant abélien, on a $\mathcal{R}_H = {}_H\mathcal{R}$ et :

$$x \equiv y \pmod{n\mathbf{Z}} \quad \Leftrightarrow \quad (x - y) \in n\mathbf{Z},$$

$$\text{d'où} \quad x \equiv y \pmod{n\mathbf{Z}} \quad \Leftrightarrow \quad x \equiv y \pmod{n}$$

(voir exemple (1.13)).

Autrement dit, l'équivalence modulo $n\mathbf{Z}$ coïncide avec la congruence modulo n , d'où

$$\frac{\mathbf{Z}}{n\mathbf{Z}} = \frac{\mathbf{Z}}{(n)}.$$

Le quotient de \mathbf{Z} par un sous-groupe $n\mathbf{Z}$ est donc muni d'une structure de groupe, induite par celle de \mathbf{Z} (exemple (1.13)); nous verrons plus loin (proposition (2.24)) qu'il en est de même pour tout quotient d'un groupe *abélien* par l'un quelconque de ses groupes.

B / Théorème de Lagrange. Indice d'un sous-groupe

PROPOSITION (2.6). *Soient G un groupe et H un sous-groupe de G , alors toute classe à droite Hx (resp^t à gauche xH) est équipotente à H .*

Preuve : On sait que deux ensembles sont dits équipotents s'il existe une bijection de l'un sur l'autre.

Dans le cas présent, on vérifie facilement que l'application $\gamma : H \rightarrow Hx$ est une bijection, d'où le résultat énoncé.

$$h \mapsto hx$$

COROLLAIRE (2.7). *Dans un groupe G , deux classes à droite ou à gauche modulo un sous-groupe H sont équipotentes.*

En effet, deux ensembles équipotents à un même troisième sont équipotents.

COROLLAIRE (2.8). *Si H est un sous-groupe fini d'un groupe quelconque G , alors, toute classe à droite Hx , ou à gauche xH , est un ensemble fini de même cardinal que H .*

THÉORÈME (2.9). (*Théorème de Lagrange*) ⁽¹⁾.

Si G est un groupe fini, alors l'ordre de tout sous-groupe H de G divise l'ordre de G .

Preuve : Soit $H \leq G$, considérons la famille des classes à droite; distinctes, modulo H dans G ; cette famille forme une partition de G .

G étant fini, il n'y a qu'un nombre fini de classe à droite distinctes modulo H ; soit k ce nombre.

Si $n = o(G)$ et $m = o(H)$, alors chaque classe à droite modulo H a m éléments, d'où $n = km$ et par suite $m = o(H)$ divise $n = o(G)$.

COROLLAIRE (2.10). Si G est un groupe fini, quel que soit $x \in G$, l'ordre de x divise l'ordre de G .

En effet, l'ordre de x est l'ordre du sous-groupe de G engendré par x .

COROLLAIRE (2.11). Si G est un groupe fini, pour tout sous-groupe H de G , le nombre des classes à droite modulo H est égal au nombre des classes à gauche modulo H .

En effet, d'après la démonstration du théorème de Lagrange, qui peut aussi être faite en prenant les classes à gauche, le nombre des classes à droite (resp^t à gauche) modulo H est égal à $\frac{o(G)}{o(H)}$.

Nous allons démontrer, plus généralement, le résultat suivant :

THÉORÈME (2.12). Pour tout sous-groupe H d'un groupe G , les ensembles $\left(\frac{G}{H}\right)_a$ et $\left(\frac{G}{H}\right)_g$ sont équipotents.

Preuve : Considérons la correspondance

$$\begin{aligned} \theta : \left(\frac{G}{H}\right)_a &\rightarrow \left(\frac{G}{H}\right)_g \\ Hx &\mapsto x^{-1}H. \end{aligned}$$

(1) Joseph-Louis Lagrange (comte de), mathématicien français (1736-1813).

— Montrons que θ est une application; il s'agit de prouver que

$$Hx = Hy \text{ implique } x^{-1}H = y^{-1}H;$$

or
$$Hx = Hy \Leftrightarrow xy^{-1} \in H$$

$$xy^{-1} \in H \Rightarrow y^{-1} \in x^{-1}H$$

et
$$y^{-1} \in x^{-1}H \Rightarrow y^{-1}H = x^{-1}H.$$

— θ est injective; en effet, supposons $\theta(Hx) = \theta(Hy)$, c'est-à-dire $x^{-1}H = y^{-1}H$. On a alors $xy^{-1} \in H$, d'où $Hx = Hy$.

— θ est surjective, car pour tout élément xH de $\left(\frac{G}{H}\right)_o$ on peut écrire $xH = \theta(Hx^{-1})$.

En conclusion : θ est une bijection, d'où le théorème.

Remarque (2.13) : En théorie des ensembles, l'équipotence de deux ensembles s'exprime par l'égalité de leurs cardinaux. Le résultat du théorème (2.12) se traduit donc par la relation :

$$\text{card} \left(\left(\frac{G}{H} \right)_d \right) = \text{card} \left(\left(\frac{G}{H} \right)_o \right) \quad (1)$$

Définition (2.14) : Étant donné un sous-groupe H d'un groupe G , le cardinal de $\left(\frac{G}{H} \right)_d \left(= \text{card} \left(\left(\frac{G}{H} \right)_o \right) \right)$ s'appelle l'indice de H dans G et se note $[G : H]$.

Si $[G : H]$ est fini, on dit que H est d'indice fini dans G .

PROPOSITION (2.15). Si G est un groupe fini, alors pour tout sous-groupe H de G , on a

$$o(G) = o(H) [G : H] \quad (2)$$

Preuve : Dans le cas où G est fini, $[G : H]$ est égal au nombre des classes à droite (resp^t à gauche) modulo H , d'où, d'après la démonstration du théorème de Lagrange, $[G : H] = \frac{o(G)}{o(H)}$.

Remarque (2.16) :

1° $[G : H]$ peut être fini, sans que ni G , ni H le soit. Par exemple, dans $(\mathbb{Z}, +)$ pour tout sous-groupe *non nul* $n\mathbb{Z}$, on sait que $\frac{\mathbb{Z}}{n\mathbb{Z}} = \frac{\mathbb{Z}}{(n)}$, donc

$$[\mathbb{Z} : n\mathbb{Z}] = n \quad (3)$$

2° Pour tout groupe G , on a

$$[G : G] = 1 \quad \text{et} \quad [G : (e)] = \text{card } G;$$

en particulier, si G est fini, $[G : (e)] = o(G)$.

THÉORÈME (2.17). (*Théorème de Poincaré*) ⁽²⁾.

Dans un groupe, l'intersection d'un nombre fini de sous-groupes d'indices finis est un sous-groupe d'indice fini.

Preuve : Soit $\{H_i\}_{1 \leq i \leq n}$ une famille finie ($n \geq 2$ dans \mathbf{N}) de sous-groupes d'un groupe G , tels que pour tout i ($1 \leq i \leq n$), $[G : H_i]$ est fini. Montrons que $[G : \bigcap_{1 \leq i \leq n} H_i]$ est fini.

— Considérons le cas $n = 2$. Pour tout $x \in G$, on a

$$(H_1 \cap H_2) x \subseteq H_1 x \cap H_2 x.$$

D'autre part, soit $y \in H_1 x \cap H_2 x$; alors

$$(yx^{-1} \in H_1 \quad \text{et} \quad yx^{-1} \in H_2) \Rightarrow y \in (H_1 \cap H_2) x,$$

$$\text{d'où} \quad (H_1 \cap H_2) x = H_1 x \cap H_2 x \quad (4)$$

Par hypothèse, les classes à droite distinctes modulo H_1 , et modulo H_2 , sont en nombres finis, respectivement, $[G : H_1]$ et $[G : H_2]$ et d'après (4) on a

$$[G : H_1 \cap H_2] \leq [G : H_1] [G : H_2] \quad (5)$$

par suite, $[G : H_1 \cap H_2]$ est fini.

— En raisonnant par récurrence, on montre alors que la propriété est vraie pour tout $n > 2$.

(²) Henri-Jules Poincaré, mathématicien français (1854-1912).

C / Formule des indices

THÉORÈME (2.18). *Si H est un sous-groupe d'indice fini dans un groupe G et si K est un sous-groupe de G contenant H , alors K est d'indice fini dans G et :*

$$[G : H] = [G : K] [K : H] \quad (6)$$

La formule (6) sera appelée : *formule des indices*.

Preuve : Soit $\{x_i\}_{i \in I}$ une famille de représentants des classes à droite distinctes modulo K dans G .

La famille des $\{Kx_i\}_{i \in I}$ forme une partition de G :

$$G = \bigcup_{i \in I} Kx_i, \quad Kx_i \neq Kx_j \Leftrightarrow i \neq j$$

et $\text{card}(I) = [G : K].$

Soit $\{y_\lambda\}_{\lambda \in \Lambda}$ une famille de représentants des classes à droites distinctes modulo H dans K . On a :

$$K = \bigcup_{\lambda \in \Lambda} Hy_\lambda, \quad Hy_\lambda \neq Hy_\mu \Leftrightarrow \lambda \neq \mu$$

et $\text{card}(\Lambda) = [K : H].$

Soit $g \in G$, il existe un unique $i \in I$ tel que $g \in Kx_i$.

On en déduit qu'il existe un unique $a \in K$ tel que $g = ax_i$.

D'autre part, il existe un unique $\lambda \in \Lambda$ tel que $a \in Hy_\lambda$.

On en déduit que $g \in Hy_\lambda x_i$; par suite, on a :

$$G = \bigcup_{(\lambda, i) \in \Lambda \times I} Hy_\lambda x_i.$$

Démontrons que la famille des $Hy_\lambda x_i$, pour $(\lambda, i) \in \Lambda \times I$ forme une partition de G . Supposons $Hy_\lambda x_i = Hy_\mu x_j$.

$$H \subseteq K \Rightarrow KH = K;$$

or $Hy_\lambda x_i = Hy_\mu x_j \Rightarrow KH y_\lambda x_i = KH y_\mu x_j.$

$$KH y_\lambda = Ky_\lambda = K, \text{ car } y_\lambda \in K; \text{ de même } KH y_\mu = K;$$

on en déduit :

$$Kx_i = Kx_j, \quad \text{d'où } i = j;$$

par suite, on a

$$Hy_\lambda = Hy_\mu, \quad \text{d'où } \lambda = \mu.$$

La famille $\{y_\lambda x_i\}_{(\lambda, i) \in \Lambda \times I}$ est donc une famille de représentants des classes à droite distinctes de G modulo H , d'où :

$$[G : H] = \text{card}(\Lambda \times I).$$

Par hypothèse, $[G : H]$ est fini, par suite, Λ et I sont des ensembles finis, en particulier :

$$[G : K] = \text{card}(I) \text{ est fini}$$

et $\text{card}(\Lambda \times I) = \text{card}(\Lambda) \text{card}(I)$ implique :

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

Remarque (2.19) : Le théorème (2.18) peut être généralisé dans le sens suivant : si H et K sont deux sous-groupes de G tels que $H \subseteq K$, alors la formule (6) est valable dès que deux quelconques des indices qui y figurent sont finis et le troisième est alors fini.

2 — Propriétés des relations d'équivalence modulo un sous-groupe

A / *Comptabilité d'une relation d'équivalence avec une loi de composition*

Soit \mathcal{R} une relation d'équivalence définie dans un ensemble (E, \cdot) . On dit que :

1° \mathcal{R} est compatible à droite (resp^t à gauche) avec la loi \cdot , si, quels que soient x, y, a dans E ,

$$x \mathcal{R} y \Rightarrow x.a \mathcal{R} y.a \tag{7}$$

$$(\text{resp}^t \ x \mathcal{R} y \Rightarrow a.x \mathcal{R} a.y) \tag{7'}$$

2° \mathcal{R} est compatible avec la loi \cdot , si, quels que soient x, x', y, y' dans E ,

$$(x \mathcal{R} x' \text{ et } y \mathcal{R} y') \Rightarrow x \cdot y \mathcal{R} x' \cdot y' \quad (8)$$

PROPOSITION (2.20). Une relation d'équivalence \mathcal{R} définie dans un ensemble (E, \cdot) est compatible avec la loi \cdot , si et seulement si elle est compatible à droite et à gauche avec cette loi.

Démonstration laissée au lecteur.

\mathcal{R} étant une relation d'équivalence dans (E, \cdot) , posons $\bar{E} = \frac{E}{\mathcal{R}}$ et $\bar{x} = \text{cl}_{\mathcal{R}}(x)$, pour tout $x \in E$.

PROPOSITION (2.21). Compte tenu des notations ci-dessus, la correspondance $\lambda : \bar{E} \times \bar{E} \rightarrow \bar{E}$ définit une loi de composition interne dans \bar{E} ,

$$(\bar{x}, \bar{y}) \mapsto \overline{x \cdot y}$$

si et seulement si \mathcal{R} est compatible avec la loi \cdot .

Dans ce cas, la loi de composition interne définie par λ est appelée loi quotient de celle de E par \mathcal{R} ; en général, elle est encore notée \cdot et quels que soient \bar{x} et \bar{y} dans \bar{E} , on a :

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y} \quad (9)$$

Preuve : λ définit une loi de composition interne dans \bar{E} si et seulement si λ est une application, c'est-à-dire, si et seulement si, quels que soient $\bar{x}, \bar{x}', \bar{y}, \bar{y}'$ dans \bar{E} :

$$(\bar{x} = \bar{x}' \text{ et } \bar{y} = \bar{y}') \Rightarrow \overline{x \cdot y} = \overline{x' \cdot y'} \quad (10)$$

or la relation (10) équivaut à (8), d'où la propriété énoncée.

Remarques (2.22) :

1° Les définitions de l'addition et de la multiplication dans $\frac{\mathbf{Z}}{(n)}$ (exemple (1.13) et exercice 21, chap. I^{er}) sont une illustration de la proposition (2.21).

2° La formule (9) implique que si, dans E , la loi \cdot est associative ou commutative, il en est de même de la loi quotient

dans \bar{E} ; de plus, si e est élément neutre dans (E, \cdot) , alors \bar{e} est élément neutre dans (\bar{E}, \cdot) et si $x \in E$ admet un symétrique x^{-1} dans E , \bar{x} est symétrisable dans \bar{E} et $\bar{x}^{-1} = \overline{x^{-1}}$.

B / Propriétés des relations du type \mathcal{R}_H et ${}_H\mathcal{R}$.
Premier théorème d'isomorphisme

a) Cas général :

PROPOSITION (2.23). Pour tout sous-groupe H d'un groupe G , la relation d'équivalence \mathcal{R}_H (resp^t ${}_H\mathcal{R}$) est compatible à droite (resp^t à gauche) avec la loi de composition de G .

Réciproquement, si \mathcal{R} est une relation d'équivalence définie dans un groupe G , compatible à droite (resp^t à gauche) avec la loi de composition du groupe, alors il existe un unique sous-groupe H de G tel que $\mathcal{R} = \mathcal{R}_H$ (resp^t $\mathcal{R} = {}_H\mathcal{R}$).

Preuve :

1° H étant un sous-groupe de G , supposons x et y dans G , tels que $x \mathcal{R}_H y$ et soit $a \in G$.

$$x \mathcal{R}_H y \Leftrightarrow xy^{-1} \in H;$$

$$\text{or} \quad (xa)(ya)^{-1} = x(aa^{-1})y^{-1} = xy^{-1},$$

$$\text{d'où} \quad (x \mathcal{R}_H y \text{ et } a \in G) \Rightarrow xa \mathcal{R}_H ya.$$

2° Réciproquement, \mathcal{R} étant une relation d'équivalence définie dans G et compatible à droite avec la loi de composition du groupe, désignons par H la classe d'équivalence de e modulo \mathcal{R} et montrons que H est un sous-groupe de G . $e \in H \Rightarrow H \neq \emptyset$; pour x et y dans H , on a $x \mathcal{R} e$ et $y \mathcal{R} e$; la compatibilité à droite de \mathcal{R} avec la loi de composition de G implique alors : $xy^{-1} \mathcal{R} y^{-1}$ et $e \mathcal{R} y^{-1}$, donc $xy^{-1} \mathcal{R} e$ et par suite $xy^{-1} \in H$.

Vérifions maintenant que $\mathcal{R} = \mathcal{R}_H$.

Supposons $x \mathcal{R} y$; la compatibilité à droite de \mathcal{R} avec la loi de composition de G implique $xy^{-1} \mathcal{R} e$, d'où $xy^{-1} \in H$; on en déduit : $\mathcal{R} \subseteq \mathcal{R}_H$.

Supposons $x \mathcal{R}_H y$, c'est-à-dire $xy^{-1} \in H$.

$$xy^{-1} \in H \quad \Leftrightarrow \quad xy^{-1} \mathcal{R} e$$

et $xy^{-1} \mathcal{R} e \quad \Rightarrow \quad x \mathcal{R} y,$

par multiplication à droite par y , d'où $\mathcal{R}_H \subseteq \mathcal{R}$; on en conclut que $\mathcal{R} = \mathcal{R}_H$.

b) Cas où le groupe G est abélien.

Pour tout sous-groupe H de G , on a alors $\mathcal{R}_H = {}_H\mathcal{R}$ (remarques (2.3) 6°); cette relation d'équivalence est, d'après les propositions (2.23) et (2.20), compatible avec la loi de composition de G ; par suite, l'ensemble quotient de G par $\mathcal{R}_H (= {}_H\mathcal{R})$, noté $\frac{G}{H}$, est muni de la loi de composition quotient de celle de G (proposition (2.21)) telle que quels que soient \bar{x} et \bar{y} dans $\frac{G}{H}$:

$$\bar{x}\bar{y} = \overline{xy} \quad (11)$$

De la remarque (2.8) 2°, on déduit alors le résultat suivant :

PROPOSITION (2.24). *Si G est un groupe abélien, pour tout sous-groupe H de G , la relation d'équivalence $\mathcal{R}_H = {}_H\mathcal{R}$ est compatible avec la loi de composition de G et l'ensemble $\frac{G}{H}$ muni de la loi de composition quotient de celle de G par $\mathcal{R}_H (= {}_H\mathcal{R})$ est un groupe abélien.*

Remarques (2.25) :

1° G étant abélien, pour tout $\bar{x} \in \frac{G}{H}$, on a $\bar{x} = Hx = xH$.

La formule (11) peut donc s'écrire sous la forme :

$$(Hx)(Hy) = Hxy \quad (\text{ou} \quad (xH)(yH) = xyH) \quad (12)$$

En notation additive, (11) et (12) deviennent :

$$\bar{x} + \bar{y} = \overline{x + y} \quad (11')$$

$$\begin{aligned} (H + x) + (H + y) &= H + (x + y) \\ (\text{ou} \quad (x + H) + (y + H) &= (x + y) + H) \end{aligned} \quad (12')$$

2° Si π est la surjection canonique : $G \rightarrow \frac{G}{H}$, alors, compte

$$x \mapsto \bar{x}$$

tenu de (11), π est un épimorphisme de groupes.

c) Cas où le sous-groupe H de G est le noyau d'un morphisme de groupes.

Soient deux groupes quelconques G et G' et $f \in \text{Hom}(G, G')$.

Posons $H = \text{Ker } f$ et considérons les relations \mathcal{R}_H et ${}_H\mathcal{R}$.

Dans G , on a :

$$x \mathcal{R}_H y \Leftrightarrow xy^{-1} \in \text{Ker } f$$

$$x \mathcal{R}_H y \Leftrightarrow f(xy^{-1}) = e', \text{ élément unité de } G'.$$

$$x \mathcal{R}_H y \Leftrightarrow f(x) (f(y))^{-1} = e'$$

d'où $x \mathcal{R}_H y \Leftrightarrow f(x) = f(y).$

On vérifie de même que $x {}_H\mathcal{R} y \Leftrightarrow f(x) = f(y)$,
d'où $\mathcal{R}_H = {}_H\mathcal{R}$.

Posons alors $\frac{G}{H} = \left(\frac{G}{H}\right)_a = \left(\frac{G}{H}\right)_o$ (remarque (2.3), 7°).

Puisque $H = \text{Ker } f$, ce quotient sera plus précisément noté $\frac{G}{\text{Ker } f}$ et en s'appuyant, comme dans le cas abélien, sur les propositions (2.20), (2.21), (2.23) et la remarque (2.22) 2°, on obtient la propriété suivante :

PROPOSITION (2.26). Pour tout morphisme f d'un groupe G dans un groupe G' , l'ensemble quotient $\frac{G}{\text{Ker } f}$ est un groupe par rapport à la loi de composition quotient, définie par : $\bar{x}\bar{y} = \overline{xy}$, quels que soient \bar{x} et \bar{y} dans $\frac{G}{\text{Ker } f}$ et la surjection canonique $\pi : G \rightarrow \frac{G}{\text{Ker } f}$ est un épimorphisme de groupes.

$$x \mapsto \bar{x}$$

THÉORÈME (2.27). (1^{er} théorème d'isomorphisme) :

Pour tout morphisme f d'un groupe G dans un groupe G' , on a :

$$\frac{G}{\text{Ker } f} \simeq \text{Im } f.$$

Preuve : Considérons la correspondance

$$\varphi : \frac{G}{\text{Ker } f} \rightarrow \text{Im } f$$

$$\bar{x} \mapsto f(x).$$

— Montrons que φ est une *application*, c'est-à-dire que $\bar{x}' = \bar{x}$ implique $f(x') = f(x)$

$$\bar{x}' = \bar{x} \Leftrightarrow x' \mathcal{R}_H x, \quad \text{où } H = \text{Ker } f.$$

Or, on a vu plus haut que :

$$(x' \mathcal{R}_H x, \text{ avec } H = \text{Ker } f) \Leftrightarrow f(x') = f(x) \quad (13)$$

donc φ est bien une application.

— La définition de φ implique sa surjectivité.

— On remarque que (13) exprime l'injectivité de φ .

— Enfin

$$\varphi(\bar{x}\bar{x}') = \varphi(\overline{xx'}) = f(xx') = f(x)f(x'),$$

$$\text{d'où } \varphi(\bar{x}\bar{x}') = \varphi(\bar{x})\varphi(\bar{x}');$$

on en conclut que φ est un *isomorphisme* de groupes.

Exercices Chapitre II

1) Soient H et K deux sous-groupes *finis* d'un groupe G , tels que $o(H) = p$ et $o(K) = q$. Montrer que si p et q sont premiers entre eux, alors $H \cap K$ est réduit à l'élément neutre de G .

2) Soient H et K deux sous-groupes d'un groupe G . On suppose $[G : K]$ *fini*.

a) Soit $\{x_i\}_{i \in I}$ une famille de représentants des classes à droite distinctes de H modulo $H \cap K$.

— Démontrer que, dans G , on a :

$$Kx_i = Kx_j \Leftrightarrow i = j.$$

En déduire la relation : $[H : H \cap K] \leq [G : K]$; en conclure que $[H : H \cap K]$ est fini.

— Prouver que $[H : H \cap K] = [G : K]$, si $G = HK$.

b) On suppose de plus $[G : H]$ fini; montrer que les résultats précédents impliquent :

$$[G : H \cap K] \leq [G : H] [G : K] \quad (\text{formule (5) chap. II})$$

et que l'égalité a lieu si $G = HK$.

3) Soient H et K deux sous-groupes finis d'un groupe G .

On pose $[K : H \cap K] = n$. Soit $\{x_i\}_{1 \leq i \leq n}$ une famille de représentants des classes à droite distinctes de K modulo $H \cap K$.

a) Démontrer que les $\{Hx_i\}_{1 \leq i \leq n}$ forment une partition de l'ensemble HK (qui n'est pas nécessairement un sous-groupe).

b) $|HK|$ et $|KH|$ désignant les cardinaux de HK et KH , prouver que

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

c) Lorsque HK est un sous-groupe de G , vérifier que $o(HK)$, donné par la formule précédente, peut aussi être obtenu à partir du résultat b) de l'exercice 2 ci-dessus.

4) H et K étant deux sous-groupes d'un groupe G , on note F le sous-groupe de G engendré par $H \cup K$.

On suppose que $[F : H]$ et $[F : K]$ sont finis et premiers entre eux. A l'aide de résultats de l'exercice 2 prouver les égalités :

$$[F : K] = [H : H \cap K] \quad \text{et} \quad [F : H] = [K : H \cap K].$$

5) Soient H et K deux sous-groupes (non nécessairement distincts) d'un groupe G . On considère la relation binaire $\mathcal{R}_{H,K}$ définie dans G par :

$$x \mathcal{R}_{H,K} y \Leftrightarrow \exists (h, k) \in H \times K, \quad y = h x k.$$

a) Vérifier que $\mathcal{R}_{H,K}$ est une relation d'équivalence dans G et que la classe modulo $\mathcal{R}_{H,K}$ d'un élément $x \in G$ est $HxK = \{h x k; (h, k) \in H \times K\}$.

HxK sera appelée « classe double de x modulo H et K » [35].

b) x étant donné dans G , vérifier que l'application

$$\begin{aligned} \lambda : HxK &\rightarrow x^{-1} HxK \\ h x k &\mapsto x^{-1} h x k \end{aligned}$$

est une bijection.

c) On suppose que le groupe G est fini; soit $r \in \mathbf{N}^*$ le nombre des classes doubles distinctes, de G modulo H et K ; on les notera $Hx_i K$, $1 \leq i \leq r$.

Pour tout i ($1 \leq i \leq r$), justifier les propriétés suivantes :

$$\alpha) |Hx_i K| = |x_i^{-1} Hx_i K| \quad (\text{égalité des cardinaux});$$

$$\beta) x_i^{-1} Hx_i \text{ est un sous-groupe de } G \text{ et } o(x_i^{-1} Hx_i) = o(H);$$

$$\gamma) |Hx_i K| = \frac{o(H) o(K)}{o(x_i^{-1} Hx_i \cap K)} \quad (\text{voir l'exercice 3}).$$

En déduire la relation :

$$o(G) = o(H) o(K) \sum_{i=1}^r d_i^{-1}$$

où, pour tout i ($1 \leq i \leq r$), $d_i = o(x_i^{-1} Hx_i \cap K)$.

d) D'après les résultats précédents, *a priori*, dans un groupe G , deux classes doubles distinctes modulo H et K ne sont pas, en général, équipotentes; montrer que la décomposition du groupe symétrique S_3 en classes doubles modulo $H = \langle \tau_1 \rangle$ et $K = \langle \tau_2 \rangle$ confirme cette remarque et permet aussi de vérifier que $H \neq K$ implique, en général, dans un groupe non abélien, $\mathcal{R}_{H,K} \neq \mathcal{R}_{K,H}$ (τ_1, τ_2 : voir notations (1.15)).

- 6) Soit \mathbf{R} considéré comme espace affine euclidien de dimension 1, muni de la distance habituelle d telle que $d(x, y) = |x - y|$.

A tout $a \in \mathbf{R}$ on associe la translation :

$$\tau_a : \mathbf{R} \rightarrow \mathbf{R} \quad \text{telle que } \tau_a(x) = x + a$$

$$\text{et } \sigma_a : \mathbf{R} \rightarrow \mathbf{R} \quad \text{telle que } \sigma_a(x) = a - x.$$

a) Vérifier que, quels que soient a, b dans \mathbf{R} , $\sigma_a^2 = \text{id}_{\mathbf{R}}$ et $\sigma_b \circ \tau_a = \tau_{-a} \circ \sigma_b$.

b) Montrer que sur la droite réelle, σ_a est une symétrie par rapport à un point.

c) Démontrer que toute isométrie de \mathbf{R} est soit une translation, soit une symétrie par rapport à un point; en déduire que l'ensemble $\mathcal{I}(1)$ des isométries de \mathbf{R} est un sous-groupe non abélien du groupe symétrique $S_{\mathbf{R}}$.

d) $T = \{\tau_a; a \in \mathbf{R}\}$ étant un sous-groupe abélien de $S_{\mathbf{R}}$ (exercice 13, chap. I^{er}) montrer que $[\mathcal{I}(1) : T] = 2$.

- 7) Soit $\mathcal{I}(2)$ le groupe des isométries du plan affine euclidien P ; les notations étant celles de l'exercice 26, chap. I^{er}, on pose

$$\mathcal{D}(2) = \mathcal{E}(P) \cup \left(\bigcup_{O \in P} \mathcal{R}(P, O) \right).$$

En utilisant les résultats de l'exercice 26, chap. I^{er}, démontrer que $\mathcal{D}(2)$ est l'ensemble des isométries pouvant s'écrire comme produit d'un nombre pair de symétries (du type s_A); en déduire que $\mathcal{D}(2)$ est un sous-groupe de $\mathcal{I}(2)$ tel que $[\mathcal{I}(2) : \mathcal{D}(2)] = 2$.

$\mathcal{D}(2)$ est appelé : *groupe des déplacements de P* .

- 8) Soient a et b deux entiers *non nuls, distincts* et *fixés* dans \mathbb{Z} .
On considère le groupe (additif) $\mathbb{Z} \times \mathbb{Z}$ et l'application

$$\varphi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

$$(x, y) \mapsto ax + by.$$

a) Montrer que φ est un morphisme de groupes.

Déterminer $\text{Ker } \varphi$ et $\text{Im } \varphi$ (d étant pgcd de a et b , $\text{Im } \varphi$ pourra être exprimé à l'aide de d).

b) Soit n un entier *non nul, fixé* dans \mathbb{N} .

On considère dans \mathbb{Z} la loi de composition interne notée $*$ et définie par :

$$x * y = ax + by, \quad \text{quels que soient } x \text{ et } y \text{ dans } \mathbb{Z}.$$

Démontrer que la loi $*$ induit dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ une loi de composition quotient que l'on notera $\bar{*}$.

c) Démontrer que, dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$, la loi $\bar{*}$ est :

- associative si et seulement si n divise $a(a-1)$ et $b(b-1)$;
- commutative si et seulement si n divise $(a-b)$.

d) Prouver que $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \bar{*} \right)$ est un groupe si et seulement si n divise $(a-1)$ et $(b-1)$; dans ce cas, le groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \bar{*} \right)$ est-il abélien?

- 9) G étant un groupe, soient $K \leq G$ et $g \in G$. On pose $K' = gKg^{-1}$; démontrer l'égalité $[G : K] = [G : K']$.

$$\left[\text{On pourra considérer la correspondance } \left(\frac{G}{K} \right)_a \rightarrow \left(\frac{G}{K'} \right)_a \right]$$

$$Kx \mapsto K'gx.$$

10) Soient G un groupe et H un sous-groupe d'indice fini dans G .

Pour tout $g \in G$, HgH sera appelée : *classe double de G modulo H* (voir l'exercice 5, ci-dessus).

a) Montrer que le nombre des classes doubles de G modulo H est fini.

b) Etant donné $g \in G$, vérifier que l'on peut écrire :

$$HgH = \bigcup_{1 \leq i \leq p} Hgx_i, \quad \text{où } p = [H : H \cap g^{-1}Hg],$$

$x_i \in H$ pour tout i ($1 \leq i \leq p$) et $Hgx_i \cap Hgx_j = \emptyset$, si $i \neq j$.

En utilisant l'exercice 9 ci-dessus, prouver que l'on a

$$HgH = \bigcup_{1 \leq j \leq p} y_j gH,$$

où $y_j \in H$ pour tout j ($1 \leq j \leq p$) et $y_i gH \cap y_j gH = \emptyset$, si $i \neq j$.

On pose $z_i = y_i g x_i$, vérifier que

$$HgH = \bigcup_{1 \leq i \leq p} H z_i = \bigcup_{1 \leq i \leq p} z_i H.$$

c) En conclusion de ce qui précède, prouver que, si $[G : H] = r$, il existe dans G des éléments a_1, a_2, \dots, a_r formant une famille de représentants, à la fois, de l'ensemble des classes à droite et de l'ensemble des classes à gauche modulo H .

CHAPITRE III

Groupes monogènes. Groupes symétriques S_n Groupes diédraux

Les familles de groupes que nous étudions dans ce chapitre représentent des types fondamentaux de structures de groupes, qui servent souvent de références dans la description d'autres groupes, éventuellement plus complexes. Par exemple, nous verrons, au chapitre VIII, que tout groupe abélien de type fini est isomorphe à un produit direct de groupes monogènes.

1 — Groupes monogènes

A / Caractérisation des groupes monogènes

La notion de groupe monogène a été définie au chapitre I^{er} (définition (1.40) 2^o). Si G est un groupe monogène engendré par l'élément x , on dit que x est un *générateur* de G et si le groupe est multiplicatif, on écrit :

$$G = \langle x \rangle = \{x^k; k \in \mathbf{Z}\} \quad (\text{formule (19), chap. I}^{\text{er}}).$$

Nous savons (exemples (1.42)) qu'il existe des groupes monogènes infinis, tels que \mathbf{Z} et des groupes monogènes finis, c'est-à-dire cycliques (définition (1.43)).

PROPOSITION (3.1). *Toute image homomorphe d'un groupe monogène est monogène.*

Preuve : Soit un groupe monogène $G = \langle x \rangle$ et soit G' un groupe image homomorphe de G (définition (1.60)); f étant un épimorphisme de G sur G' ,

$$G = \{x^k; k \in \mathbf{Z}\} \Rightarrow \text{Im } f = G' = \{(f(x))^k; k \in \mathbf{Z}\},$$

donc G' est monogène engendré par $f(x)$.

COROLLAIRE (3.2). *Quel que soit $n > 0$ dans \mathbf{N} , le groupe $\frac{\mathbf{Z}}{n\mathbf{Z}}$ est cyclique.*

En effet $(\mathbf{Z}, +)$ est monogène engendré par 1 (exemple (1.42) 1°); d'autre part (remarque (2.11) 2°) la surjection canonique $\pi : (\mathbf{Z}, +) \rightarrow \left(\frac{\mathbf{Z}}{n\mathbf{Z}}, +\right)$ est un épimorphisme de groupes, donc $\frac{\mathbf{Z}}{n\mathbf{Z}}$ est monogène, engendré par $\pi(1) = \bar{1}$, et comme $\frac{\mathbf{Z}}{n\mathbf{Z}}$ est fini d'ordre n , $\frac{\mathbf{Z}}{n\mathbf{Z}}$ est cyclique.

Le théorème suivant fournit alors une caractérisation des groupes monogènes.

THÉORÈME (3.3). *Si G est un groupe monogène, alors G vérifie l'une des conditions suivantes :*

- 1) $G \simeq \mathbf{Z}$; dans ce cas G est monogène infini; ou
- 2) il existe $n > 0$ dans \mathbf{N} tel que $G \simeq \frac{\mathbf{Z}}{n\mathbf{Z}}$, alors G est cyclique d'ordre n .

Preuve : Soit un groupe monogène : $G = \langle x \rangle = \{x^k; k \in \mathbf{Z}\}$

Considérons l'application $\psi : \mathbf{Z} \rightarrow G$.

$$k \mapsto x^k$$

La définition de ψ implique sa surjectivité.

D'autre part, $\psi(k+l) = x^{k+l} = x^k x^l$, donc ψ est un épimorphisme de groupes. Deux cas sont alors à envisager :

1^{er} cas : ψ est injectif; par suite, ψ est un isomorphisme de groupes, d'où $G \simeq \mathbf{Z}$; G est donc monogène infini.

2^e cas : ψ est non injectif; $\text{Ker } \psi$ est alors un sous-groupe non nul de \mathbf{Z} , donc il existe un unique $n > 0$ dans \mathbf{N} tel que $\text{Ker } \psi = n\mathbf{Z}$.

D'après le 1^{er} théorème d'isomorphisme (théorème (2.12)), on a

$$\text{Im } \psi \simeq \frac{G}{\text{Ker } \psi},$$

donc $G \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$; G est cyclique d'ordre n .

COROLLAIRE (3.4).

Deux groupes monogènes infinis sont isomorphes.

Deux groupes cycliques de même ordre n sont isomorphes.

On peut dire aussi « qu'à un isomorphisme près » les seuls groupes monogènes sont les groupes quotients de \mathbb{Z} (\mathbb{Z} étant identifié à $\frac{\mathbb{Z}}{(0)}$).

Remarques (3.5) :

1° Dans le cas où G est cyclique d'ordre n , l'isomorphisme de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ induit par l'épimorphisme ψ du théorème (3.3) est

$$\bar{\psi} : \frac{\mathbb{Z}}{n\mathbb{Z}} \rightarrow G \quad (\text{voir la démonstration du théorème (2.12)}).$$

$$\bar{k} \mapsto x^k$$

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

implique :

$$G = \{e, x, \dots, x^{n-1}\} \quad (1)$$

Pour k quelconque dans \mathbb{Z} , il existe q et r entiers tels que $k = nq + r$, avec $0 \leq r \leq n-1$, d'où

$$x^k = (x^n)^q x^r = x^r, \quad \text{car } x^n = e.$$

D'autre part, pour tout $k \in \mathbb{Z}$, x^{n-k} est l'inverse de x^k dans G , puisque $x^{n-k} x^k = e$; de plus $1 \leq k \leq n-1$ implique $1 \leq n-k \leq n-1$.

En notation additive, un groupe $G = \langle x \rangle$ cyclique d'ordre n s'écrit :

$$G = \{0, x, 2x, \dots, (n-1)x\} \quad (1')$$

2° G étant un groupe quelconque, d'après le théorème (3.3), pour un élément $x \in G$, on a :

$$x \text{ d'ordre infini dans } G \Leftrightarrow \langle x \rangle \simeq \mathbf{Z};$$

$$x \text{ d'ordre fini } m \text{ dans } G \Leftrightarrow \langle x \rangle \simeq \frac{\mathbf{Z}}{m\mathbf{Z}}.$$

ψ étant l'épimorphisme $\mathbf{Z} \rightarrow \langle x \rangle$ tel que $\psi(k) = x^k$, on sait (théorème (3.3)) que :

$$\langle x \rangle \simeq \mathbf{Z} \Leftrightarrow \psi \text{ injectif}$$

$$\left(\exists m \in \mathbf{N}^* \text{ et } \langle x \rangle \simeq \frac{\mathbf{Z}}{m\mathbf{Z}} \right) \Leftrightarrow \psi \text{ non injectif.}$$

On en déduit que :

$$x \text{ d'ordre infini dans } G \Leftrightarrow \forall (k, l) \ (k \neq l \text{ dans } \mathbf{Z} \Rightarrow x^k \neq x^l)$$

$$x \text{ d'ordre fini dans } G \Leftrightarrow \exists (k, l) \ (k \neq l \text{ dans } \mathbf{Z} \text{ et } x^k = x^l)$$

$$x \text{ d'ordre fini dans } G \Leftrightarrow \exists r \in \mathbf{Z}^*, \ x^r = e.$$

PROPOSITION (3.6). Si $G = \langle x \rangle$ est un groupe cyclique d'ordre n , dont l'élément neutre est e , alors :

$$(k \in \mathbf{Z} \text{ et } x^k = e) \Leftrightarrow k \in n\mathbf{Z}$$

et n est le plus petit entier strictement positif tel que $x^n = e$.

de Preuve : Si $G = \langle x \rangle$ est cyclique d'ordre n , $n\mathbf{Z}$ est le noyau l'épimorphisme $\psi: \mathbf{Z} \rightarrow G$ tel que $\psi(k) = x^k$; par suite

$$(k \in \mathbf{Z} \text{ et } x^k = e) \Leftrightarrow k \in n\mathbf{Z}.$$

n est donc, dans \mathbf{N}^* , le plus petit entier tel que $x^n = e$.

COROLLAIRE (3.7). Soit G un groupe fini d'ordre n .

Soit $x \in G$ tel que $o(x) = m$, alors :

- 1) $(h \in \mathbb{Z} \text{ et } x^h = e) \Leftrightarrow h \in m\mathbb{Z}$;
- 2) m est dans \mathbb{N}^* , le plus petit entier tel que $x^m = e$;
- 3) $x^n = e$.

1) et 2) se déduisent de la remarque (3.5), 2° et de la proposition (3.6). D'autre part, d'après le théorème de Lagrange, m divise n , c'est-à-dire que $n \in m\mathbb{Z}$, donc $x^n = e$.

Exemple (3.8) : Pour tout entier $n > 0$, le groupe multiplicatif U_n des racines n -ième de l'unité dans \mathbb{C} , est cyclique d'ordre n .

On sait déjà (exemple (1.30)) que U_n est un groupe fini d'ordre n ; il suffit de montrer que U_n contient un élément d'ordre n .

Or, $U_n = \{z_k\}_{0 \leq k \leq n-1}$, où $z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$.

Pour tout k ($0 \leq k \leq n-1$), on a donc $z_k = z_1^k$ et n est le plus petit entier strictement positif tel que $z_1^n = e$. On en déduit que $U_n = \langle z_1 \rangle$.

PROPOSITION (3.9). Tout groupe fini d'ordre premier p est cyclique.

Preuve : Soit G un groupe fini d'ordre premier p ; p étant plus grand que 1, il existe $x \in G$ tel que $x \neq e$. Si $m = o(x)$, on a $m \neq 1$ et m divise p (théorème de Lagrange); par suite $m = p$, donc $G = \langle x \rangle$.

B / Sous-groupe d'un groupe monogène

a) *Propriété générale :*

THÉORÈME (3.10) :

1° Tout sous-groupe, non réduit à l'élément neutre, d'un groupe monogène infini est monogène infini.

2° Tout sous-groupe d'un groupe cyclique est cyclique.

Preuve : Compte tenu du théorème (3.3), il suffit de montrer que tout sous-groupe non nul de \mathbf{Z} est monogène infini et que, pour $n \neq 0$ dans \mathbf{N} , tout sous-groupe de $\frac{\mathbf{Z}}{n\mathbf{Z}}$ est cyclique.

1° On sait (exemple (1.28)) que tout sous-groupe non nul de \mathbf{Z} est de la forme $n\mathbf{Z}$, $n \neq 0$ dans \mathbf{N} .

$$n\mathbf{Z} = \{nk = kn; k \in \mathbf{Z}\}$$

et $k \neq l$ dans \mathbf{Z} implique $kn \neq ln$, donc $n\mathbf{Z}$ est un groupe (additif) monogène infini engendré par n .

2° Soit $n \neq 0$ dans \mathbf{N} et π l'épimorphisme canonique $\mathbf{Z} \rightarrow \frac{\mathbf{Z}}{n\mathbf{Z}}$. Soit K un sous-groupe de $\frac{\mathbf{Z}}{n\mathbf{Z}}$; π étant surjectif, on a $K = \pi(\pi^{-1}(K))$; or $\pi^{-1}(K)$ est un sous-groupe de \mathbf{Z} (proposition (1.55)), donc il existe un unique $k \in \mathbf{N}$ tel que $\pi^{-1}(K) = k\mathbf{Z}$.

K est alors l'image homomorphe par π du groupe monogène $k\mathbf{Z}$, par suite K est monogène, engendré par $\pi(k)$ (proposition (3.1)) et K est cyclique, puisque K est fini.

b) Sous-groupes d'un groupe cyclique. Etudions, tout d'abord, les sous-groupes de $\frac{\mathbf{Z}}{n\mathbf{Z}}$, pour $n \neq 0$ dans \mathbf{N} .

En reprenant les notations de la démonstration du théorème (3.10), on remarque que, K étant un sous-groupe de $\frac{\mathbf{Z}}{n\mathbf{Z}}$, $\pi(0) = \bar{0}$ appartient à K ; par suite, on a :

$$\pi^{-1}(\bar{0}) \subseteq \pi^{-1}(K),$$

c'est-à-dire $n\mathbf{Z} \subseteq k\mathbf{Z}$; autrement dit, k divise n dans \mathbf{N}^* .

Déterminons l'ordre du sous-groupe K .

Posons $\pi(k) = \bar{k}$; on a $K = \langle \bar{k} \rangle$ dans $\frac{\mathbf{Z}}{n\mathbf{Z}}$, d'où

$$o(K) = o(\bar{k}) \text{ dans } \frac{\mathbf{Z}}{n\mathbf{Z}}$$

$o(\bar{k})$ est le plus petit entier $d > 0$, tel que $d\bar{k} = \bar{0}$.

$$\text{Or, } d\bar{k} = d\pi(k) = \pi(dk),$$

puisque π est un morphisme de groupes additifs.

k divisant n dans \mathbf{N}^* , $o(\bar{k})$ est nécessairement l'entier $d = \frac{n}{k}$.
On a ainsi prouvé la propriété suivante :

PROPOSITION (3.11). Soient $n \in \mathbf{N}^*$ et π l'épimorphisme canonique $\mathbf{Z} \rightarrow \frac{\mathbf{Z}}{n\mathbf{Z}}$. Pour tout sous-groupe K de $\frac{\mathbf{Z}}{n\mathbf{Z}}$, il existe un unique diviseur k de n , dans \mathbf{N}^* , tel que $\pi(k)$ engendre K et $o(K) = \frac{n}{k}$.

COROLLAIRE (3.12). Le nombre des sous-groupes de $\frac{\mathbf{Z}}{n\mathbf{Z}}$ ($n \neq 0$ dans \mathbf{N}) est égal au nombre des diviseurs de n dans \mathbf{N}^* .

En effet, d'après la proposition (3.11), $\frac{\mathbf{Z}}{n\mathbf{Z}}$ n'a pas d'autres sous-groupes que les $\langle \pi(k) \rangle$ où k divise n , dans \mathbf{N}^* . De plus, si k et k' sont deux diviseurs de n , tels que $k \neq k'$ dans \mathbf{N}^* , les ordres des sous-groupes $\langle \pi(k) \rangle$ et $\langle \pi(k') \rangle$ sont respectivement $\frac{n}{k}$ et $\frac{n}{k'}$, donc ces sous-groupes sont distincts.

Si $n > 1$, on remarque que n a au moins deux diviseurs distincts dans \mathbf{N}^* , 1 et n , qui correspondent, respectivement, au sous-groupe plein $\frac{\mathbf{Z}}{n\mathbf{Z}}$ et au sous-groupe réduit à l'élément neutre $(\bar{0})$.

Exemple (3.13) : Les diviseurs de 6, dans \mathbf{N} , étant 1, 2, 3 et 6, on peut affirmer que $\frac{\mathbf{Z}}{6\mathbf{Z}}$ a quatre sous-groupes distincts :

$$\begin{aligned}\langle \bar{1} \rangle &= \frac{\mathbf{Z}}{6\mathbf{Z}}, & \langle \bar{2} \rangle &= \{ \bar{2}, \bar{4}, \bar{0} \}, \\ & & \langle \bar{3} \rangle &= \{ \bar{3}, \bar{0} \} \quad \text{et} \quad \langle \bar{6} \rangle = (\bar{0}).\end{aligned}$$

Les sous-groupes $\langle \bar{4} \rangle$ et $\langle \bar{5} \rangle$ coïncident donc nécessairement avec l'un des quatre sous-groupes précédents.

On peut vérifier que $\langle \bar{4} \rangle = \langle \bar{2} \rangle$ et $\langle \bar{5} \rangle = \frac{\mathbf{Z}}{6\mathbf{Z}}$; ces résultats seront justifiés par les propriétés des générateurs d'un groupe cyclique (paragraphe C /, ci-dessous).

De l'étude des sous-groupes de $\frac{\mathbf{Z}}{n\mathbf{Z}}$, pour $n \neq 0$, on déduit le

théorème suivant, relatif aux sous-groupes d'un groupe cyclique quelconque (que l'on notera multiplicativement) :

THÉORÈME (3.14). $G = \langle x \rangle$ étant un groupe cyclique d'ordre n , alors, pour tout diviseur d de n , il existe un et un seul sous-groupe d'ordre d de G et ce sous-groupe est engendré par x^k où $k = \frac{n}{d}$.

Preuve : π désigne toujours l'épimorphisme canonique $\mathbf{Z} \rightarrow \frac{\mathbf{Z}}{n\mathbf{Z}}$. D'après la remarque (3.4) : $\bar{\psi} : \frac{\mathbf{Z}}{n\mathbf{Z}} \rightarrow G$ est un isomorphisme de groupes.

$$\pi(k) \mapsto x^k$$

Tout sous-groupe de G est donc l'image par $\bar{\psi}$ d'un sous-groupe de $\frac{\mathbf{Z}}{n\mathbf{Z}}$.

Soit d un diviseur de n , dans \mathbf{N}^* ; posons $k = \frac{n}{d}$.

D'après la proposition (3.11) et le corollaire (3.12), $\langle \pi(k) \rangle$ est l'unique sous-groupe de $\frac{\mathbf{Z}}{n\mathbf{Z}}$ d'ordre $d = \frac{n}{k}$.

On en déduit que G a un et un seul sous-groupe d'ordre d , engendré par $\bar{\psi}(\pi(k)) = x^k$.

Remarques (3.15) :

1° Si le groupe $G = \langle x \rangle$ est noté additivement, dans l'énoncé du théorème (3.14), x^k doit être remplacé par kx .

2° L'étude ci-dessus montre que, lorsqu'un groupe G est cyclique d'ordre n , il existe une bijection entre l'ensemble des diviseurs de n dans \mathbf{N}^* et l'ensemble des sous-groupes de G .

Nous verrons plus loin (chap. VI) que cette propriété n'est pas vérifiée, en général, par un groupe fini quelconque; plus précisément, si G est un groupe fini d'ordre n et si d divise n dans \mathbf{N}^* , alors :

- il n'existe pas nécessairement un sous-groupe de G , d'ordre d (exercice 10, chap. IV);
- s'il existe un sous-groupe de G , d'ordre d , il n'est pas nécessairement unique.

PROPOSITION (3.16). *Soit G un groupe non réduit à l'élément neutre e ; alors G n'a pas d'autre sous-groupe que G et (e) , si et seulement si G est cyclique d'ordre premier.*

Preuve :

— Soit G un groupe cyclique d'ordre premier p ; $p > 1$ implique $G \neq (e)$; d'après le théorème de Lagrange, l'ordre d'un sous-groupe de G ne peut être que 1 ou p , donc G n'a pas d'autre sous-groupe que (e) et G .

Réciproquement, considérons un groupe $G \neq (e)$ dont les seuls sous-groupes sont G et (e) .

Soit $x \neq e$, dans G ; le sous-groupe $\langle x \rangle$ de G est nécessairement différent de (e) , donc $\langle x \rangle = G$, c'est-à-dire que G est monogène.

Si G était infini, G serait isomorphe à \mathbf{Z} , donc aurait d'autres sous-groupes que G et (e) ; par suite, G est cyclique.

G n'ayant pas d'autre sous-groupe que G et (e) , l'ordre de G n'a pas, dans \mathbf{N}^* , d'autre diviseur que lui-même et 1, c'est donc un nombre premier.

C / Générateurs d'un groupe monogène

a) Préliminaires. Rappelons que dans \mathbf{Z} deux éléments non nuls a et b sont dits *premiers entre eux*, si leurs seuls diviseurs communs sont 1 et -1 ; autrement dit, si 1 est PGCD de a et b (PGCD = plus grand commun diviseur).

— On suppose alors connu le résultat suivant [49] :

THÉORÈME DE BEZOUT ⁽¹⁾. *Deux entiers non nuls a et b sont premiers entre eux dans \mathbf{Z} , si et seulement s'il existe u et v dans \mathbf{Z} , tels que :*

$$au + bv = 1 \quad (2)$$

Notation : Pour a et b non nuls dans \mathbf{Z} , on écrira

$$(a, b) = 1 \quad (3)$$

pour exprimer que a et b sont premiers entre eux.

⁽¹⁾ Etienne Bezout, mathématicien français (1730-1783).

En effet, dans \mathbf{Z} , un PGCD de a et b est souvent noté (a, b) et (3) exprime que 1 est PGCD de a et b .

b) Générateurs d'un groupe monogène. Un groupe monogène quelconque sera noté multiplicativement.

Remarque (3.17) : Soit $G = \langle x \rangle = \{x^k; k \in \mathbf{Z}\}$; alors, pour que x^k soit un générateur de G , il faut et il suffit que $x \in \langle x^k \rangle$, sous-groupe de G engendré par x^k ; d'où

$$x^k \text{ générateur de } G \Leftrightarrow \exists m \in \mathbf{Z}, \quad x^{km} = x \quad (4)$$

THÉORÈME (3.18). *Soit un groupe monogène $G = \langle x \rangle$.*

1° Si G est infini, alors les seuls générateurs de G sont x et x^{-1} .

2° Si G est cyclique d'ordre $n > 1$, alors l'ensemble des générateurs de G est formé par les x^k , tels que k et n sont premiers entre eux dans \mathbf{Z} .

Preuve :

1° Si G est monogène infini, alors $\psi: \mathbf{Z} \rightarrow G$ est un isomorphisme de groupe (théorème (3.3)).

$$k \mapsto x^k$$

Tout générateur de G est donc l'image par ψ d'un générateur de $(\mathbf{Z}, +)$.

Or les seuls générateurs de $(\mathbf{Z}, +)$ sont 1 et -1 (exemple (1.42)), d'où le résultat énoncé.

2° On suppose $G = \langle x \rangle$, cyclique d'ordre $n > 1$.

Cherchons s'il existe un entier $k \neq 1$ tel que x^k engendre G . D'après la remarque (3.17), on a

$$G = \langle x^k \rangle \Leftrightarrow \exists m \in \mathbf{Z}, \quad x^{km} = x$$

$$G = \langle x^k \rangle \Leftrightarrow \exists m \in \mathbf{Z}, \quad x^{km-1} = e$$

$$G = \langle x^k \rangle \Leftrightarrow \exists m \in \mathbf{Z}, \quad (km - 1) \in n\mathbf{Z}$$

$$G = \langle x^k \rangle \Leftrightarrow \exists (m, q) \in \mathbf{Z} \times \mathbf{Z}, \quad km - nq = 1.$$

D'après le théorème de Bezout, la dernière condition écrite exprime que k et n sont premiers entre eux dans \mathbf{Z} .

Remarque (3.19) : Soit $G = \langle x \rangle$ cyclique d'ordre n , donc $G = \{e, x, \dots, x^{n-1}\}$. Quel que soit $k \in \mathbf{Z}$ tel que $(k, n) = 1$ (notation définie plus haut par (3)), il existe s et k' dans \mathbf{Z} tels que

$$k = ns + k' \quad \text{et} \quad 1 \leq k' \leq n - 1.$$

On a alors

$$x^k = x^{k'}, \quad \text{car } x^{ns} = (x^n)^s = e$$

et $(k', n) = 1$, car tout diviseur commun à k' et n divise aussi k .

On en conclut que, si $G = \langle x \rangle$ est cyclique d'ordre n , alors les générateurs de G sont les x^k tels que k est premier avec n et $1 \leq k \leq n - 1$.

Pour n donné dans N^* , posons

$$E(n) = \{k \in N; 1 \leq k \leq n - 1 \text{ et } (k, n) = 1\}.$$

Définition (3.20) : On appelle *fonction d'Euler* ⁽²⁾ l'application $\varphi : N^* \rightarrow N^*$ telle que

$$\varphi(1) = 1$$

et quel que soit $n > 1$, $\varphi(n) = \text{card}(E(n))$.

La conclusion de la remarque (3.19) implique la propriété suivante :

PROPOSITION (3.21). *Le nombre des générateurs d'un groupe cyclique d'ordre n est égal à $\varphi(n)$, φ étant la fonction d'Euler.*

Remarque (3.22) :

1° La fonction d'Euler est appelée dans certains ouvrages « Indicateur » ou « Indicatrice » d'Euler.

2° La proposition (3.21) n'a d'intérêt que si l'on sait calculer $\varphi(n)$; c'est ce que nous ferons dans le paragraphe D / suivant. On peut déjà remarquer que si p est un nombre premier, alors :

$$\varphi(p) = p - 1.$$

c) *Caractérisation des générateurs du groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$ pour $n > 1$.*

Remarque (3.23) : Si, pour $n > 1$, on considère $\frac{\mathbb{Z}}{n\mathbb{Z}} = \overline{(n)}$ comme anneau commutatif et unitaire (exercice 21, chap. I^{er}), alors un élément $\bar{k} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ est dit *inversible*, s'il existe $\bar{k}' \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ tel que $\bar{k}\bar{k}' = \bar{1}$.

⁽²⁾ Leonhard Euler, mathématicien et astronome suisse (1707-1783).

PROPOSITION (3.24). Pour $n > 1$ dans \mathbf{N} , les générateurs du groupe cyclique $\left(\frac{\mathbf{Z}}{n\mathbf{Z}}, +\right)$ sont les éléments inversibles de l'anneau $\frac{\mathbf{Z}}{n\mathbf{Z}}$ et leur ensemble forme un groupe multiplicatif, abélien, d'ordre $\varphi(n)$.

Preuve : D'après le théorème (3.18) et la remarque (3.19), un élément \bar{k} de $\frac{\mathbf{Z}}{n\mathbf{Z}}$ est générateur du groupe $\left(\frac{\mathbf{Z}}{n\mathbf{Z}}, +\right)$ si et seulement si k est premier avec n . Appliquons le théorème de Bezout :

$$\begin{aligned}(k, n) = 1 &\Leftrightarrow \exists (k', q) \in \mathbf{Z} \times \mathbf{Z}, \quad kk' + nq = 1 \\ &\Leftrightarrow \exists \bar{k}' \in \frac{\mathbf{Z}}{n\mathbf{Z}}, \quad \bar{k}\bar{k}' = \bar{1}.\end{aligned}$$

Les générateurs du groupe $\left(\frac{\mathbf{Z}}{n\mathbf{Z}}, +\right)$ sont donc les éléments inversibles de l'anneau $\frac{\mathbf{Z}}{n\mathbf{Z}}$; notons G_n leur ensemble et vérifions que la multiplication de l'anneau $\frac{\mathbf{Z}}{n\mathbf{Z}}$ induit une loi de composition interne dans G_n .

Soient \bar{k}_1, \bar{k}_2 dans G_n et \bar{k}'_1, \bar{k}'_2 leurs inverses dans $\frac{\mathbf{Z}}{n\mathbf{Z}}$; alors $(\bar{k}_1 \bar{k}_2)(\bar{k}'_2 \bar{k}'_1) = \bar{1}$, car la multiplication de l'anneau est *associative*, on en déduit que $\bar{k}_1 \bar{k}_2 \in G_n$.

D'autre part, $\bar{1} \in G_n$ et de plus, si \bar{k} est dans G_n , alors son inverse \bar{k}' est nécessairement dans G_n .

Ainsi G_n est un groupe par rapport à la multiplication de l'anneau $\frac{\mathbf{Z}}{n\mathbf{Z}}$; ce groupe est abélien, car l'anneau $\frac{\mathbf{Z}}{n\mathbf{Z}}$ est commutatif (exercice 21, chap. I) et il est d'ordre $\varphi(n)$, d'après la proposition (3.21).

Remarque (3.25) :

1° Si p est premier, le groupe G_p est d'ordre $\varphi(p) = p - 1$, donc $G_p = \frac{\mathbf{Z}}{p\mathbf{Z}} - \{\bar{0}\}$, ce qui confirme que $\frac{\mathbf{Z}}{p\mathbf{Z}}$ est un corps (exercice 21, chap. I).

2° On peut vérifier que dans tout anneau unitaire l'ensemble des éléments inversibles forme un groupe par rapport à la multiplication de l'anneau.

D / Produits directs de groupes cycliques. Calcul de $\varphi(n)$

Remarque (3.26).

Le calcul de $\varphi(n)$ s'appuyant sur le résultat de la proposition (3.24), il est commode, dans ce paragraphe, d'utiliser quelques propriétés liées à la structure d'anneau commutatif unitaire de $\frac{\mathbb{Z}}{n\mathbb{Z}}$, pour $n > 1$ dans \mathbb{N} .

Pour cette raison, nous supposerons connues [49] les notions de *morphisme* et de *produit direct* d'anneaux unitaires et nous admettrons, pour les anneaux unitaires, le *1^{er} théorème d'isomorphisme* analogue à celui vu pour les groupes (théorème (2.27)).

a) *Produits directs de groupes cycliques.* Le groupe produit direct de deux groupes cycliques n'est pas nécessairement cyclique, puisque nous savons (exemple (1.86)) que le groupe de Klein, $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$, n'est pas cyclique.

Dans ce paragraphe, nous allons déterminer dans quel cas le groupe produit direct de deux et, plus généralement, de n groupes cycliques est cyclique ($n \geq 2$ dans \mathbb{N}).

Rappelons préalablement quelques propriétés arithmétiques de \mathbb{Z} (voir [49], par exemple) :

Etant donné deux entiers non nuls et positifs m et n , dont $d > 0$ est un PGCD et $l > 0$ est un PPCM (plus petit commun multiple), on a :

$$a) \quad dl = mn;$$

par suite, compte tenu de la notation (3), on obtient :

$$b) \quad (m, n) = 1 \Leftrightarrow mn \text{ est PPCM de } m \text{ et } n;$$

$$c) \quad m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z} \tag{5}$$

On en déduit immédiatement le résultat suivant :

LEMME (3.27). *Si m et n sont deux entiers non nuls et positifs, alors*

$$m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z} \Leftrightarrow (m, n) = 1 \tag{6}$$

Remarque (3.28) : A titre d'exercice, on pourra démontrer le lemme (3.27), sans l'aide des propriétés rappelées plus haut, mais en utilisant le théorème de Gauss [49] :

THÉORÈME DE GAUSS ⁽³⁾. *a, b, c étant trois éléments non nuls de \mathbf{Z} , si a et b sont premiers entre eux et a divise bc , alors a divise c .*

THÉORÈME (3.29). *Si m et n sont deux entiers positifs non nuls, alors les anneaux unitaires (donc en particulier les groupes additifs) $\frac{\mathbf{Z}}{m\mathbf{Z}} \times \frac{\mathbf{Z}}{n\mathbf{Z}}$ et $\frac{\mathbf{Z}}{mn\mathbf{Z}}$ sont isomorphes si et seulement si m et n sont premiers entre eux.*

Preuve : Notons respectivement σ et π les surjections canoniques :

$$\mathbf{Z} \rightarrow \frac{\mathbf{Z}}{m\mathbf{Z}} \quad \text{et} \quad \mathbf{Z} \rightarrow \frac{\mathbf{Z}}{n\mathbf{Z}}.$$

σ et π sont des morphismes de groupes additifs; de plus, la définition de la multiplication dans $\frac{\mathbf{Z}}{m\mathbf{Z}}$ et dans $\frac{\mathbf{Z}}{n\mathbf{Z}}$ (exercice 21, chap. I) implique que σ et π sont des morphismes d'anneaux unitaires.

On en déduit que l'application

$$\begin{aligned} f: \mathbf{Z} &\rightarrow \frac{\mathbf{Z}}{m\mathbf{Z}} \times \frac{\mathbf{Z}}{n\mathbf{Z}} \\ x &\mapsto (\sigma(x), \pi(x)) \end{aligned}$$

est aussi un morphisme d'anneaux unitaires

$$\text{Ker } f = \{x \in \mathbf{Z}; \sigma(x) = \sigma(0) \text{ et } \pi(x) = \pi(0)\}$$

d'où $\text{Ker } f = m\mathbf{Z} \cap n\mathbf{Z}$.

D'après le lemme (3.27), on a (en utilisant la notation (3)) :

$$(m, n) = 1 \quad \Leftrightarrow \quad \text{Ker } f = mn\mathbf{Z} \quad (7)$$

$$\text{donc} \quad (m, n) = 1 \quad \Leftrightarrow \quad \text{Im } f \simeq \frac{\mathbf{Z}}{mn\mathbf{Z}} \quad (8)$$

⁽³⁾ C. F. Gauss, mathématicien, physicien, astronome allemand (1777-1855).

Or, $\text{Im } f$ est un sous-anneau de $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$, qui est fini et de cardinal mn ; on en déduit la relation :

$$(m, n) = 1 \Leftrightarrow f \text{ surjectif} \quad (9)$$

et par suite :

$$(m, n) = 1 \Leftrightarrow \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \frac{\mathbb{Z}}{mn\mathbb{Z}} \quad (10)$$

cet isomorphisme d'anneaux unitaires est, en particulier, un *isomorphisme de groupes additifs*.

En convenant de désigner, d'une façon générale, par C_k un groupe cyclique d'ordre k , on obtient la propriété suivante :

COROLLAIRE (3.30). *Le produit direct de deux groupes cycliques C_m et C_n est un groupe cyclique, si et seulement si m et n sont premiers entre eux.*

En effet, le groupe $C_m \times C_n$ est cyclique, si et seulement s'il est isomorphe à C_{mn} .

Remarques (3.31) :

1° Une démonstration directe du corollaire (3.30) est proposée dans l'exercice 1, chapitre III.

2° On verra dans l'exercice 2, chapitre III, qu'en explicitant la surjectivité de f on peut donner une autre démonstration de la relation (9) ci-dessus.

3° Le théorème (3.29) et par suite le corollaire (3.30) se généralisent pour un nombre fini d'entiers m_1, m_2, \dots, m_k :

COROLLAIRE (3.32). *Soient m_1, m_2, \dots, m_k ($k \geq 2$ dans \mathbb{N}) des entiers positifs non nuls, alors les anneaux unitaires*

$$\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{m_k\mathbb{Z}} \quad \text{et} \quad \frac{\mathbb{Z}}{m_1 m_2 \dots m_k \mathbb{Z}}$$

sont isomorphes si et seulement si les m_i ($1 \leq i \leq k$) sont deux à deux premiers entre eux.

Cette dernière condition est donc nécessaire et suffisante, pour que le groupe produit direct $\prod_{1 \leq i \leq k} C_{m_i}$ soit cyclique, c'est-à-dire isomorphe à $C_{m_1 m_2 \dots m_k}$.

Démonstration laissée au lecteur.

b) Calcul de $\varphi(n)$ pour $n > 1$.

LEMME (3.33). Si m et n sont deux entiers positifs premiers entre eux, alors :

$$\varphi(mn) = \varphi(m) \varphi(n) \quad (11)$$

Preuve : D'après la proposition (3.24), $\varphi(mn)$ est le nombre des éléments inversibles de l'anneau $\frac{\mathbb{Z}}{mn\mathbb{Z}}$.

D'autre part, dans l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$, un élément $(\sigma(x), \pi(y))$ est inversible si et seulement si $\sigma(x)$ et $\pi(y)$ sont respectivement inversibles dans $\frac{\mathbb{Z}}{m\mathbb{Z}}$ et $\frac{\mathbb{Z}}{n\mathbb{Z}}$; on en déduit que le nombre des éléments inversibles dans $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ est $\varphi(m) \varphi(n)$.

Si m et n sont premiers entre eux, le résultat du théorème (3.29) implique alors :

$$\varphi(mn) = \varphi(m) \varphi(n).$$

Remarque (3.34) :

1° Compte tenu du corollaire (3.32), si m_1, m_2, \dots, m_k ($k \geq 2$ dans \mathbb{N}) sont des entiers positifs deux à deux premiers entre eux, alors :

$$\varphi(m_1 m_2 \dots m_k) = \varphi(m_1) \varphi(m_2) \dots \varphi(m_k) \quad (12)$$

2° Tout entier $n > 1$ s'écrivant sous la forme

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

les p_i étant des nombres premiers distincts et les α_i des entiers strictement positifs, la remarque précédente implique :

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k}) \quad (13)$$

On est donc ramené à calculer $\varphi(p^\alpha)$ pour p premier et $\alpha \geq 1$ dans \mathbb{N} .

LEMME (3.35). Si $p \in \mathbf{N}$ est un nombre premier, pour tout $\alpha \geq 1$ dans \mathbf{N} , on a

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1) \quad (14)$$

Preuve : On remarque que $\varphi(p^\alpha)$ est le nombre des entiers k tels que :

$$1 \leq k < p^\alpha \quad \text{et} \quad k \text{ non multiple de } p.$$

Or les entiers m , tels que $1 \leq m \leq p^\alpha$, qui sont multiples de p , sont de la forme :

$$m = pq \quad \text{avec} \quad 1 \leq q \leq p^{\alpha-1};$$

il y en a donc $p^{\alpha-1}$.

On en déduit que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

THÉORÈME (3.36). Soit $n > 1$ dans \mathbf{N} ; si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, avec $k \geq 1$, les p_i étant des nombres premiers distincts et les α_i des entiers strictement positifs, alors :

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \quad (15)$$

La formule (15) est une conséquence directe des relations (13) et (14).

2 — Groupes symétriques S_n

Pour tout entier $n \geq 1$, le groupe symétrique S_n (exemple (1.14)) est le groupe des permutations de l'ensemble $\{1, 2, \dots, n\}$, noté désormais N_n .

Plus généralement, nous avons vu (lemme (1.74)) que S_n pouvait être considéré comme le groupe des permutations de tout ensemble fini de cardinal n .

Rappelons que S_n est un groupe fini d'ordre $n!$, non abélien pour $n > 2$.

A / Notion de σ -orbite (ou orbite suivant σ)

a) *Support d'une permutation :*

Définition (3.37) : Soit $\sigma \in S_n$, le support de σ est l'ensemble :

$$\text{supp}(\sigma) = \{i \in \mathbb{N}_n; \sigma(i) \neq i\}.$$

Remarques (3.38) :

1° Dans S_n , $\sigma = e$ si et seulement si $\text{supp } \sigma = \emptyset$.

2° Quel que soit $\sigma \neq e$ dans S_n , la restriction de σ à $\text{supp}(\sigma)$ est une permutation de l'ensemble $\text{supp}(\sigma)$.

En effet, soit $i \in \text{supp}(\sigma)$; posons $\sigma(i) = j$.

Si j n'appartenait pas à $\text{supp}(\sigma)$, on aurait $\sigma(j) = j$; σ étant injectif, $\sigma(i) = \sigma(j)$ impliquerait $i = j$, ce qui est contraire à l'hypothèse $i \in \text{supp}(\sigma)$.

La restriction σ' de σ à son support est donc une application injective de l'ensemble fini non vide $\text{supp}(\sigma)$ dans lui-même; par suite, σ' est une permutation de l'ensemble $\text{supp}(\sigma)$, en vertu du théorème suivant [57] :

« Si E et F sont deux ensembles finis non vides de même cardinal, alors, pour une application f de E dans F , on a :

$$f \text{ injective} \Leftrightarrow f \text{ surjective};$$

donc, en particulier :

$$f \text{ injective} \Rightarrow f \text{ bijective.} \gg$$

3° D'après la remarque précédente, $\text{supp}(\sigma^{-1}) = \text{supp}(\sigma)$; on en déduit :

$$\text{supp}(\sigma^k) \subseteq \text{supp}(\sigma), \text{ pour tout } k \in \mathbb{Z}.$$

PROPOSITION (3.39). Dans tout groupe S_n , deux permutations dont les supports sont disjoints commutent.

Preuve : La propriété étant immédiate pour $n = 1$, supposons $n > 1$ et considérons $\sigma_1 \neq \sigma_2$ dans S_n tels que

$$\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \emptyset.$$

Si l'une des deux permutations est l'identité, la propriété est vérifiée; supposons les deux supports non vides.

Soit $i \in \text{supp}(\sigma_1)$, alors $i \notin \text{supp}(\sigma_2)$ et $\sigma_1(i) \notin \text{supp}(\sigma_2)$, par suite :

$$\sigma_1 \circ \sigma_2(i) = \sigma_1(i) \quad \text{et} \quad \sigma_2 \circ \sigma_1(i) = \sigma_1(i).$$

De même pour $i \in \text{supp}(\sigma_2)$, on a :

$$\sigma_1 \circ \sigma_2(i) = \sigma_2(i) \quad \text{et} \quad \sigma_2 \circ \sigma_1(i) = \sigma_2(i).$$

D'autre part, s'il existe $i \in N_n$ tel que $i \notin \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2)$, alors $\sigma_1 \circ \sigma_2(i) = i$ et $\sigma_2 \circ \sigma_1(i) = i$.

On en conclut que $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

b) *Notion de σ -orbite* (ou orbite suivant σ). A toute permutation $\sigma \in S_n$, on associe la relation binaire \mathcal{R}_σ définie dans N_n par :

$$i \mathcal{R}_\sigma k \Leftrightarrow \exists r \in \mathbf{Z}, \quad \sigma^r(i) = k.$$

Il est facile de vérifier que \mathcal{R}_σ est une relation d'équivalence dans N_n et que la classe d'équivalence modulo \mathcal{R}_σ d'un élément $i \in N_n$ est :

$$\Omega_\sigma(i) = \{\sigma^r(i); r \in \mathbf{Z}\} \quad (16)$$

Définition (3.40) : Pour tout $\sigma \in S_n$ et tout $i \in N_n$,

$\Omega_\sigma(i)$ s'appelle la σ -orbite de i (ou l'orbite de i suivant σ).

Remarques (3.41) :

1° Supposons $n > 1$ et $\sigma \neq e$ dans S_n tel que $o(\sigma) = p$, on a alors : $\langle \sigma \rangle = \{\sigma^r; r \in \mathbf{Z}\} = \{e, \sigma, \dots, \sigma^{p-1}\}$; par suite, en notant $|\Omega_\sigma(i)|$ le cardinal de la σ -orbite de i , on a, pour tout $i \in N_n$:

$$1 \leq |\Omega_\sigma(i)| \leq p \quad (17)$$

Si $i \notin \text{supp}(\sigma)$, alors $\Omega_\sigma(i) = \{i\}$, donc $|\Omega_\sigma(i)| = 1$.

Une σ -orbite de cardinal 1 sera dite *ponctuelle*.

Si $i \in \text{supp}(\sigma)$, on a nécessairement $2 \leq |\Omega_\sigma(i)| \leq p$.

2° Si $\{i_1, i_2, \dots, i_t\}$ est une famille de représentants des σ -orbites distinctes de N_n , les $\{\Omega_\sigma(i_q)\}_{1 \leq q \leq t}$ forment une partition de N_n , d'où

$$n = \sum_{1 \leq q \leq t} |\Omega_\sigma(i_q)| \quad (18)$$

Exemple (3.42) : Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$

$$\Omega_\sigma(1) = \{1, 5, 3\}, \quad \Omega_\sigma(2) = \{2\}, \quad \Omega_\sigma(4) = \{4, 6\}.$$

B / Cycles dans S_n . Transpositions

A titre d'exemple, considérons la permutation :

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix}.$$

Le support de γ est $\{2, 4, 5, 6\}$ et on remarque que :

$$\gamma(2) = 4, \quad \gamma(4) = 6, \quad \gamma(6) = 5 \quad \text{et} \quad \gamma(5) = 2.$$

On dit que, dans le groupe S_6 , γ est un cycle de longueur 4 et γ est noté $(2, 4, 6, 5)$. La notion générale de cycle dans S_n est la suivante :

Définition (3.43) : Une permutation $\gamma \in S_n$ est un cycle de longueur r ($1 \leq r \leq n$ dans \mathbb{N}) s'il existe un ensemble ordonné de r entiers distincts dans $N_n : j_1, j_2, \dots, j_r$, tels que :

$$\gamma(j_1) = j_2, \quad \gamma(j_2) = j_3, \dots, \gamma(j_{r-1}) = j_r, \quad \gamma(j_r) = j_1$$

et pour tout $k \in N_n \setminus \{j_1, j_2, \dots, j_r\}$, $\gamma(k) = k$.

Un tel cycle sera noté $\gamma = (j_1, j_2, \dots, j_r)$.

L'ensemble $\{j_1, j_2, \dots, j_r\}$ est le support de γ .

Remarque (3.44) :

1° Un cycle (j_1, j_2, \dots, j_r) peut aussi être noté $(j_k, j_{k+1}, \dots, j_r, j_1, j_2, \dots, j_{k-1})$, quel que soit k ($1 < k \leq n$).

2° Tout cycle de longueur 1 est l'identité e : en effet, si $\gamma = (j)$, on a $\gamma(j) = j$ et pour tout $k \neq j$ dans N_n , $\gamma(k) = k$, donc $\gamma = e$.

Définition (3.45) : Un cycle de longueur 2 dans S_n ($n \geq 2$) est appelé *transposition*. Si $\tau = (j_1, j_2)$, on a $\tau(j_1) = j_2$, $\tau(j_2) = j_1$ et $\tau(k) = k$, pour tout $k \in N_n \setminus \{j_1, j_2\}$.

Une transposition dans S_n est donc une permutation qui, dans N_n , échange deux éléments et laisse invariants tous les autres (lorsque $n \geq 3$).

Exemples (3.46) :

- $S_2 = \{e, \tau\}$ où τ est la transposition qui échange 1 et 2.
- Dans S_3 , les permutations τ_1, τ_2, τ_3 (notations (1.15)) sont des transpositions et σ_1, σ_2 sont des cycles de longueur 3.

Remarque (3.47) : Pour $n \geq 2$ dans N , le nombre des transpositions dans S_n est égal au nombre de couples $(i, j) \in N_n \times N_n$ tels que $i \neq j$; ce nombre est donc $C_n^2 = \frac{n(n-1)}{2}$ ([16], [49]).

Définition (3.48) : Dans S_n ($n \geq 2$), le cycle de longueur n :

$$\gamma_1 = (1, 2, \dots, n) = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 4 & \dots & 1 \end{pmatrix}$$

est appelé *permutation circulaire* des entiers 1, 2, ..., n .

Remarques (3.49) :

1° Dans S_n ($n \geq 3$) un cycle de longueur n n'est pas nécessairement la permutation circulaire.

Par exemple, dans S_4 : $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ est le cycle (1, 3, 4, 2) différent de (1, 2, 3, 4).

2° Dans S_n , un cycle de longueur r ($1 \leq r \leq n$) sera appelé un *r-cycle*.

PROPOSITION (3.50). Dans tout groupe S_n , un *r-cycle* est un élément d'ordre r .

Preuve : Soit $\gamma = (j_1, j_2, \dots, j_r)$ un *r-cycle* dans S_n .

— Si $r = 1$, alors $\gamma = e$, donc $o(\gamma) = 1$.

— Supposons $1 < r \leq n$; pour tout k ($1 \leq k \leq r$), on a :

$$\gamma(j_k) = j_{k+1}, \quad \gamma^2(j_k) = j_{k+2}, \dots, \gamma^{r-k}(j_k) = j_r, \dots, \gamma^r(j_k) = j_k.$$

D'autre part, si $r < n$ et $i \notin \text{supp}(\gamma)$, alors $\gamma(i) = i$.

Les r éléments j_1, j_2, \dots, j_r étant distincts, r est le plus petit entier positif tel que $\gamma^r = e$, d'où $o(\gamma) = r$.

COROLLAIRE (3.51). *Si τ est une transposition dans S_n , alors $\tau^2 = e$ donc $\tau^{-1} = \tau$.*

Remarques (3.52) :

1° Dans tout groupe symétrique S_n , l'inverse d'un r -cycle est un r -cycle. En effet, si $\gamma = (j_1, j_2, \dots, j_r)$, alors

$$\gamma^{-1} = \gamma^{r-1} = (j_r, j_{r-1}, \dots, j_1).$$

Cependant, pour p entier tel que $2 \leq p \leq r-2$, γ^p n'est pas nécessairement un cycle (exercice 22, chap. III).

Par exemple, dans S_4 , si γ_1 est la permutation circulaire :

$$\gamma_1^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ n'est pas un cycle.}$$

2° On déduit de l'exemple précédent qu'un produit de cycles n'est pas nécessairement un cycle.

On remarquera cependant que pour $1 \leq n \leq 3$, tout élément de S_n est un cycle.

PROPOSITION (3.53). *Dans S_n ($n \geq 2$), une permutation $\gamma \neq e$ est un cycle si et seulement si, dans la décomposition de N_n en γ -orbites, il n'existe qu'une seule γ -orbite non ponctuelle; le cardinal de celle-ci est alors égal à la longueur du cycle.*

Preuve : Soit γ un r -cycle dans S_n , $1 < r \leq n$. Posons

$$\gamma = (j_1, j_2, \dots, j_r);$$

d'après la proposition (3.50), γ est d'ordre r dans S_n , d'où

$$\Omega_\gamma(j_1) = \{j_1, \gamma(j_1), \dots, \gamma^{r-1}(j_1)\},$$

donc $\Omega_\gamma(j_1) = \{j_1, j_2, \dots, j_r\}$.

D'autre part, si $r \neq n$ et $i \notin \text{supp}(\gamma)$, on a $\Omega_\gamma(i) = \{i\}$; il n'existe donc qu'une seule γ -orbite non ponctuelle et son cardinal est r .

— Réciproquement, soit $\gamma \in S_n$ tel qu'il n'existe qu'une seule γ -orbite non ponctuelle de cardinal r :

$$\Omega_\gamma(j) = \{j, \gamma(j), \dots, \gamma^{r-1}(j)\}$$

$\Omega_\gamma(j)$ non ponctuelle implique $1 < r \leq n$ et $\gamma \neq e$.

Posons $j = j_1$, $\gamma(j) = j_2, \dots, \gamma^{r-1}(j) = j_r$; l'hypothèse implique alors que γ coïncide avec le r -cycle (j_1, j_2, \dots, j_r) .

C / Décomposition d'une permutation en un produit de cycles ou en un produit de transpositions

Remarque (3.54) : Dans un groupe S_n , on dira que deux cycles sont disjoints, si leurs supports sont disjoints.

D'après la proposition (3.39), deux cycles disjoints commutent.

THÉORÈME (3.55). Toute permutation $\sigma \neq e$ dans S_n s'écrit sous la forme :

$$\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_s \quad (19)$$

où $s \in \mathbf{N}^*$, $\gamma_1, \gamma_2, \dots, \gamma_s$ sont des cycles disjoints, tous différents de e et la décomposition (19) est unique à l'ordre des facteurs près.

Preuve : Soit $\sigma \neq e$ dans S_n ; le support de σ étant non vide, il existe au moins une σ -orbite non ponctuelle $\Omega_\sigma(i)$.

Si $\Omega_\sigma(i) = \{i, \sigma(i), \dots, \sigma^{p-1}(i)\}$ avec $2 \leq p \leq n$; posons

$$i = j_1, \quad \sigma(i) = j_2, \dots, \sigma^{p-1}(i) = j_p$$

et notons γ le cycle (j_1, j_2, \dots, j_p) .

La restriction de σ à $\{j_1, j_2, \dots, j_p\}$ est égal à la restriction de γ à son support. Ainsi, à toute σ -orbite non ponctuelle Ω , on peut associer un cycle γ dont le support est Ω .

Soit $\{\Omega_q\}_{1 \leq q \leq s}$, la famille des σ -orbites non ponctuelles distinctes dans N_n . A toute σ -orbite Ω_q associons, comme plus haut, le cycle γ_q , dont le support est Ω_q . Les σ -orbites Ω_q ($1 \leq q \leq s$) étant deux à deux disjointes, les cycles γ_q ($1 \leq q \leq s$) sont deux à deux disjoints, donc ils commutent entre eux.

Posons $\sigma' = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_s$ et comparons σ' et σ .

Soit $j \in \bigcup_{1 \leq q \leq s} \Omega_q$; il existe l ($1 \leq l \leq s$) tel que $j \in \Omega_l$.

Puisque $\sigma|_{\Omega_l} = \gamma_l|_{\Omega_l}$, on a $\sigma(j) = \gamma_l(j)$.

D'autre part, on peut écrire $\sigma' = \gamma_l \circ \prod_{\substack{1 \leq q \leq s \\ q \neq l}} \gamma_q$; pour $q \neq l$, $\gamma_q(j) = j$, d'où $\sigma'(j) = \gamma_l(j)$.

De plus, s'il existe $k \in \mathbb{N}_n \setminus \bigcup_{1 \leq q \leq s} \Omega_q$, on a $\sigma(k) = k$ et aussi $\sigma'(k) = k$. On en conclut que $\sigma = \sigma'$.

Supposons que $\sigma = \gamma'_1 \circ \gamma'_2 \circ \dots \circ \gamma'_r$ soit une autre décomposition de σ en un produit de cycles disjoints, tous différents de e . Pour tout p ($1 \leq p \leq r$), notons Ω'_p la γ'_p -orbite non ponctuelle; les cycles γ'_p étant disjoints, les σ -orbites non ponctuelles sont alors les Ω'_p , pour $1 \leq p \leq r$. La décomposition de \mathbb{N}_n en σ -orbites étant unique, on en déduit que $r = s$ et qu'il existe une permutation π dans le groupe symétrique S_s telle que $\Omega'_p = \Omega_{\pi(p)}$ et par suite $\gamma'_p = \gamma_{\pi(p)}$; d'où l'unicité de la décomposition (19) à l'ordre des facteurs près.

Remarque (3.56) :

1° Compte tenu de son unicité, la décomposition d'une permutation σ sous la forme (19) sera appelée : *décomposition canonique de σ en un produit de cycles*.

2° Le théorème (3.55) exprime que tout groupe S_n est engendré par l'ensemble de ses cycles.

Exemple (3.57) : Soit σ la permutation du groupe S_6 considérée dans l'exemple (3.42). La décomposition de \mathbb{N}_6 en σ -orbites implique $\sigma = \gamma_1 \circ \gamma_2$ où $\gamma_1 = (1, 5, 3)$ et $\gamma_2 = (4, 6)$.

On écrira

$$\sigma = (1, 5, 3) (4, 6).$$

Remarque (3.58) : Etant donné $\sigma \in S_n$, si $\{\Omega_q\}_{1 \leq q \leq t}$ est la famille de toutes les σ -orbites distinctes, alors, en associant éventuellement à toute σ -orbite ponctuelle le cycle e de longueur 1, on obtient, par la méthode du théorème (3.55), une décomposition de σ en produit de t cycles disjoints :

$$\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_t$$

telle que

$$\sum_{1 \leq q \leq t} \text{long}(\gamma_q) = n,$$

car pour tout $q (1 \leq q \leq t)$, $\text{long}(\gamma_q) = |\Omega_q|$.

PROPOSITION (3.59). Soit $\sigma \neq e$ dans S_n ($n \geq 2$); si $\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_s$ est la décomposition canonique de σ , alors l'ordre de σ dans le groupe S_n est égal au PPCM des longueurs des cycles γ_q ($1 \leq q \leq s$).

Preuve : Pour tout q ($1 \leq q \leq s$) posons $\Omega_q = \text{supp}(\gamma_q)$ et $r_q = \text{long}(\gamma_q) = |\Omega_q|$. Soit l le PPCM des r_q , dans \mathbb{N}^* . Quel que soit q ($1 \leq q \leq s$), l est multiple de r_q , donc $\gamma_q^l = e$; or, les γ_q commutent donc

$$\sigma^l = \gamma_1^l \circ \gamma_2^l \circ \dots \circ \gamma_s^l = e;$$

on en déduit que, si $k = o(\sigma)$, alors k divise l .

D'autre part, $\gamma_q \Omega_q = \sigma_{\Omega_q}$, d'où $\gamma_q^k \Omega_q = (\gamma_q \Omega_q)^k = \sigma_{\Omega_q}^k = e$; Ω_q étant le support de γ_q^k , on a $\gamma_q^k = e$; par suite, k est multiple de r_q , quel que soit $q (1 \leq q \leq s)$, donc l divise k . On en conclut que $k = l$.

THÉORÈME (3.60). Pour tout $n \geq 2$ dans \mathbb{N} , toute permutation $\sigma \in S_n$ se décompose, de manière non unique, en un produit de transpositions non permutables, en général.

Preuve : $n \geq 2$ implique qu'il existe au moins une transposition τ dans S_n . $e = \tau^2$, donc e est produit de transpositions.

Sachant que toute permutation $\sigma \neq e$ dans S_n est un produit de cycles (théorème (3.55)), il suffit de prouver que tout cycle est un produit de transpositions.

Soit $\gamma = (j_1, j_2, \dots, j_r)$ dans S_n , tel que $1 < r \leq n$.

Notons (j_p, j_q) la transposition qui échange j_p et j_q tels que $1 \leq p < q \leq n$; en écrivant $(j_p, j_q)(j_1, j_m)$ à la place de $(j_p, j_q) \circ (j_1, j_m)$, posons :

$$\gamma' = (j_1, j_2)(j_2, j_3) \dots (j_{r-1}, j_r).$$

Pour tout k ($1 \leq k \leq r-1$), on a $\gamma'(j_k) = j_{k+1} = \gamma(j_k)$; de plus $\gamma'(j_r) = j_1 = \gamma(j_r)$. S'il existe $k \in N_n \setminus \text{supp}(\gamma)$, alors $\gamma'(k) = k = \gamma(k)$.

On en déduit que $\gamma' = \gamma$, d'où

$$(j_1, j_2, \dots, j_r) = (j_1, j_2)(j_2, j_3) \dots (j_{r-1}, j_r) \quad (20)$$

De la décomposition canonique d'une permutation σ en un produit de cycles, on peut donc déduire une décomposition de σ en produit de transpositions, mais cette dernière *n'est pas unique* si $n \geq 3$, car, étant donné une transposition quelconque (j, k) dans S_n , on vérifie facilement que

$$(j, k) = (1, j)(1, k)(1, j) \quad (21)$$

D'autre part, si j, k, l sont trois entiers distincts dans N_n , on a

$$(j, k)(k, l) \neq (k, l)(j, k);$$

on en déduit que dans une décomposition d'une permutation $\sigma \in S_n$ ($n \geq 3$) en un produit de transpositions, *deux transpositions distinctes non disjointes ne sont pas permutable*.

Exemples (3.61) :

1° Soit $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix}$; γ est le cycle $(2, 4, 6, 5)$ dans S_6 .

En appliquant la formule (20), on obtient :

$$\gamma = (2, 4)(4, 6)(6, 5).$$

2° Soit $\sigma \in S_6$ la permutation de l'exemple (3.42), dont la décomposition canonique (19) a été déterminée dans l'exemple (3.57) : $\sigma = (1, 5, 3)(4, 6)$.

Compte tenu de la formule (20), on a $\sigma = (1, 5)(5, 3)(4, 6)$.

D'après la relation (21), on peut écrire

$$(5, 3) = (1, 5)(1, 3)(1, 5),$$

on en déduit que $\sigma = (1, 3)(1, 5)(4, 6)$.

Remarques (3.62) : Le théorème (3.60) peut être démontré directement, c'est-à-dire sans passer par la décomposition en cycles (exercice 33, chap. III). Ce théorème exprime que, *pour* $n \geq 2$,

le groupe S_n est engendré par l'ensemble de ses transpositions. Mais il existe des familles plus restreintes de générateur de S_n , comme le montrent les deux propositions suivantes (voir aussi l'exercice 24, chap. III).

PROPOSITION (3.63). *Tout groupe symétrique S_n ($n \geq 2$) est engendré par l'ensemble des $(n-1)$ transpositions de la forme $(1, i)$, telles que $2 \leq i \leq n$.*

Ce résultat se déduit de la formule (21) et du théorème (3.60).

PROPOSITION (3.64). *Tout groupe S_n ($n \geq 2$) est engendré par les $(n-1)$ transpositions de la forme $(i, i+1)$ telles que $1 \leq i \leq n-1$.*

Preuve : Il suffit de montrer que dans S_n toute transposition (p, q) telle que $1 \leq p < q \leq n$ est produit de transposition de la forme $(i, i+1)$.

On raisonne par récurrence sur $(q-p)$.

— Pour $q-p=1$, on a $(p, q) = (p, p+1)$.

— Pour $q-p > 1$, on vérifie que :

$$(p, q) = (q-1, q)(p, q-1)(q-1, q);$$

l'hypothèse de récurrence implique alors le résultat énoncé.

D / Signature d'une permutation

Définition (3.65) : Soit $\sigma \in S_n$ ($n \geq 1$); si t est le nombre des σ -orbites distinctes dans N_n , on pose :

$$\varepsilon(\sigma) = (-1)^{n-t} \quad (22)$$

et $\varepsilon(\sigma)$ sera appelée *signature de la permutation σ* .

Remarque (3.66) :

— Si $\sigma = e$, alors $t = n$, donc $\varepsilon(e) = 1$.

— Si τ est une transposition dans S_n , alors $t = n-1$, d'où

$$\varepsilon(\tau) = -1 \quad (23)$$

— Si γ est un r -cycle dans S_n , on a $t = n-r+1$, d'où

$$\varepsilon(\gamma) = (-1)^{r-1} \quad (24)$$

LEMME (3.67). Soit $\sigma \in S_n$ ($n \geq 2$); alors, quelle que soit la transposition $\tau \in S_n$, on a :

$$\varepsilon(\sigma \circ \tau) = -\varepsilon(\sigma) \quad (25)$$

Preuve : Supposons $\tau = (i, j)$.

On remarque que si $\Omega_\sigma(k)$ est une σ -orbite ne contenant ni i , ni j , alors $\Omega_{\sigma \circ \tau}(k) = \Omega_\sigma(k)$. Considérons alors les σ -orbites contenant i ou j .

1^{er} cas : i et j sont dans deux σ -orbites distinctes; soit :

$$\Omega_\sigma(i) = \{i, \sigma(i), \dots, \sigma^{p-1}(i)\}$$

$$\Omega_\sigma(j) = \{j, \sigma(j), \dots, \sigma^{q-1}(j)\}.$$

Déterminons $\Omega_{\sigma \circ \tau}(i)$.

$$\sigma \circ \tau(i) = \sigma(j);$$

on en déduit que :

$$\text{pour } 1 \leq r \leq q-1, \quad (\sigma \circ \tau)^r(i) = \sigma^r(j) \quad \text{et} \quad (\sigma \circ \tau)^q(i) = j;$$

$$\text{alors } \sigma \circ \tau(j) = \sigma(i) \Rightarrow (\sigma \circ \tau)^{q+1}(i) = \sigma(i),$$

donc pour

$$1 \leq s \leq p-1, \quad (\sigma \circ \tau)^{q+s}(i) = \sigma^s(i) \quad \text{et} \quad (\sigma \circ \tau)^{q+p}(i) = i;$$

par suite :

$$\Omega_{\sigma \circ \tau}(i) = \{i, \sigma(j), \dots, \sigma^{q-1}(j), j, \sigma(i), \dots, \sigma^{p-1}(i)\}.$$

Les éléments des σ -orbites distinctes de i et de j se trouvent donc regroupés dans une même $\sigma \circ \tau$ -orbite.

2^e cas : i et j sont dans une même σ -orbite; soit :

$$\Omega_\sigma(i) = \{i, \sigma(i), \dots, \sigma^{p-1}(i)\}.$$

$j \neq i$ et $j \in \Omega_\sigma(i)$ implique qu'il existe un unique entier r tel que $1 \leq r \leq p-1$ et $\sigma^r(i) = j$.

Déterminons $\Omega_{\sigma \circ \tau}(i)$.

$$\sigma \circ \tau(i) = \sigma(j) = \sigma^{r+1}(i),$$

d'où, pour

$$1 \leq l < p - r, \quad (\sigma \circ \tau)^l(i) = \sigma^{r+l}(i) \quad \text{et} \quad (\sigma \circ \tau)^{p-r}(i) = i;$$

par suite,

$$\Omega_{\sigma \circ \tau}(i) = \{i, \sigma^{r+1}(i), \dots, \sigma^{p-1}(i)\}.$$

On constate que $j \notin \Omega_{\sigma \circ \tau}(i)$ et de $\sigma \circ \tau(j) = \sigma(i)$ on déduit

$$\Omega_{\sigma \circ \tau}(j) = \{j, \sigma(i), \dots, \sigma^{r-1}(i)\}.$$

La σ -orbite contenant i et j se trouve scindée en deux $\sigma \circ \tau$ -orbites distinctes, contenant respectivement i et j .

On en conclut que si t est le nombre des σ -orbites distinctes, dans le premier cas, le nombre des $\sigma \circ \tau$ -orbites distinctes est $t - 1$ et, dans le second cas, il est $t + 1$, d'où

$$\varepsilon(\sigma \circ \tau) = -\varepsilon(\sigma).$$

THÉORÈME (3.68). Soit $\sigma \in S_n$ ($n \geq 2$);

Si σ est un produit de k transpositions, alors :

$$\varepsilon(\sigma) = (-1)^k \tag{26}$$

et si $\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k = \tau'_1 \circ \tau'_2 \circ \dots \circ \tau'_l$ sont deux décompositions de σ en produit de transpositions, alors les entiers k et l sont de même parité.

Preuve : Pour toute transposition $\tau \in S_n$, on a $\varepsilon(\tau) = -1$ (remarque (3.66)); par suite, la formule (26) se déduit facilement de la relation (25) du lemme (3.67). D'autre part,

$$\tau_1 \circ \tau_2 \circ \dots \circ \tau_k = \tau'_1 \circ \tau'_2 \circ \dots \circ \tau'_l$$

implique $(-1)^k = (-1)^l$, donc les entiers k et l sont nécessairement de même parité.

Remarque (3.69) : D'après ce qui précède, associer à tout $\sigma \in S_n$ sa signature $\varepsilon(\sigma)$ revient à définir une application $\varepsilon : S_n \rightarrow \{-1, 1\}$
 $\sigma \mapsto \varepsilon(\sigma).$

En considérant $\{-1, 1\}$ comme un *groupe multiplicatif* (sous-groupe de (\mathbb{Q}^*, \times) : exercice 8, chap. I), on démontre le résultat fondamental suivant :

THÉORÈME (3.70). Pour $n \geq 2$ dans \mathbf{N} , l'application

$$\begin{aligned}\varepsilon : S_n &\rightarrow \{-1, 1\} \\ \sigma &\mapsto \varepsilon(\sigma)\end{aligned}$$

est un épimorphisme de groupes.

Preuve : La condition $n \geq 2$ implique la surjectivité de ε ; vérifions que ε est un morphisme de groupes.

Soient σ et σ' dans S_n telles que :

$$\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k \quad \text{et} \quad \sigma' = \tau'_1 \circ \tau'_2 \circ \dots \circ \tau'_l$$

où les τ_i ($1 \leq i \leq k$) et les τ'_j ($1 \leq j \leq l$) sont des transpositions.

On a alors : $\sigma \circ \sigma' = \tau_1 \circ \dots \circ \tau_k \circ \tau'_1 \circ \dots \circ \tau'_l$, d'où, en appliquant la formule (26) :

$$\varepsilon(\sigma \circ \sigma') = (-1)^{k+l} = (-1)^k (-1)^l$$

et par suite

$$\varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma) \varepsilon(\sigma').$$

Définition (3.71) : Une permutation $\sigma \in S_n$ est dite *paire* si $\varepsilon(\sigma) = 1$ et *impaire* si $\varepsilon(\sigma) = -1$.

Remarques (3.72) :

1° Toute transposition est une permutation impaire.

2° Une permutation $\sigma \in S_n$ ($n \geq 2$) est paire (resp^t impaire) si et seulement si elle est produit d'un nombre pair (resp^t impair) de transpositions.

3° Quel que soit $\sigma \in S_n$, σ et σ^{-1} sont de même parité, c'est-à-dire que $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$; en effet, $\varepsilon(\sigma^{-1}) = (\varepsilon(\sigma))^{-1}$ dans le groupe $\{-1, 1\}$.

4° Etant donné $\sigma \in S_n$, le calcul de $\varepsilon(\sigma)$ se fait en appliquant les formules (22), (24), (26) et en utilisant les propriétés de mor-

phisme de l'application ε . En particulier, si on connaît la décomposition canonique de σ :

$$\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_l$$

telle que pour tout q ($1 \leq q \leq s$), $\text{long}(\gamma_q) = r_q$, alors

$$\varepsilon(\sigma) = (-1)^l \quad \text{où } l = \sum_{1 \leq q \leq s} r_q - s,$$

puisque, pour tout q ($1 \leq q \leq s$), $\varepsilon(\gamma_q) = (-1)^{r_q-1}$ (formule (24)).

Lorsque s est le nombre *total* des σ -orbites distinctes de N_n , on retrouve la formule (22).

Exemple (3.73) :

1° Soit σ dans S_8 la permutation considérée dans l'exemple (3.42); le nombre t des σ -orbites distinctes est 3, d'où ici $n - t = 6 - 3 = 3$. En appliquant la formule (22) on obtient $\varepsilon(\sigma) = (-1)^3 = -1$; σ est une permutation *impaire*, ce qui est confirmé par le calcul de $\varepsilon(\sigma)$ à partir de la décomposition canonique de σ (exemple (3.57)), ou à partir d'une décomposition de σ en produit de transpositions (exemple (3.61)).

2° Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 5 & 6 & 8 & 1 & 7 & 3 \end{pmatrix}$ dans S_8 .

Déterminons les σ -orbites :

$$\Omega_\sigma(1) = \{1, 4, 6\}; \quad \Omega_\sigma(2) = \{2\};$$

$$\Omega_\sigma(3) = \{3, 5, 8\}; \quad \Omega_\sigma(7) = \{7\}.$$

Il y a 4 σ -orbites distinctes, d'où $\varepsilon(\sigma) = (-1)^4 = 1$ (formule (22)), σ est une permutation *paire*.

Remarque (3.73) : Il existe plusieurs définitions de la signature d'une permutation (voir par exemple [5], [54], [56], [57]) mais toutes sont équivalentes car on peut démontrer que, pour $n \geq 2$, il n'existe qu'un seul épimorphisme ε de S_n sur le groupe multiplicatif $\{-1, 1\}$ et que $\varepsilon(\tau) = -1$ pour toute transposition $\tau \in S_n$.

La définition classique de $\varepsilon(\sigma)$ par la formule

$$\varepsilon(\sigma) = \prod_{1 \leq i < k \leq n} \frac{\sigma(k) - \sigma(i)}{k - i} \quad (27)$$

amène au calcul de la signature à l'aide du « nombre d'inversions de σ », méthode que nous n'avons pas considérée dans cet ouvrage (se reporter aux références indiquées plus haut).

E / Groupe alterné A_n

Etant donné un groupe symétrique S_n , désignons par A_n l'ensemble des permutations paires de S_n .

Pour $n = 1$, on a $A_1 = S_1 = (\epsilon)$.

Pour $n \geq 2$, $A_n = \{\sigma \in S_n; \epsilon(\sigma) = 1\}$ est le noyau de l'épimorphisme $\epsilon: S_n \rightarrow \{-1, 1\}$. A_n est donc un sous-groupe de S_n .

$(A_n = \text{Ker } \epsilon \text{ et } \epsilon \text{ surjectif}) \Rightarrow \frac{S_n}{A_n} \simeq \{-1, 1\}$; (théorème 2.27),

par suite, $[S_n : A_n] = 2$, d'où $o(A_n) = \frac{n!}{2}$, puisque $o(S_n) = n!$; on en déduit l'énoncé suivant :

PROPOSITION (3.75). *Pour tout $n \geq 2$, l'ensemble A_n des permutations paires de S_n forme un sous-groupe de S_n , d'ordre $\frac{n!}{2}$.*

Définition (3.76) : Pour tout $n \in \mathbb{N}^*$, le groupe A_n des permutations paires de S_n est appelé *groupe alterné de degré n* .

Remarque (3.77) : Pour $n \geq 2$, les deux classes de S_n modulo A_n sont A_n et $\tau A_n = \{\tau \circ \sigma; \sigma \in A_n\}$ où τ est une transposition quelconque de S_n .

$$A_n = \text{Ker } \epsilon \Rightarrow \tau A_n = A_n \tau = \{\sigma \circ \tau; \sigma \in A_n\}.$$

τA_n est l'ensemble des permutations impaires de S_n et cet ensemble n'est pas un sous-groupe de S_n .

3 — Groupes diédraux D_n

Soient P le plan affine euclidien et $\mathcal{J}(2)$ le groupe des isométries du plan P (exemple (1.34)).

On rappelle que $\mathcal{J}(2)$ est un sous-groupe du groupe symé-

trique SP et que, dans le plan P , toute rotation, toute symétrie par rapport à une droite est un élément du groupe $\mathcal{I}(2)$ (exercice 26, chap. I).

Pour $n \geq 2$, dans N notons \mathcal{P}_n un polygone régulier à n sommets dans le plan P . Soit D_n l'ensemble des isométries du plan P qui conservent le polygone \mathcal{P}_n , autrement dit, qui conservent globalement l'ensemble de ses n sommets.

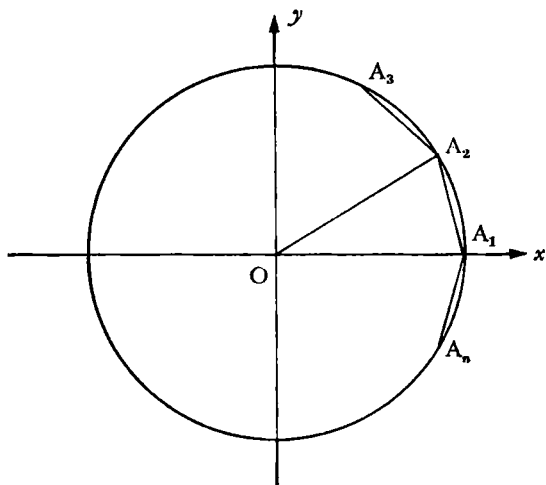
On vérifie facilement que D_n est un sous-groupe de $\mathcal{I}(2)$.

Définition (3.70) : Pour tout $n \geq 2$ dans N , le groupe D_n est appelé *groupe diédral de degré n* .

PROPOSITION (3.71). Pour tout $n \geq 2$ dans N , le groupe diédral D_n est fini, d'ordre $2n$.

Preuve : Soit O le centre du polygone \mathcal{P}_n dont les sommets seront notés A_1, A_2, \dots, A_n .

Considérons dans le plan P le repère orthonormé Oxy tel que A_1 soit sur Ox . En prenant pour unité de longueur le rayon du cercle circonscrit au polygone \mathcal{P}_n , les sommets A_1, A_2, \dots, A_n peuvent être considérés comme les images des racines n -ième de l'unité dans le plan complexe.



a) Pour k entier tel que $0 \leq k \leq n-1$, notons ρ_k la rotation de centre O et d'angle $\frac{2k\pi}{n}$, dans le plan P .

Pour tout entier α tel que $1 \leq \alpha \leq n$, on a

$$\rho_k(A_\alpha) = A_\beta, \quad 1 \leq \beta \leq n \quad \text{et} \quad \beta \equiv \alpha + k \pmod{n}$$

D_n contient donc l'ensemble Γ_n des rotations ρ_k , $0 \leq k \leq n-1$.

D'autre part, pour j et k compris entre 0 et $n-1$, $\rho_k \circ \rho_j = \rho_l$, avec $0 \leq l \leq n-1$ et $l \equiv j + k \pmod{n}$; de plus, dans le groupe D_n , $\rho_k^{-1} = \rho_{n-k}$; d'où $\Gamma_n \leq D_n$. U_n étant le groupe cyclique des racines n -ième de l'unité dans \mathbb{C} (exemple (3.8)), d'après ce qui précède, l'application :

$$\begin{aligned} \Gamma_n &\rightarrow U_n \\ \rho_k &\mapsto \exp \frac{2k\pi i}{n} \end{aligned}$$

est un isomorphisme de groupes; par suite,

Γ_n est un groupe cyclique d'ordre n .

Γ_n peut être considéré comme engendré par ρ_1 ; alors pour tout k ($0 \leq k \leq n-1$), $\rho_k = \rho_1^k$; en particulier $\rho_0 = \rho_1^0 = \text{id}_P$, que l'on notera e ; d'où

$$\Gamma_n = \{e, \rho_1, \rho_1^2, \dots, \rho_1^{n-1}\} \quad (28)$$

b) Soit σ la symétrie par rapport à Ox , dans le plan P .

$\sigma(A_1) = A_1$ et pour tout α tel que $2 \leq \alpha \leq n$, $\sigma(A_\alpha) = A_{n-\alpha+2}$; par suite, $\sigma_1 \in D_n$ et on remarque que $\sigma^2 = e$.

D'autre part, $\sigma \notin \Gamma_n$; en effet, on a $\sigma \neq e$ et $\sigma(A_1) = A_1$, or pour tout k ($1 \leq k \leq n-1$), $\rho_1^k(A_1) = A_{1+k}$.

On en déduit que, quel que soit k ($0 \leq k \leq n-1$), $\rho_1^k \circ \sigma \notin \Gamma_n$, car $\rho_1^k \circ \sigma \in \Gamma_n$ impliquerait $\sigma \in \Gamma_n$.

De plus, les n éléments $\rho_1^k \circ \sigma$, $0 \leq k \leq n-1$, sont distincts; en effet,

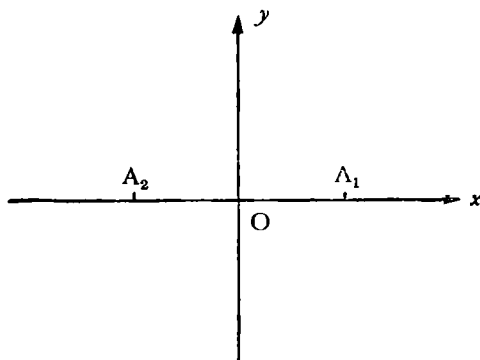
$$\rho_1^k \circ \sigma = \rho_1^j \circ \sigma \Rightarrow \rho_1^k = \rho_1^j \Rightarrow k = j.$$

c) Les résultats obtenus dans a) et b) prouvent que D_n contient au moins $2n$ éléments distincts :

$$e, \rho_1, \dots, \rho_1^{n-1}, \sigma, \rho_1 \circ \sigma, \dots, \rho_1^{n-1} \circ \sigma.$$

Vérifions que D_n contient exactement $2n$ éléments.

— Si $n = 2$:



Les seules isométries du plan P qui conservent A_1 et A_2 sont : la symétrie σ par rapport à Ox , la symétrie par rapport à O , c'est-à-dire la rotation ρ_1 de centre O et d'angle π , la symétrie par rapport à Oy qui coïncide avec $\rho_1 \circ \sigma = \sigma \circ \rho_1$ et l'identité e ; d'où

$$D_2 = \{e, \rho_1, \sigma, \rho_1 \circ \sigma\} \quad (29)$$

— Pour $n \geq 3$, soit $f \in \mathcal{I}(2)$ tel que $f(\mathcal{P}_n) = \mathcal{P}_n$.

f transforme A_1 en l'un des n sommets A_1, A_2, \dots, A_n .

Lorsque $f(A_1)$ est fixé, il ne reste que deux positions possibles pour $f(A_2)$, car f conserve les distances :

$$d(f(A_1), f(A_2)) = d(A_1, A_2).$$

Par suite, dès que $f(A_2)$ est fixé, les $f(A_i)$ pour $3 \leq i \leq n$ sont déterminés de façon unique.

On en conclut qu'il n'existe que $2n$ isométries du plan P qui conservent le polygone \mathcal{P}_n , d'où :

$$D_n = \{e, \rho_1, \dots, \rho_1^{n-1}, \sigma, \rho_1 \circ \sigma, \dots, \rho_1^{n-1} \circ \sigma\} \quad (30)$$

D_n est donc engendré par ρ_1 et σ .

On remarque que de la même manière on aurait pu prouver que :

$$D_n = \{e, \rho_1, \dots, \rho_1^{n-1}, \sigma, \sigma \circ \rho_1, \dots, \sigma \circ \rho_1^{n-1}\} \quad (30')$$

PROPOSITION (3.72). *Les notations sont celles de la proposition (3.71) :*

- 1° dans tout groupe diédral D_n ($n \geq 2$ dans \mathbb{N}), tout élément $\rho_1^k \circ \sigma$ ($0 \leq k \leq n-1$) est d'ordre 2;
 2° D_n est non abélien pour $n \geq 3$.

Preuve :

1° Pour $k = 0$, $\rho_1^0 \circ \sigma = \sigma$; or on a $\sigma \neq e$ et $\sigma^2 = e$, donc $o(\sigma) = 2$.

Pour $k = 1$, considérons $(\rho_1 \circ \sigma)^2$.

— Si $n = 2$, on a vu que $\rho_1 \circ \sigma$ est la symétrie par rapport à Oy , d'où $o(\rho_1 \circ \sigma) = 2$.

— Si $n \geq 3$, on a vu, dans la partie c) de la démonstration de la proposition (3.71), que toute isométrie $f \in D_n$ est déterminée par les images de A_1 et A_2 ; or on vérifie facilement que :

$$(\rho_1 \circ \sigma)^2(A_1) = A_1 \quad \text{et} \quad (\rho_1 \circ \sigma)^2(A_2) = A_2,$$

d'où $(\rho_1 \circ \sigma)^2 = e$; par suite $o(\rho_1 \circ \sigma) = 2$, car $\rho_1 \circ \sigma \neq e$.

Pour $k > 1$

$$\sigma \circ \rho_1^k \circ \sigma = \sigma \circ \rho_1^k \circ \sigma^{-1}, \quad \text{puisque } \sigma^{-1} = \sigma;$$

$$\text{alors } \sigma \circ \rho_1^k \circ \sigma = (\sigma \circ \rho_1 \circ \sigma^{-1})^k$$

$$\text{d'où } \sigma \circ \rho_1^k \circ \sigma = \rho_1^{-k}, \quad \text{car } \sigma \circ \rho_1 \circ \sigma^{-1} = \rho_1^{-1};$$

par suite

$$(\rho_1^k \circ \sigma)^2 = e$$

et $\rho_1^k \circ \sigma \neq e$ implique $o(\rho_1^k \circ \sigma) = 2$.

2° Pour $n = 2$, $D_2 = \{e, \rho_1, \sigma, \rho_1 \circ \sigma\}$ tel que $\rho_1 \circ \sigma = \sigma \circ \rho_1$, donc D_2 est abélien.

On remarque que $D_2 = \langle \rho_1 \rangle \langle \sigma \rangle$ et $\langle \rho_1 \rangle \cap \langle \sigma \rangle = (e)$, d'où

$$D_2 \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \quad (\text{groupe de Klein})$$

Pour $n \geq 3$, $\sigma \circ \rho_1 \circ \sigma^{-1} = \rho_1^{-1}$ et $\rho_1^{-1} = \rho_1^{n-1} (\neq \rho_1)$, donc D_n est non abélien.

Remarques (3.73) :

1° Pour tout k ($0 \leq k \leq n-1$), $(\rho_1^k \circ \sigma)^2 = e$ implique $\sigma \circ \rho_1^k = \rho_1^{-k} \circ \sigma$, d'où

$$\sigma \circ \rho_1^k = \rho_1^{n-k} \circ \sigma \quad (31)$$

Compte tenu de la proposition (1.47) et de l'égalité (30) (ou (30')), on a

$$D_n = \Gamma_n \langle \sigma \rangle = \langle \sigma \rangle \Gamma_n \quad (32)$$

2° On peut vérifier que les n éléments $\rho_1^k \circ \sigma$, $0 \leq k \leq n-1$, sont les *symétries du plan P par rapport aux n axes de symétries du polygone \mathcal{P}_n* , ce qui justifie géométriquement le fait que ces éléments sont d'ordre 2 dans le groupe D_n .

3° Pour $n > 3$, D_n a un unique sous-groupe cyclique d'ordre n , Γ_n , puisque tout élément de $D_n \setminus \Gamma_n$ est d'ordre 2.

4° Pour $n \geq 3$, D_n est isomorphe à un sous-groupe de S_n et pour $n = 3$, $D_3 \simeq S_3$. En effet, quel que soit $f \in D_n$, la restriction de f à l'ensemble des sommets A_1, A_2, \dots, A_n du polygone \mathcal{P}_n est une permutation de ces points; on peut donc considérer l'application :

$$\begin{aligned} \gamma : D_n &\rightarrow S_n \\ f &\mapsto \gamma_f \end{aligned}$$

tel que $\gamma_f(i) = j \Leftrightarrow f(A_i) = A_j$.

On vérifie que γ est un monomorphisme de groupes, d'où $D_n \simeq \text{Im } \gamma$.

Pour $n = 3$, $o(D_3) = 6 = o(S_3)$; l'application injective γ est alors surjective, d'où $D_3 \simeq S_3$.

Pour $n > 3$, on a $2n < n!$, donc D_n est isomorphe à un sous-groupe propre du groupe symétrique S_n .

PROPOSITION (3.74). *Tout groupe G engendré par deux éléments a et b tels que*

$$o(a) = n \quad (n \geq 2), \quad o(b) = 2 \quad \text{et} \quad o(ab) = 2 \quad (33)$$

est isomorphe au groupe diédral D_n .

Preuve : Par hypothèse $G = \langle a, b \rangle$, par suite tout élément de G est un produit de puissances entières (positives, négatives ou nulles) de a et de b . Le groupe G peut donc être considéré comme engendré par $\langle a \rangle \cup \langle b \rangle$.

Par hypothèse,

$$\langle a \rangle = \{a^0 = e, a, a^2, \dots, a^{n-1}\} \quad \text{et} \quad \langle b \rangle = \{b^0 = e, b\}.$$

En raisonnant comme dans les démonstrations des propositions (3.71) et (3.72), on prouve ici que :

- pour $0 \leq k \leq n-1$, les éléments $a^k b$ sont deux à deux distincts et $b \notin \langle a \rangle$ implique qu'aucun d'eux n'appartient à $\langle a \rangle$;
- de plus $o(ab) = 2$ implique, quel que soit k ($0 \leq k \leq n-1$),

$$o(a^k b) = 2 \tag{34}$$

$$\text{d'où} \quad ba^k = a^{n-k} b \tag{35}$$

On en déduit que $\langle a \rangle \langle b \rangle = \langle b \rangle \langle a \rangle$ est un sous-groupe de G et c'est alors le sous-groupe de G engendré par $\langle a \rangle \cup \langle b \rangle$ (voir remarque (1.48) 1°), par suite

$$G = \langle a \rangle \langle b \rangle,$$

$$\text{d'où} \quad G = \{e, a, \dots, a^{n-1}, b, ab, \dots, a^{n-1} b\}.$$

Le groupe G est donc d'ordre $2n$ et est parfaitement déterminé par la donnée de ses deux générateurs a et b satisfaisant aux conditions (33).

Or les générateurs ρ_1 et σ du groupe diédral D_n satisfont aux conditions (33); par suite un morphisme $\varphi \in \text{Hom}(D_n, G)$ tel que $\varphi(\rho_1) = a$ et $\varphi(\sigma) = b$ est nécessairement un isomorphisme de D_n sur G .

Remarque (3.75) :

Le groupe diédral D_4 n'est pas isomorphe au groupe des quaternions Q_8 .

Ces groupes sont tous deux d'ordre 8 et non abéliens, mais Q_8 n'a qu'un seul élément d'ordre 2, alors que D_4 en a cinq.

Exercices Chapitre III

Un groupe cyclique d'ordre k , multiplicatif, sera noté C_k .

- 1) Soient deux groupes cycliques C_m et C_n ($m \neq n$).

On pose $C_m = \langle x \rangle$ et $C_n = \langle y \rangle$.

a) Soient $a \in C_m$ et $b \in C_n$ tels que $o(a) = r$ et $o(b) = s$.
Quel est l'ordre de l'élément (a, b) dans le groupe $C_m \times C_n$?

b) A l'aide du résultat obtenu dans a), démontrer le corollaire (3.30).

2) Soient m et n des entiers non nuls dans \mathbb{N} .

a) Démontrer que m et n sont premiers entre eux, si et seulement si, quels que soient a et b dans \mathbb{Z} , il existe $x \in \mathbb{Z}$ tel que :

$$x \equiv a \pmod{m} \quad \text{et} \quad x \equiv b \pmod{n}.$$

[Utiliser le théorème de Bezout.]

b) On note, respectivement, σ et π les surjections canoniques :

$$\mathbb{Z} \rightarrow \frac{\mathbb{Z}}{m\mathbb{Z}} \quad \text{et} \quad \mathbb{Z} \rightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

A l'aide du résultat a), prouver que l'application

$$f: \mathbb{Z} \rightarrow \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

$$x \mapsto (\sigma(x), \pi(x))$$

est surjective si et seulement si m et n sont premiers entre eux; retrouver alors le résultat du théorème (3.29).

3) a) Déterminer le groupe multiplicatif G_{15} formé par les éléments inversibles de l'anneau $\frac{\mathbb{Z}}{15\mathbb{Z}}$.

b) Démontrer la propriété : $G_{15} \simeq C_2 \times C_4$.

4) a) (Théorème d'Euler) : Soit $n \in \mathbb{N}^*$; soit $a \in \mathbb{Z}^*$, *premier avec* n ; φ désignant la fonction d'Euler, démontrer la relation : $a^{\varphi(n)} \equiv 1 \pmod{n}$.

b) (Théorème de Fermat) ⁽⁴⁾ : Soient p un nombre *premier* et $a \in \mathbb{Z}$, prouver la relation : $a^p \equiv a \pmod{p}$.

5) a) Soit G un groupe *abélien* et $S = \{a_1, a_2, \dots, a_r\}$ une partie finie non vide de G ($r \geq 1$ dans \mathbb{N}).

Vérifier que

$$\langle S \rangle = \{a_1^{k_1} a_2^{k_2} \dots a_r^{k_r}; k_i \in \mathbb{Z} \text{ pour tout } i (1 \leq i \leq r)\}.$$

Comment s'écrivent les éléments de $\langle S \rangle$ si le groupe G est additif?

(4) Pierre-Simon de Fermat : mathématicien français (1601-1665).

b) Soit G un groupe abélien de type fini; démontrer que si tout élément de G est d'ordre fini, alors G est fini.

- 6) Soit G un groupe fini dans lequel tout élément x vérifie la condition : $x^2 = e$ [d'après l'exercice 5, chap. I, G est abélien].

Soit $\{a_1, a_2, \dots, a_r\}$, $r \geq 1$ dans N , une famille génératrice de G ; on suppose cette famille minimale, c'est-à-dire qu'aucune famille génératrice de G ne contient moins de r éléments.

a) Montrer que tout $x \in G$ s'écrit de façon unique :

$$x = a_1^{k_1} a_2^{k_2} \dots a_r^{k_r}, \quad \text{avec } k_i \in \{0, 1\}, \quad \text{pour tout } i \quad (1 \leq i \leq r).$$

b) Prouver que l'on a : $G \simeq C_2 \times C_2 \times \dots \times C_2$ (r fois); en déduire l'ordre de G .

- 7) Montrer que le groupe additif $\mathbf{Z} \times \mathbf{Z}$ est de type fini, mais n'est pas monogène.

- 8) a) Démontrer que le groupe $(\mathbf{Q}, +)$ n'est pas monogène.

[On pourra supposer $\langle \frac{m}{n} \rangle = \mathbf{Q}$ et montrer que $\frac{1}{2n} \in \mathbf{Q}$ conduit à une contradiction.] En déduire que le groupe $(\mathbf{R}, +)$ n'est pas monogène.

b) Démontrer que le groupe \mathbf{Q} est engendré par l'ensemble :

$$\left\{ \frac{1}{n!}; n \in \mathbf{N} \right\}.$$

c) Montrer que tout sous-groupe monogène, non nul, de \mathbf{Q} est infini.

d) Prouver que tout sous-groupe de type fini, non nul, de \mathbf{Q} est isomorphe au groupe \mathbf{Z} .

- 9) Soit \mathcal{H} le groupe des transformations conformes du plan (exercice 27, chap. I).

a) Soit G le sous-groupe de \mathcal{H} engendré par l'homographie g définie par $g(z) = z + 1$, pour tout $z \in \mathbf{C}$ et $g(\infty) = \infty$.

Montrer que G est isomorphe au groupe \mathbf{Z} .

b) Soient α et β dans \mathbf{C} tels que $\alpha \neq 1$; on considère $h \in \mathcal{H}$ tel que $h(z) = \alpha z + \beta$, pour tout $z \in \mathbf{C}$ et $h(\infty) = \infty$.

Démontrer que h est d'ordre fini dans \mathcal{H} si et seulement si α est une racine de l'unité dans \mathbf{C} .

- 10) Soit C_n un groupe cyclique d'ordre $n > 1$; on suppose $n = rs$ dans \mathbb{N}^* .

a) Soit $f: C_n \rightarrow C_n$ tel que, pour tout $a \in C_n$, $f(a) = a^r$.
Vérifier que $f \in \text{End}(C_n)$ et que $\text{Ker } f = \{a \in C_n; o(a) \text{ divise } r\}$.
En déduire que si $C_n = \langle x \rangle$, alors, pour tout $a \in \text{Ker } f$, il existe $k \in \mathbb{N}^*$, tel que $a = x^{sk}$.

Déterminer les ordres des sous-groupes $\text{Ker } f$ et $\text{Im } f$ de C_n .

b) Soit h l'endomorphisme de C_n tel que, pour tout $a \in C_n$, $h(a) = a^s$. Prouver que $\text{Im } f \subseteq \text{Ker } h$ et $\text{Im } h = \text{Ker } f$; en déduire que $\text{Im } f = \text{Ker } h$.

- 11) Dans le groupe $\text{GL}(2, \mathbb{C})$, trouver les ordres des matrices suivantes :

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

$$\begin{pmatrix} 2 & -3i \\ 1 & +i \end{pmatrix}, \quad \begin{pmatrix} 2 & -2i \\ -3 & +2i \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}.$$

- 12) Soit G l'ensemble des matrices de la forme $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ où a, b, c sont des nombres réels tels que $ac \neq 0$.

a) Vérifier que G est un sous-groupe de $\text{GL}(2, \mathbb{R})$ et que G est infini, non abélien.

b) Soit H l'ensemble des éléments de G pour lesquels $a = c = 1$. Prouver que H est un sous-groupe de G isomorphe au groupe $(\mathbb{R}, +)$.

c) Déterminer dans le groupe G tous les éléments d'ordre 2. Montrer que, dans G , le produit de deux éléments d'ordre 2 peut être d'ordre infini.

En vue des exercices 13, 14, 15 ci-dessous, on rappelle que si a et b sont deux entiers non nuls et si d est un diviseur commun à a et b dans \mathbb{Z}^* , alors d est P.G.C.D. de a et b si et seulement si :

$$(a = da' \text{ et } b = db') \Rightarrow a' \text{ et } b' \text{ premiers entre eux;}$$

$$l = da' b' \text{ est alors P.P.C.M. de } a \text{ et } b.$$

- 13) Soit C_n un groupe cyclique d'ordre $n > 1$ et soit k un entier tel que $1 \leq k \leq n - 1$.

Démontrer que $o(x^k) = \frac{n}{d}$ où d est P.G.C.D. de k et n .

- 14) Soit G un groupe quelconque; soient x et y deux éléments d'ordre fini dans G , tels que $o(x) = m > 1$ et $o(y) = n > 1$.

On suppose que x et y commutent dans G .

a) Prouver que xy est d'ordre fini dans G .

En serait-il nécessairement de même si x et y ne commuteraient pas? (voir l'exercice 12 ci-dessus).

b) Montrer que si m et n sont premiers entre eux, alors $o(xy) = mn$.

c) On suppose m et n non premiers entre eux et $\langle x \rangle \cap \langle y \rangle = \langle e \rangle$, e étant l'élément unité de G .

Prouver que $o(xy) = l$ où l est p.p.c.m. de m et n .

Si $\langle x \rangle \cap \langle y \rangle \neq \langle e \rangle$, vérifier que l'on peut seulement affirmer que $o(xy)$ divise l . Trouver au moins un exemple pour lequel $o(xy) < l$.

d) Étant donné une permutation $\sigma \neq e$ dans un groupe symétrique S_p ($p \geq 3$), retrouver, à l'aide des résultats précédents, que si $\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_s$ est la décomposition *canonique* de σ en un produit de cycles, alors l'ordre de σ , dans le groupe S_p , est le p.p.c.m. des longueurs des cycles γ_i ($1 \leq i \leq s$) (proposition (3.59)).

15) Soit G un groupe *abélien* fini ($G \neq \{e\}$).

Soit $s = \sup \{o(x); x \in G\}$. Démontrer que $x^s = e$, quel que soit $x \in G$ (voir l'exercice 14 ci-dessus).

16) Soit p un nombre premier; on considère le groupe $G = \frac{\mathbb{Z}}{p^2\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$.

Combien le groupe G contient-il :

- a) d'éléments d'ordre p ?
- b) d'éléments d'ordre p^2 ?
- c) de sous-groupes d'ordre p ?
- d) de sous-groupes d'ordre p^2 ?

17) *Étude du groupe des automorphismes d'un groupe monogène.*

Soit G un groupe monogène; on pose $G = \langle x \rangle$.

a) Montrer que, quel que soit $\alpha \in \text{Aut}(G)$, $\alpha(x)$ est un générateur de G .

b) On suppose G cyclique d'ordre $n > 1$. Étant donné un entier k premier avec n et tel que $1 \leq k \leq n-1$, on considère l'application $\lambda: G \rightarrow G$. Vérifier que $\lambda \in \text{Aut}(G)$.

$$a \mapsto a^k$$

Démontrer alors qu'il existe un isomorphisme de groupes de $\text{Aut}(G)$ sur le groupe multiplicatif G_n des éléments inversibles de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$; en conclure que le groupe $\text{Aut}(G)$ est abélien et d'ordre $\varphi(n)$.

c) On suppose G monogène infini; prouver que le groupe $\text{Aut}(G)$ est cyclique d'ordre 2.

d) A l'aide des résultats précédents, trouver des exemples de groupes non isomorphes dont les groupes d'automorphismes sont isomorphes.

- 18) Soit G un groupe *abélien, fini*, d'ordre $n > 1$; on note e son élément unité. On suppose que G satisfait à la condition (D) suivante :

(D) : { pour tout entier positif d divisant n , il existe au plus d éléments x de G tels que $x^d = e$.

On pose $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, les p_i ($1 \leq i \leq k$) étant des nombres premiers distincts et les α_i des entiers strictement positifs.

a) Montrer que pour tout i ($1 \leq i \leq k$) il existe au moins un élément $b_i \in G$ tel que $b_i^{\frac{n}{p_i^{\alpha_i}}} \neq e$. Vérifier que $b_i^{\frac{n}{p_i^{\alpha_i}}} \neq e$ implique $b_i^{\frac{n}{p_i^{\alpha_i}}} \neq e$.

En déduire que pour tout i ($1 \leq i \leq k$) il existe $a_i \in G$ tel que $o(a_i) = p_i^{\alpha_i}$.

b) Démontrer, en utilisant le résultat b) de l'exercice 14 ci-dessus, que le groupe G est cyclique.

c) Soit K un corps fini (il est commutatif d'après le théorème de Wedderburn ⁽⁶⁾ [39]). On considère le groupe multiplicatif $K^* = K \setminus \{0\}$. Sachant que tout polynôme à une indéterminée sur un corps commutatif K , de degré $d \geq 1$, a au plus d racines dans K , démontrer à l'aide du résultat b) ci-dessus que le groupe K^* est cyclique.

En conclure que, si p est un nombre premier, le groupe G_p des éléments inversibles du corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est cyclique d'ordre $(p-1)$.

- 19) Soit G un groupe *fini* d'ordre $n > 1$, d'élément unité e .

On ne suppose pas G abélien, mais on suppose que G vérifie la condition (D) de l'exercice 18 ci-dessus.

On note D l'ensemble des entiers positifs diviseurs de n .

On remarque que D contient au moins 1 et n .

a) Pour tout $d \in D$, on désigne par $\alpha(d)$ le nombre des éléments de G , d'ordre d ; on a $\alpha(d) \geq 0$. Justifier l'égalité :

$$n = \sum_{d \in D} \alpha(d) \quad (1)$$

⁽⁶⁾ J. H. Maclagan Wedderburn, 1882-1948.

b) φ désignant la fonction d'Euler, démontrer que :

$$(d \in D \text{ et } \alpha(d) \neq 0) \Rightarrow \alpha(d) = \varphi(d).$$

c) En considérant un groupe cyclique C_n , justifier l'égalité :

$$n = \sum_{d \in D} \varphi(d) \quad (2)$$

d) Dédurre des résultats ci-dessus que l'on a $\alpha(n) > 0$; en conclure que G est cyclique.

20) Groupe des éléments inversibles de l'anneau $\frac{\mathbb{Z}}{p^n \mathbb{Z}}$, où p est un nombre premier et $n \geq 1$ dans \mathbb{N} .

On note G_{p^n} le groupe multiplicatif des éléments inversibles de $\frac{\mathbb{Z}}{p^n \mathbb{Z}}$. On rappelle que, pour $n = 1$, le groupe G_p est cyclique (voir exercice 18 ci-dessus).

1° Justifier la propriété : G_{p^n} est un groupe abélien d'ordre $p^{n-1}(p-1)$.

2° On considère le cas $p = 3$, $n = 2$. Déterminer le groupe G_9 , vérifier qu'il est cyclique et trouver tous ses générateurs.

Dans les trois questions suivantes, on suppose que le nombre premier p est impair et le but de ces questions est de prouver que, dans ce cas, pour tout $n \geq 1$ dans \mathbb{N} , le groupe G_{p^n} est cyclique.

3° Pour $n > 1$ dans \mathbb{N} et $x \in \mathbb{Z}$, on note \bar{x} la classe de x modulo $p^n \mathbb{Z}$ et \dot{x} la classe de x modulo p . On considère la correspondance :

$$\begin{aligned} \varphi : G_{p^n} &\rightarrow G_p \\ \bar{x} &\mapsto \dot{x} \end{aligned}$$

a) Vérifier que φ est une application et montrer que c'est un épimorphisme de groupes.

b) Quel est l'ordre du sous-groupe $\text{Ker } \varphi$ de G_{p^n} ?

Caractériser les éléments $x \in \mathbb{Z}$ tels que $\bar{x} \in \text{Ker } \varphi$.

c) Soit \dot{x} un générateur du groupe G_p ; dans G_{p^n} , on considère l'élément $\bar{y} = (\bar{x})^{p^{n-1}}$. Trouver l'ordre de \bar{y} dans G_{p^n} .

4° a) Soit $r \in \mathbb{N}$ tel que $1 \leq r \leq p-1$; C_p^r désignant le nombre des combinaisons de p éléments r à r , vérifier que $C_p^r = p\lambda$, où $\lambda \in \mathbb{N}^*$ et p ne divise pas λ .

b) Démontrer que, pour tout $r \in \mathbb{N}$, on a

$$(1+p)^p - 1 = p^{r+1} \mu, \quad \text{où } \mu \in \mathbb{N}^* \text{ et } p \text{ ne divise pas } \mu.$$

[Faire un raisonnement par récurrence sur r .]

c) Trouver l'ordre de $\overline{1+p}$ dans G_{p^n} .

5° Montrer que les résultats précédents impliquent que le groupe G_{p^n} est cyclique [voir exercice 14 ci-dessus].

En conclure que G_{p^n} est isomorphe à $\frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}}$.

6° On considère le cas où $p = 2$ et $n > 1$.

a) Déterminer les groupes G_4 , G_8 ; sont-ils cycliques?

b) Pour $n > 3$, prouver, grâce à un morphisme de groupes convenable de G_{2^n} dans G_8 , que le groupe G_{2^n} n'est pas cyclique.

- 21) Pour chacune des permutations suivantes, déterminer : sa décomposition canonique en produit de cycles disjoints, son ordre, sa signature et une décomposition en produit de transpositions

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 2 & 1 & 8 & 7 & 9 & 11 & 12 & 10 & 5 & 6 \end{pmatrix}$$

Calculer σ_1^{50} , σ_2^{100} , σ_3^{10} .

- 22) Etant donné un r -cycle γ , dans S_n ($n \geq 3$, $r \geq 3$) tel que $\gamma = (j_1, j_2, \dots, j_r)$, vérifier l'égalité :

$$\gamma = (j_1, j_r) (j_1, j_{r-1}) \dots (j_1, j_2).$$

- 23) Soit γ un r -cycle dans S_n ($n \geq 2$); pour quelles valeurs de p entier tel que $1 \leq p \leq r-1$, γ^p est-il un cycle?

- 24) Soit $n \geq 3$ dans N et γ un r -cycle dans S_n tel que

$$\gamma = (j_1, j_2, \dots, j_r).$$

a) Etant donné $\sigma \in S_n$, démontrer que $\sigma \circ \gamma \circ \sigma^{-1}$ est le r -cycle $(\sigma(j_1), \sigma(j_2), \dots, \sigma(j_r))$.

b) Soit $\gamma_1 = (1, 2, \dots, n)$ la permutation circulaire dans S_n ; p étant un entier tel que $1 \leq p \leq n$, expliciter la permutation γ_1^p .

On pose $\tau_1 = (1, 2)$; calculer $\gamma_1^p \circ \tau_1 \circ \gamma_1^{-p}$; en déduire que les permutations τ_1 et γ_1 engendrent S_n .

- 25) En application du résultat a) de l'exercice 24 ci-dessus, démontrer que, pour $n \geq 3$, le groupe $\text{Int}(S_n)$ des automorphismes intérieurs de S_n est isomorphe à S_n .

- 26) Soit $n \geq 4$ dans N . Pour i, j, k, l distincts dans N_n , vérifier les relations :

$$(i, j) (j, k) = (i, j, k) \quad \text{et} \quad (i, j) (k, l) = (i, j, k) (j, k, l).$$

En déduire que le groupe alterné A_n est engendré :

- par l'ensemble des 3-cycles de S_n ;
 - par l'ensemble des 3-cycles de la forme $(1, i, j)$ pour $2 \leq i \leq n$, $2 \leq j \leq n$;
 - par l'ensemble des 3-cycles de la forme $(1, 2, i)$, $3 \leq i \leq n$.
- 27) Dans S_4 on pose : $K = \{e, (1, 2) (3, 4), (1, 3) (2, 4), (1, 4) (2, 3)\}$.
Vérifier que K est un sous-groupe commutatif de A_4 ; écrire sa table de multiplication; en déduire que K est isomorphe au groupe de Klein.

- 28) a) Soit $H = \{\sigma \in S_5; \sigma(1) = 1\}$. Vérifier que H est un sous-groupe de S_5 et trouver son ordre.

b) Soit $K = \{\sigma \in S_5; \sigma(1) = 1 \text{ ou } \sigma(1) = 2\}$. Montrer que K n'est pas un sous-groupe de S_5 .

c) r et n étant des entiers tels que $3 \leq r \leq n$, on pose

$$F = \{\sigma \in S_n; \forall i (1 \leq i \leq r), \sigma(i) \in \{1, 2, \dots, r\}\}.$$

Prouver que F est un sous-groupe de S_n et déterminer son ordre.

- 29) Dans S_9 on considère les permutations suivantes :

$$\pi = (1, 2, 3) (4, 5, 6) (7, 8, 9), \quad \sigma = (4, 5, 6) (7, 8, 9),$$

$$\tau = (1, 4, 7) (2, 5, 8) (3, 6, 9).$$

a) Vérifier que π commute avec σ et τ .

b) Quels sont les ordres des permutations π, σ, τ et $\sigma \circ \tau$?

c) Calculer $\tau \circ \sigma \circ \tau^{-1}$ et $\tau^{-1} \circ \sigma \circ \tau$; en déduire que π est une puissance de $\sigma \circ \tau$.

- 30) Soit G un groupe fini, d'élément unité e . U désignant l'ensemble des éléments d'ordre 2 dans G , on suppose $\text{card}(U) > 1$.

a) Montrer que G est nécessairement d'ordre pair.

b) Soient u et v dans U , vérifier que l'on a $u^{-1} = u$ et $v^{-1} = v$; en déduire que le sous-groupe $\langle u, v \rangle$ de G engendré par u et v est tel que :

$$\langle u, v \rangle = \{e, u, v, (uv)^m, u(uv)^n, v(uv)^p; (m, n, p) \in \mathbb{Z}^3\}.$$

c) On pose $t = uw$ et on note k l'ordre de t dans G ; montrer que l'on peut écrire

$$\langle u, v \rangle = \{t, \dots, t^{k-1}, e, u, ut, \dots, ut^{k-1}\}.$$

Calculer $(ut)^2$; en conclure que $\langle u, v \rangle$ est isomorphe au groupe diédral D_k [on pourra distinguer les cas $k = 2$ et $k > 2$].

31) Soit \mathbf{R} considéré comme espace affine euclidien de dimension 1.

Les notations sont celles de l'exercice 6, chap. II.

A tout $n \in \mathbf{Z}$ on associe la translation $\tau_n : \mathbf{R} \rightarrow \mathbf{R}$ telle que $\tau_n(x) = x + n$.

a) Vérifier que, pour tout $n \in \mathbf{Z}$, on a $\tau_1^n = \tau_n$.

b) On pose $S_{\mathbf{R}}(\mathbf{Z}) = \{\varphi \in \mathcal{J}(1); \varphi(\mathbf{Z}) = \mathbf{Z}\}$; prouver que $S_{\mathbf{R}}(\mathbf{Z})$ est formé par l'ensemble des τ_1^n et des $\tau_1^n \circ \sigma_0$, pour $n \in \mathbf{Z}$, σ_0 étant l'isométrie de \mathbf{R} telle que $x \mapsto -x$ (voir l'exercice 6, chap. II); en déduire que $S_{\mathbf{R}}(\mathbf{Z})$ est un sous-groupe de $\mathcal{J}(1)$.

Le groupe $S_{\mathbf{R}}(\mathbf{Z})$ est appelé : *groupe diédral infini* et il est généralement noté D_{∞} .

32) a) Soit $n \geq 3$ dans \mathbf{N} ; on pose $\alpha = \exp\left(\frac{2\pi i}{n}\right)$ dans \mathbf{C} .

Démontrer que le groupe multiplicatif engendré par les matrices complexes :

$$X = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \quad \text{et} \quad Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

est isomorphe au groupe diédral D_n .

b) Vérifier que le groupe diédral D_4 est isomorphe au groupe multiplicatif engendré par les matrices réelles

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

33) Soit $n \geq 2$ dans \mathbf{N} . Démontrer par récurrence sur n que toute permutation $\sigma \in S_n$ est un produit de transpositions appartenant à S_n .

[Pour $n > 2$ et $\sigma \neq e$, dans S_n , vérifier qu'on ne restreint pas la généralité en supposant $\sigma(n) = k \neq n$; poser alors $\tau = (k, n)$; montrer que $\tau \circ \sigma$ peut être considéré comme un élément de S_{n-1} et utiliser l'hypothèse de récurrence.]

CHAPITRE IV

Sous-groupes normaux

1 — Notion de sous-groupe normal (ou distingué). Groupe quotient

Les résultats du chapitre II montrent que, dans un groupe G , les seules relations d'équivalence \mathcal{R} qui permettent de définir dans l'ensemble $\frac{G}{\mathcal{R}}$ une loi de composition quotient telle que $\frac{G}{\mathcal{R}}$ soit un groupe canoniquement homomorphe à G , sont les relations d'équivalence compatibles avec la loi de composition de G ; de plus, si \mathcal{R} est une telle relation, il existe un sous-groupe H de G tel que $\mathcal{R} = \mathcal{R}_H = {}_H\mathcal{R}$ (conséquence de la proposition (2.23)).

Or on sait (exemple (2.4)) que dans un groupe non abélien, pour un sous-groupe H quelconque, on a en général $\mathcal{R}_H \neq {}_H\mathcal{R}$; cependant, si H est le noyau d'un morphisme, alors les équivalences à droite et à gauche modulo H coïncident (proposition (2.26)).

Il est donc important de savoir distinguer, dans un groupe G , les sous-groupes H pour lesquels $\mathcal{R}_H = {}_H\mathcal{R}$, en effet, comme nous le verrons par la suite, ces sous-groupes jouent un rôle fondamental.

Définition (4.1) : Dans un groupe G , un sous-groupe H est dit *normal* (ou *distingué*) si $\mathcal{R}_H = {}_H\mathcal{R}$.

Remarque (4.2) :

- 1° Dans tout groupe G , (e) et G sont des sous-groupes normaux.
- 2° Dans un groupe abélien, tout sous-groupe est normal.

Notations (4.3) :

1° On écrira $H < G$ pour exprimer que H est un sous-groupe normal de G .

2° Si $H \triangleleft G$, on écrit :

$$x \equiv y \pmod{H}$$

« x équivalent à y modulo H », à la place de $x \mathcal{R}_H y$ ($\Leftrightarrow x_H \mathcal{R} y$).

L'ensemble quotient $\left(\frac{G}{H}\right)_d = \left(\frac{G}{H}\right)_o$ est noté $\frac{G}{H}$.

Le théorème suivant précise l'intérêt des sous-groupes normaux signalé dans l'introduction de ce chapitre; il est conséquence directe des propositions (2.21), (2.23) et de la remarque (2.22) :

THÉORÈME (4.4). *Si H est un sous-groupe normal d'un groupe G , alors l'ensemble quotient $\frac{G}{H}$ peut être muni de la loi de composition quotient induite par celle de G , telle que :*

$$\bar{x}\bar{y} = \overline{xy}, \text{ quels que soient } \bar{x}, \bar{y} \text{ dans } \frac{G}{H};$$

relativement à cette loi, $\frac{G}{H}$ est un groupe et l'application canonique $\pi : G \rightarrow \frac{G}{H}$ est un épimorphisme de groupes.

Définition (4.5) : Si $H \triangleleft G$, le groupe $\frac{G}{H}$ est appelé : *groupe quotient* de G par le sous-groupe normal H .

On a rappelé plus haut que le noyau d'un morphisme de groupes est un sous-groupe normal. Le théorème (4.4) montre que, réciproquement, tout sous-groupe normal est le noyau d'un morphisme de groupes; en effet, $H \triangleleft G$ implique $H = \text{Ker } \pi$, où π est l'épimorphisme canonique $G \rightarrow \frac{G}{H}$; d'où une première caractérisation des sous-groupes normaux :

THÉORÈME (4.6). *Dans un groupe G , on a $H \triangleleft G$ si et seulement s'il existe un groupe G' et un morphisme $f \in \text{Hom}(G, G')$ tel que $H = \text{Ker } f$.*

Exemple (4.7) :

1° On a vu au chapitre III que, pour tout entier $n > 1$, le groupe alterné A_n est le noyau du morphisme de groupes $\epsilon : S_n \rightarrow \{-1, 1\}$; on a donc $A_n \triangleleft S_n$.

2° Si E est un espace vectoriel de dimension finie sur un corps commutatif K , le groupe linéaire spécial $SL(E)$ est par définition le noyau du morphisme de groupes d tel que :

$$\begin{aligned} d : GL(E) &\rightarrow K^* \\ u &\mapsto \det(u), \end{aligned}$$

où $\det(u)$ est le déterminant de l'automorphisme linéaire u [50]; on en déduit que : $SL(E) \triangleleft GL(E)$.

On a donc aussi, pour tout entier $n > 1$, $SL(n, K) \triangleleft GL(n, K)$ (voir exemple (1.63)).

3° Pour un espace vectoriel euclidien E de dimension finie, le groupe orthogonal $O(E)$ est le noyau du morphisme λ tel que :

$$\begin{aligned} \lambda : GO(E) &\rightarrow \mathbf{R}_+^*, \\ u &\mapsto \lambda_u \end{aligned}$$

où λ_u est le rapport de la similitude u (exemple (1.64)); par suite on a :

$$O(E) \triangleleft GO(E).$$

2 — Notion de groupe simple

Définition (4.8) : Un groupe G est dit *simple* si $G \neq (e)$ et s'il n'a pas d'autre sous-groupe *normal* que G et (e) .

PROPOSITION (4.9). *Les seuls groupes simples abéliens sont les groupes cycliques d'ordre premier.*

Preuve : Un groupe cyclique G d'ordre premier est abélien et il n'a pas d'autres sous-groupes que (e) et G , donc il est nécessairement simple.

Réciproquement, supposons que G soit un groupe abélien simple; cette hypothèse implique $G \neq (e)$, donc il existe $x \neq e$

dans G . Le sous-groupe $\langle x \rangle$ étant normal dans le groupe abélien G , nécessairement $\langle x \rangle = G$.

Le groupe G est donc monogène et, puisqu'il est simple, il ne peut être que cyclique d'ordre premier.

Remarques et exemples : Dès les premiers développements de la *Théorie des groupes*, plusieurs familles infinies de groupes simples non abéliens sont connues; citons comme exemples :

- 1° les groupes alternés A_n , pour $n \geq 5$ (exercice 6, chap. V);
- 2° les groupes linéaires projectifs spéciaux $\text{PSL}_n(K)$ ([2], [8]) : K étant un corps commutatif et n un entier tel que $n > 1$, si $Z(\text{SL}_n(K))$ désigne le centre du groupe linéaire spécial $\text{SL}_n(K)$ (exemples (1.63) et (4.7)), on démontre que le groupe

$$\text{PSL}_n(K) = \frac{\text{SL}_n(K)}{Z(\text{SL}_n(K))}$$

est simple, sauf pour $n = 2$ et $K = \frac{\mathbb{Z}}{2\mathbb{Z}}$ ou $K = \frac{\mathbb{Z}}{3\mathbb{Z}}$ (voir [2], [41], [65]).

Un groupe $\text{PSL}_n(K)$ est fini ou infini suivant que K est fini ou infini.

Il existe d'autres familles de groupes simples, définies de façon analogue, c'est-à-dire à partir de certains sous-groupes de $\text{GL}_n(K)$ (voir les références ci-dessus).

Les groupes de matrices (groupes linéaires) ainsi que tous les groupes qui s'y rattachent (sous-groupes, groupes quotients, etc.) sont désignés depuis H. Weyl (1885-1955) [74] sous l'appellation : « *Groupes classiques* » ([19], [22]); aussi les groupes simples évoqués plus haut sont dits : « *Groupes simples classiques* », ils ont été mis en évidence par C. Jordan (1838-1922) [42] et L. E. Dickson (1874-1954) [21].

Par ailleurs, E. L. Mathieu (1835-1890) avait découvert vers 1860 cinq groupes finis simples qui n'appartenaient à aucune famille infinie connue de groupes simples, ce qui leur a valu l'appellation de groupes simples « *sporadiques* ». Il s'agissait de certains sous-groupes des groupes alternés A_{11} , A_{12} , A_{22} , A_{23} et A_{24} ; ils furent respectivement notés M_{11} , M_{12} , M_{22} , M_{23} , M_{24} [65].

Aucun autre groupe simple fini ne fut trouvé avant 1955; cette année-là, le mathématicien français C. Chevalley (1909-) donna une méthode de construction de familles de groupes simples,

parmi lesquelles on retrouvait celles qui étaient déjà connues [12].

Un autre résultat fondamental fut démontré en 1963 par les mathématiciens américains W. Feit et J. G. Thomson [29] :

« Tout groupe simple fini, non abélien, est d'ordre pair »

l'intérêt de cette propriété est d'impliquer l'existence d'au moins un élément d'ordre 2 dans tout groupe fini simple non abélien; cela résulte directement du 1^{er} théorème de Sylow (chap. VI), mais on peut aussi le démontrer de façon élémentaire (exercice 33, chap. IV).

A partir de 1964-1965, la découverte de nouveaux groupes « sporadiques » incita plusieurs mathématiciens, pour la plupart américains, à intensifier leurs recherches et à unir leurs efforts en vue d'aboutir à une « classification » complète de tous les groupes simples finis [33]; ils semblent y être parvenus vers la fin de l'année 1980 ([3], [17]).

3 — Etudes des sous-groupes normaux

A / Caractérisations et propriétés

THÉORÈME (4.10). *H est un sous-groupe normal d'un groupe G si et seulement s'il vérifie l'une des cinq conditions équivalentes suivantes :*

$$Hx = xH, \quad \forall x \in G \quad (1)$$

$$xHx^{-1} = H, \quad \forall x \in G \quad (2)$$

$$x^{-1}Hx = H, \quad \forall x \in G \quad (3)$$

$$xhx^{-1} \in H, \quad \forall h \in H, \quad \forall x \in G \quad (4)$$

$$x^{-1}hx \in H, \quad \forall h \in H, \quad \forall x \in G \quad (5)$$

Preuve : Par définition, $H \triangleleft G$ équivaut à $\mathcal{R}_H = {}_H\mathcal{R}$, or,

$$\mathcal{R}_H = {}_H\mathcal{R} \Leftrightarrow Hx = xH, \quad \forall x \in G,$$

d'où $H \triangleleft G \Leftrightarrow (1)$.

--- Supposons $Hx = xH$; pour tout $h \in H$, il existe $h' \in H$ tel que $hx = xh'$, c'est-à-dire $h = xh'x^{-1}$; d'où $H \subseteq xHx^{-1}$.

L'hypothèse implique aussi que, pour tout $h \in H$, il existe

$h'' \in H$ tel que $xh = h''x$, c'est-à-dire $xhx^{-1} = h''$, d'où $xHx^{-1} \subseteq H$; par suite (1) \Leftrightarrow (2).

— Compte tenu de la bijection $x \mapsto x^{-1}$ de G sur lui-même, on a (2) \Leftrightarrow (3) et aussi (5) \Leftrightarrow (4).

— Montrons que (1) équivaut à (4).

Si $Hx = xH$, alors pour tout $h \in H$, $xh \in Hx$, donc $xhx^{-1} \in H$; on en déduit : (1) \Rightarrow (4). Supposons (4) vérifiée; soit $xh \in xH$; alors (4) implique $xhx^{-1} \in H$, donc il existe $h' \in H$ tel que $xhx^{-1} = h'$, c'est-à-dire $xh = h'x$; par suite $xH \subseteq Hx$. On prouverait de même que $Hx \subseteq xH$, d'où (4) \Rightarrow (1).

Remarques (4.11) :

1° Si H et K sont deux sous-groupes d'un groupe G , tels que $H \subseteq K$, alors l'une quelconque des cinq propriétés du théorème (4.10) caractérisant un sous-groupe normal permet de vérifier que : $H \triangleleft G \Rightarrow H < K$.

Par contre

$$H \triangleleft K \Rightarrow H < G;$$

$$H \triangleleft G \Rightarrow K < G \quad \text{et} \quad (H < K, K \triangleleft G) \Rightarrow H \triangleleft G$$

(voir exercice 9, chap. IV).

2° Le théorème (4.10) exprime que *H est un sous-groupe normal de G si et seulement si H est stable par tout automorphisme intérieur de G .*

Exemples (4.12) :

1° Pour tout groupe G , on a $\text{Int}(G) < \text{Aut}(G)$; $\text{Int}(G)$ est le groupe des automorphismes intérieurs de G , c'est-à-dire de la forme : $\sigma_g : G \rightarrow G$ et on vérifie facilement que, quel que soit

$$x \mapsto gxg^{-1}$$

$\alpha \in \text{Aut}(G)$,

$$\alpha \circ \sigma_g \circ \alpha^{-1} = \sigma_{\alpha(g)}.$$

2° Considérons dans le groupe symétrique S_3 engendré par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{et} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

(exemples (1.41) et (2.4)), le sous-groupe $N = \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$.

On a $S_3 = \{e, \tau, \sigma, \sigma^2, \sigma \circ \tau, \tau \circ \sigma\}$ et $\sigma^2 \circ \tau = \tau \circ \sigma$, $\tau \circ \sigma^2 = \sigma \circ \tau$; par suite, les classes à droite et à gauche modulo N sont :

$$\begin{cases} N = \{e, \sigma, \sigma^2\} \\ N_\tau = \{\tau, \sigma \circ \tau, \tau \circ \sigma\} \end{cases} \quad \begin{cases} N = \{e, \sigma, \sigma^2\} \\ {}_\tau N = \{\tau, \tau \circ \sigma, \sigma \circ \tau\}; \end{cases}$$

pour tout $\alpha \in S_3$, on a $N\alpha = \alpha N$, d'où $N \triangleleft S_3$.

3° Soit G un groupe quelconque et $Z(G)$ son centre :

$$Z(G) = \{a \in G; ax = xa, \forall x \in G\}.$$

$Z(G)$ est un sous-groupe de G et quels que soient $x \in G$ et $a \in Z(G)$, $xax^{-1} \in Z(G)$, donc $Z(G) \triangleleft G$.

On vérifie que, plus généralement :

$$(H \leq G \text{ et } H \subseteq Z(G)) \Rightarrow H \triangleleft G.$$

PROPOSITION (4.13). Pour un groupe G de centre $Z(G)$, on a :

$$\frac{G}{Z(G)} \text{ monogène} \Rightarrow G \text{ abélien.}$$

Preuve : Soit π la surjection canonique $G \rightarrow \frac{G}{Z(G)}$.

$\frac{G}{Z(G)}$ étant monogène, il existe $a \in G$ tel que $\pi(a)$ engendre $\frac{G}{Z(G)}$.

Pour tout $x \in G$, posons $\bar{x} = \pi(x)$. Soient x et y quelconques dans G :

$$\frac{G}{Z(G)} = \langle \bar{a} \rangle \Rightarrow (\exists (m, n) \in \mathbf{Z} \times \mathbf{Z}, \bar{x} = \bar{a}^m, \bar{y} = \bar{a}^n);$$

par suite, il existe z_1 et z_2 dans $Z(G)$ tels que :

$$x = a^m z_1 \quad \text{et} \quad y = a^n z_2;$$

on en déduit que $xy = a^{m+n} z_1 z_2 = yx$, donc G est abélien.

On note que, si G est un groupe abélien, $Z(G) = G$ implique évidemment $\frac{G}{Z(G)}$ monogène.

PROPOSITION (4.14). Soient G un groupe et H un sous-groupe de G , alors :

$$[G : H] = 2 \Rightarrow H \triangleleft G.$$

Preuve : $[G : H] = 2 \Rightarrow H \neq G$.

$$[G : H] = 2 \Leftrightarrow \begin{cases} \forall x \in G \setminus H, & G = H \cup Hx = H \cup xH \\ H \cap Hx = \emptyset, & H \cap xH = \emptyset. \end{cases}$$

$$[G : H] = 2 \Leftrightarrow Hx = G \setminus H = xH,$$

$$\text{d'où } [G : H] = 2 \Rightarrow H \triangleleft G.$$

Exemples (4.15) :

1° Pour tout entier $n \geq 2$, on sait que $[S_n : A_n] = 2$, on retrouve ainsi la propriété : $A_n \triangleleft S_n$ (exemple (4.7) 1°).

2° Dans le groupe diédral D_n d'ordre $2n$, le sous-groupe cyclique d'ordre n , Γ_n , est d'indice 2, d'où $\Gamma_n \triangleleft D_n$.

3° $\mathcal{I}(2)$ et $\mathcal{D}(2)$ désignant respectivement le groupe des isométries et le groupe des déplacements du plan affine euclidien, d'après l'exercice 7, chapitre II, on a $[\mathcal{I}(2) : \mathcal{D}(2)] = 2$, d'où $\mathcal{D}(2) \triangleleft \mathcal{I}(2)$.

4° Soit $O(E)$ le groupe orthogonal d'un espace vectoriel euclidien E , de dimension finie (exemple (1.64)). On démontre en algèbre linéaire [51] que $u \in O(E) \Leftrightarrow (\det u)^2 = 1$. Si $O^+(E)$ désigne le groupe des rotations de E , c'est-à-dire le noyau du morphisme de groupes :

$$\begin{aligned} O(E) &\rightarrow \{-1, 1\}, \\ u &\mapsto \det u \end{aligned}$$

on a $[O(E) : O^+(E)] = 2$, d'où $O^+(E) \triangleleft O(E)$.

PROPOSITION (4.16). Soient G un groupe et $\{H_i\}_{i \in I}$ une famille de sous-groupes de G , alors :

$$(H_i \triangleleft G, \forall i \in I) \Rightarrow \bigcap_{i \in I} H_i \triangleleft G.$$

Preuve : Soient $h \in \bigcap_{i \in I} H_i$ et $x \in G$; on a $h \in H_i$, quel que soit $i \in I$, par suite : $(H_i \triangleleft G, \forall i \in I) \Rightarrow xhx^{-1} \in H_i, \forall i \in I$, d'où la propriété énoncée.

PROPOSITION (4.17). Soient deux groupes G et G' et $f \in \text{Hom}(G, G')$, alors :

- a) $H \triangleleft G \Rightarrow f(H) \triangleleft f(G)$; si f est surjectif, alors $f(H)$ est normal dans G' .
 b) $H' \triangleleft G' \Rightarrow f^{-1}(H') \triangleleft G$.

Preuve :

a) Soit $y \in f(H)$ et $z \in f(G)$; il existe $h \in H$ et $x \in G$ tels que $y = f(h)$, $z = f(x)$, alors :

$$zyz^{-1} = f(x) f(h) (f(x))^{-1} = f(x) f(h) f(x^{-1}),$$

donc $zyz^{-1} = f(xhx^{-1})$.

$H \triangleleft G$ implique $xhx^{-1} \in H$, par suite, $zyz^{-1} \in f(H)$, d'où $f(H) \triangleleft f(G)$.

b) Soit

$$h \in f^{-1}(H') \quad \text{et} \quad x \in G;$$

$$f(h) \in H' \quad \text{et} \quad f(xhx^{-1}) = f(x) f(h) f(x)^{-1};$$

alors $H' \triangleleft G' \Rightarrow f(xhx^{-1}) \in H'$,

d'où $xhx^{-1} \in f^{-1}(H')$ et, par suite, $f^{-1}(H') \triangleleft G$.

PROPOSITION (4.18). Soient H et K deux sous-groupes d'un groupe G ; alors :

- a) $H \triangleleft G \Rightarrow H \cap K \triangleleft K$.
 b) $H \triangleleft G \Rightarrow HK$ sous-groupe de G et $H \triangleleft HK$.

Preuve :

a) Soit $h \in H \cap K$; l'hypothèse $H \triangleleft G$ implique

$$khk^{-1} \in H \cap K,$$

quel que soit $k \in K$, d'où $H \cap K \triangleleft K$.

b) Montrons que $H \triangleleft G$ implique $HK = KH$, ce qui prouvera que HK est un sous-groupe de G (proposition (1.47)).

Soit $h \in H$ et $k \in K$.

$$H \triangleleft G \Rightarrow k^{-1} h k \in H,$$

donc il existe $h' \in H$ tel que $k^{-1} h k = h'$, c'est-à-dire $h k = h' k$, d'où $HK \subseteq KH$.

On vérifie de même l'inclusion $KH \subseteq HK$; ainsi, HK étant un sous-groupe de G :

$$(H \leq HK \text{ et } H \triangleleft G) \Rightarrow H \triangleleft HK.$$

B / Classes de conjugaison. Normalisateur

Etant donné un groupe G , on note $\mathcal{P}(G)$ l'ensemble de ses parties.

Définitions (4.19) : Soient G un groupe et $S \neq \emptyset$ dans $\mathcal{P}(G)$. On dit que $S' \in \mathcal{P}(G)$ est *conjugée de S* , s'il existe $x \in G$ tel que $S' = xSx^{-1}$, où $xSx^{-1} = \{xsx^{-1}; s \in S\}$. On vérifie facilement que la relation de conjugaison est une relation d'équivalence dans $\mathcal{P}(G)$, en convenant de considérer la partie vide comme conjugée d'elle-même.

Etant donné $S \neq \emptyset$ dans $\mathcal{P}(G)$, la classe d'équivalence de S , modulo la relation de conjugaison, est l'ensemble $\{xSx^{-1}; x \in G\}$, appelé *classe de conjugaison de S* .

Remarques (4.20) :

1° Si S et S' sont conjuguées, non vides, dans $\mathcal{P}(G)$ et telles que $S' = xSx^{-1}$, alors S' est l'image de S par l'automorphisme intérieur σ_x ; par suite, S et S' sont des ensembles équipotents; en particulier, si S est fini, tout S' conjugué de S est fini et $|S'| = |S|$.

2° Si $S = \{g\}$ où $g \in G$, la classe de conjugaison de S est dite *classe de conjugaison de g* ; elle est formée par l'ensemble des xgx^{-1} , x décrivant G .

Tout $xgx^{-1} = \sigma_x(g)$ est dit *conjugué de g dans G* , et la relation de conjugaison dans G est une relation d'équivalence.

3° Si H est un sous-groupe de G , tout conjugué de H étant de la forme $H' = xHx^{-1} = \sigma_x(H)$ est un sous-groupe de G , isomorphe à H .

Définition (4.21) : Etant donné une partie non vide S d'un groupe G , on appelle *normalisateur de S dans G* l'ensemble

$$N_G(S) = \{x \in G; xSx^{-1} = S\} \quad (6)$$

On vérifie sans peine que, quel que soit $S \neq \emptyset$ dans $\mathcal{P}(G)$, $N_G(S)$ est un sous-groupe de G .

Si $S = \{g\}$, où $g \in G$,

$$N_G(g) = \{x \in G; xgx^{-1} = g\} = \{x \in G; xg = gx\};$$

c'est-à-dire que $N_G(g)$ coïncide avec le centralisateur de g dans G , noté $C_G(g)$ (exercice 17, chap. I).

Pour $S \in \mathcal{P}(G)$, tel que $|S| > 1$, le centralisateur de S dans G :

$$C_G(S) = \{x \in G; xsx^{-1} = s, \forall s \in S\}$$

est, en général, un sous-groupe propre de $N_G(S)$ et on vérifie que $C_G(S) \triangleleft N_G(S)$. La notion de normalisateur fournit une nouvelle caractérisation des sous-groupes normaux :

THÉORÈME (4.22). Soit H un sous-groupe d'un groupe G , alors :

$$H \triangleleft G \Leftrightarrow N_G(H) = G.$$

Ce résultat se déduit immédiatement de la définition de $N_G(H)$ et de la condition (2) du théorème (4.10).

PROPOSITION (4.23). Soit G un groupe :

- a) Pour tout sous-groupe H de G , on a $H \triangleleft N_G(H)$.
 b) Si H et K sont deux sous-groupes de G tels que $H \leq K$, alors :

$$H < K \Rightarrow K \leq N_G(H)$$

- c) $K \leq N_G(H) \Rightarrow HK \leq G$ et $H < HK$.

Preuve :

a) On remarque que la définition de $N_G(H)$ implique $H \subseteq N_G(H)$; d'autre part :

$$x \in N_G(H) \Leftrightarrow xHx^{-1} = H,$$

d'où $H \triangleleft N_G(H)$.

b) Si l'on a $H \leq K \leq G$, alors :

$$H \triangleleft K \Rightarrow kHk^{-1} = H, \quad \forall k \in K,$$

d'où $K \leq N_G(H)$.

c) Soit K un sous-groupe de $N_G(H)$; considérons $h \in H$ et $k \in K$; on a $k \in N_G(H)$, donc $k^{-1} \in N_G(H)$, par suite $k^{-1}Hk = H$; on en déduit qu'il existe $h' \in H$ tel que $k^{-1}hk = h'$, d'où $hk = kh'$, ce qui implique $HK \subseteq KH$.

De façon analogue on montre que $KH \subseteq HK$, donc HK est un sous-groupe de G .

$$H \subseteq N_G(H) \quad \text{et} \quad K \subseteq N_G(H) \quad \text{implique} \quad HK \subseteq N_G(H);$$

or d'après a) H est normal dans $N_G(H)$, par suite H , qui est un sous-groupe de HK , est normal dans HK .

Remarque (4.24) : D'après le b) de la proposition (4.23), pour tout sous-groupe H de G , $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal.

4 — Etude des groupes quotients

A / Propriété universelle du groupe quotient

THÉORÈME (4.25). Soient G un groupe et H un sous-groupe normal de G ; soit π l'épimorphisme canonique $G \rightarrow \frac{G}{H}$; alors, quels que soient le groupe G' et le morphisme $f \in \text{Hom}(G, G')$ tel que $H \subseteq \text{Ker } f$, il existe un unique morphisme $\varphi \in \text{Hom}\left(\frac{G}{H}, G'\right)$ tel que $\varphi \circ \pi = f$.

Preuve : Considérons le diagramme :

$$\begin{array}{ccc} G & \xrightarrow{\pi} & \frac{G}{H} \\ f \downarrow & \searrow \varphi & \\ G' & & \end{array} \quad (7)$$

$$\text{où } \varphi \text{ est la correspondance } G \rightarrow \frac{G}{H} \quad (8)$$

$$\bar{x} \mapsto f(x)$$

a) Vérifions que, grâce à la condition $H \subseteq \text{Ker } f$, φ est une application, c'est-à-dire que $\bar{x} = \bar{x}'$ implique $f(x) = f(x')$.

$$\bar{x} = \bar{x}' \quad \text{dans } \frac{G}{H} \quad \Leftrightarrow \quad xx'^{-1} \in H$$

$$\text{et} \quad H \subseteq \text{Ker } f \Rightarrow f(xx'^{-1}) = e',$$

e' étant l'élément unité de G' ;

$$\text{or} \quad f(xx'^{-1}) = f(x) (f(x'))^{-1} = e', \quad \text{donc } f(x) = f(x').$$

b) φ est un *morphisme* de groupes, car :

$$\varphi(\bar{x}\bar{y}) = \varphi(\overline{xy}) = f(xy)$$

$$\text{et} \quad f(xy) = f(x)f(y), \quad \text{puisque } f \text{ est un morphisme,}$$

$$\text{d'où} \quad \varphi(\bar{x}\bar{y}) = \varphi(\bar{x})\varphi(\bar{y}).$$

c) $\pi(x) = \bar{x}$, pour tout $x \in G$, implique $\varphi \circ \pi = f$, c'est-à-dire que le *diagramme* (7) *commute*.

d) Il reste à prouver l'*unicité* du morphisme φ ; supposons qu'il existe $\varphi' \in \text{Hom}\left(\frac{G}{H}, G'\right)$ tel que $\varphi' \circ \pi = f$; alors, pour tout $\bar{x} \in \frac{G}{H}$, on a :

$$\varphi'(\bar{x}) = \varphi' \circ \pi(x) = f(x),$$

$$\text{donc} \quad \varphi'(\bar{x}) = \varphi(\bar{x}) \quad \text{et par suite } \varphi' = \varphi.$$

COROLLAIRE (4.26). *Les hypothèses étant celles du théorème (4.23), dans le diagramme (7) on a :*

a) f *surjectif* $\Rightarrow \varphi$ *surjectif*;

b) $H = \text{Ker } f \Rightarrow \varphi$ *injectif*;

d'où c) f *surjectif* et $H = \text{Ker } f \Rightarrow \varphi$ *est un isomorphisme*.

Preuve :

a) Si f est surjectif, pour tout $y \in G'$, il existe $x \in G$ tel que $y = f(x)$; mais $\varphi(\bar{x}) = f(x)$, par suite, quel que soit $y \in G'$, il existe $\bar{x} \in \frac{G}{H}$ tel que $y = \varphi(\bar{x})$, donc φ est surjectif.

b) Supposons $H = \text{Ker } f$ et $\varphi(\bar{x}) = e'$; on a alors $f(x) = e'$, donc $x \in \text{Ker } f$, c'est-à-dire $x \in H$, par suite $\bar{x} = \bar{e}$, donc φ est injectif.

Remarques (4.27) :

1° On notera que la « propriété universelle » du groupe quotient énoncée dans le théorème (4.25) est une propriété du couple $\left(\frac{G}{H}, \pi\right)$.

2° En application du corollaire (4.26) on retrouve le 1^{er} théorème d'isomorphisme démontré au chapitre II (théorème (2.27)).

En effet, si $f \in \text{Hom}(G, G')$ et si f_1 désigne la restriction surjective de f , c'est-à-dire le morphisme : $f_1 : G \rightarrow \text{Im } f$, alors,

$x \mapsto f(x)$
d'après le théorème (4.25), il existe un unique morphisme $\varphi \in \text{Hom}\left(\frac{G}{\text{Ker } f}, \text{Im } f\right)$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \frac{G}{\text{Ker } f} \\ f_1 \downarrow & \swarrow \exists! \varphi & \\ \text{Im } f & & \end{array} \quad (9)$$

On a donc $\varphi \circ \pi = f_1$, d'où $\varphi(\bar{x}) = f(x)$ pour tout $x \in G$ et φ est un isomorphisme de $\frac{G}{\text{Ker } f}$ sur $\text{Im } f$, puisque f_1 est surjectif et $\text{Ker } f_1 = \text{Ker } f$.

3° $H \triangleleft G$ implique $\frac{G}{H}$ image homomorphe de G , car $\frac{G}{H} = \text{Im } \pi$ dans le diagramme (7). D'autre part, d'après le premier théorème d'isomorphisme, toute image homomorphe d'un groupe G est isomorphe à un groupe quotient de G .

On en conclut qu'à un isomorphisme près les seuls groupes images homomorphes d'un groupe donné G sont les groupes quotients de G .

A un isomorphisme près, un groupe simple n'a donc pas d'autre image homomorphe que (e) et lui-même.

B / Sous-groupes d'un groupe quotient

THÉORÈME (4.28). Soit G un groupe et $H < G$; soit π l'épimorphisme canonique $G \rightarrow \frac{G}{H}$.

a) Tout sous-groupe \bar{K} de $\frac{G}{H}$ est l'image par π d'un unique sous-groupe K de G contenant H ; plus précisément :

$$\bar{K} = \pi(K) \quad \text{où } K = \pi^{-1}(\bar{K}); \quad \text{de plus } \pi(K) = \frac{K}{H}.$$

b) Si K_1 est un sous-groupe de G tel que $H \not\subseteq K_1$, alors HK_1 est un sous-groupe de G contenant H et

$$\pi(K_1) = \frac{HK_1}{H} \tag{10}$$

Preuve :

a) Soit \bar{K} un sous-groupe de $\frac{G}{H}$; π étant un morphisme de groupes, $\pi^{-1}(\bar{K})$ est un sous-groupe de G .

Posons $K = \pi^{-1}(\bar{K})$ et $\bar{e} = \pi(e)$; $\bar{e} \in \bar{K} \Rightarrow \pi^{-1}(\bar{e}) \subseteq K$,

or $\pi^{-1}(\bar{e}) = H$, d'où $H \subseteq K$.

π étant surjectif, $K = \pi^{-1}(\bar{K})$ implique $\bar{K} = \pi(K)$.

D'autre part, $H \triangleleft G$ implique $H \triangleleft K$; on en déduit que $\pi(K) = \frac{K}{H}$.

Démontrons l'unicité du sous-groupe K de G contenant H , tel que $\bar{K} = \pi(K)$.

Supposons qu'il existe $K' \leq G$ tel que $H \subseteq K'$ et $\pi(K') = \bar{K}$; si $K = \pi^{-1}(\bar{K})$, alors, $\bar{K} = \pi(K) = \pi(K')$.

Quel que soit $k' \in K'$, il existe $k \in K$ tel que

$$\pi(k') = \pi(k), \quad \text{donc } k' \in Hk;$$

alors $H \subseteq K \Rightarrow k' \in K$,

d'où $K' \subseteq K$. On vérifie de même l'inclusion $K \subseteq K'$, par suite $K' = K$.

b) Soit $K_1 < G$ tel que $H \not\subseteq K_1$. D'après la proposition (4.18), $H \triangleleft G$ implique HK_1 sous-groupe de G et $H \triangleleft HK_1$, donc $\pi(HK_1) = \frac{HK_1}{H}$.

D'autre part, π étant un morphisme de groupes, $\pi(K_1)$ est un sous-groupe de $\frac{G}{H}$.

$$\pi(x) \in \pi(K_1) \Leftrightarrow \exists k_1 \in K_1, \quad Hx = Hk_1$$

$$\text{d'où } \pi(x) \in \pi(K_1) \Leftrightarrow \pi(x) \in \pi(HK_1),$$

c'est-à-dire que

$$\pi(K_1) = \frac{HK_1}{H}.$$

Remarques (4.29) :

1° Le a) du théorème (4.28) exprime que la correspondance $\bar{K} \mapsto \pi^{-1}(\bar{K})$ est une bijection de l'ensemble des sous-groupes de $\frac{G}{H}$ sur l'ensemble des sous-groupes de G contenant H .

2° Dans le b) du théorème (4.28), HK_1 est le sous-groupe de G engendré par $H \cup K_1$; si le groupe G est additif, (10) s'écrit :

$$\pi(K_1) = \frac{H + K_1}{H} \quad (10')$$

Exemple (4.30) : D'après ce qui précède, pour $n > 1$ dans \mathbf{N} , tout sous-groupe de $\frac{\mathbf{Z}}{n\mathbf{Z}}$ s'écrit $\frac{k\mathbf{Z}}{n\mathbf{Z}}$ avec $n\mathbf{Z} \subseteq k\mathbf{Z}$; or :

$$n\mathbf{Z} \subseteq k\mathbf{Z} \Leftrightarrow k \text{ divise } n \text{ dans } \mathbf{N}^*.$$

On retrouve ainsi le corollaire (3.12), c'est-à-dire que le nombre des sous-groupes de $\frac{Z}{nZ}$ est égal au nombre des diviseurs de n dans N^* .

PROPOSITION (4.31). Soit G un groupe et $H \triangleleft G$.

a) Si K et K' sont deux-sous groupes de G contenant H , alors :

$$H \leq K \leq K' \Rightarrow \frac{K}{H} \leq \frac{K'}{H} \quad (11)$$

$$b) \quad (H \leq K \text{ et } K \triangleleft G) \Leftrightarrow \frac{K}{H} \triangleleft \frac{G}{H} \quad (12)$$

Preuve : Soit π la surjection canonique $G \rightarrow \frac{G}{H}$.

$$a) \quad H \leq K \leq K' \Rightarrow \pi(K) \leq \pi(K'); \text{ c'est-à-dire } \frac{K}{H} \leq \frac{K'}{H}.$$

b) On suppose $H \leq K$ et $K \triangleleft G$; soit $\pi(k) \in \frac{K}{H}$ et $\pi(x) \in \frac{G}{H}$; alors $\pi(x) \pi(k) (\pi(x))^{-1} = \pi(x k x^{-1})$

$$K \triangleleft G \Leftrightarrow \forall (k, x) \in K \times G, \quad x k x^{-1} \in K,$$

$$\text{alors} \quad (H \leq K \text{ et } K \triangleleft G) \Leftrightarrow \forall (\pi(k), \pi(x)) \in \frac{K}{H} \times \frac{G}{H}, \\ \pi(x) \pi(k) (\pi(x))^{-1} \in \pi(K).$$

On en déduit que :

$$(H \leq K \text{ et } K \triangleleft G) \Leftrightarrow \frac{K}{H} \triangleleft \frac{G}{H}.$$

C / 2° et 3° théorèmes d'isomorphisme

LEMME (4.32). Soient deux groupes G et G' . Etant donné $H \triangleleft G$, $H' \triangleleft G'$ et $f \in \text{Hom}(G, G')$ tel que $f(H) \subseteq H'$, il existe un unique morphisme $\bar{f} \in \text{Hom}\left(\frac{G}{H}, \frac{G'}{H'}\right)$ tel que $\bar{f} \circ \pi = \pi' \circ f$, où π et π' sont les épimorphismes canoniques $G \rightarrow \frac{G}{H}$ et $G' \rightarrow \frac{G'}{H'}$.

Preuve : $f(H) \subseteq H' \Leftrightarrow H \subseteq f^{-1}(H')$. e' étant l'élément unité de G' , on a :

$$\text{Ker}(\pi' \circ f) = \{x \in G; \pi' \circ f(x) = \pi'(e')\}$$

$$\text{Ker}(\pi' \circ f) = \{x \in G; f(x) \in H'\},$$

d'où $\text{Ker}(\pi' \circ f) = f^{-1}(H')$.

Alors la condition $H \subseteq \text{Ker}(\pi' \circ f)$ implique, d'après le théorème (4.25), l'existence d'un unique morphisme $\bar{f} \in \text{Hom}\left(\frac{G}{\bar{H}}, \frac{G'}{\bar{H}'}\right)$ tel que $\bar{f} \circ \pi = \pi' \circ f$, d'où le diagramme commutatif :

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \downarrow & & \downarrow \pi' \\ G & \xrightarrow{\exists! \bar{f}} & G' \\ \bar{H} & & \bar{H}' \end{array} \quad (13)$$

Remarque (4.33) : Compte tenu du corollaire (4.31), dans le lemme ci-dessus on a :

1° $\pi' \circ f$ surjectif implique \bar{f} surjectif; on notera que $\pi' \circ f$ peut être surjectif, sans que f le soit (voir la preuve du théorème (4.34)).

2° $\text{Ker}(\pi' \circ f) = H$, qui équivaut à $f^{-1}(H') = H$, implique \bar{f} injectif.

THÉORÈME (4.34). (*2^e théorème d'isomorphisme.*)

Soit un groupe G et $H \triangleleft G$; alors, pour tout sous-groupe K de G , les groupes quotients $\frac{K}{H \cap K}$ et $\frac{HK}{H}$ existent et l'on a :

$$\frac{K}{H \cap K} \simeq \frac{HK}{H} \quad (14)$$

Preuve : D'après la proposition (4.17), l'hypothèse $H \triangleleft G$ implique, d'une part, $H \cap K \triangleleft K$ et, d'autre part, HK sous-groupe de G et $H \triangleleft HK$; d'où l'existence des groupes quotients $\frac{K}{H \cap K}$ et $\frac{HK}{H}$.

Désignons par j l'injection canonique : $K \rightarrow HK$.

Soient π et π' les épimorphismes canoniques associés aux groupes quotients $\frac{K}{H \cap K}$ et $\frac{HK}{K}$.

$$j(H \cap K) = H \cap K \Rightarrow j(H \cap K) \subseteq H.$$

Le lemme (4.32) implique alors l'existence d'un unique morphisme $\varphi \in \text{Hom}\left(\frac{K}{H \cap K}, \frac{HK}{K}\right)$ tel que $\varphi \circ \pi = \pi' \circ j$.

$$\begin{array}{ccc} K & \xrightarrow{j} & HK \\ \pi \downarrow & & \downarrow \pi' \\ \frac{K}{H \cap K} & \xrightarrow{\exists! \varphi} & \frac{HK}{K} \end{array}$$

$\pi' \circ j$ est surjectif; en effet, $\pi' \circ j(K) = \pi'(K) = \frac{HK}{K}$; par suite, φ est surjectif (remarque (4.33)).

D'autre part, $j^{-1}(H) = H \cap K$, puisque $j(x) = x$ pour tout $x \in K$. On en déduit que φ est injectif (remarque (4.33)). En conclusion, φ est un isomorphisme.

Remarque (4.35) : Si le groupe G est additif, la relation (14) s'écrit :

$$\frac{K}{H \cap K} \simeq \frac{H + K}{H} \quad (14')$$

et, dans le cas particulier où la somme des sous-groupes H et K est directe, on obtient :

$$\frac{H \oplus K}{H} \simeq K$$

puisque $H \cap K = (0)$.

THÉORÈME (4.36). (*3^e théorème d'isomorphisme.*)

Soient H et K deux sous-groupes d'un groupe G , tels que $H \subseteq K$, $H \triangleleft G$ et $K \triangleleft G$, alors on a :

$$\frac{G}{K} \simeq \frac{\frac{G}{H}}{\frac{K}{H}} \quad (15)$$

Preuve : Notons, respectivement, σ , π et π' les épimorphismes canoniques associés aux groupes quotients $\frac{G}{H}$, $\frac{G}{K}$, $\frac{\frac{G}{H}}{\frac{K}{H}}$.

$H \subseteq K \Rightarrow \sigma(K) = \frac{K}{H}$, sous-groupe de $\frac{G}{H}$.

D'après le lemme (4.32), il existe un unique morphisme

$$\bar{\sigma} \in \text{Hom} \left(\frac{G}{K}, \frac{\frac{G}{H}}{\frac{K}{H}} \right) \text{ tel que } \bar{\sigma} \circ \pi = \pi' \circ \sigma :$$

$$\begin{array}{ccc} G & \xrightarrow{\sigma} & \frac{G}{H} \\ \pi \downarrow & & \downarrow \pi' \\ \frac{G}{K} & \xrightarrow{\exists! \bar{\sigma}} & \frac{\frac{G}{H}}{\frac{K}{H}} \end{array}$$

π' et σ surjectifs implique $\pi' \circ \sigma$ surjectif, donc $\bar{\sigma}$ surjectif. $\text{Ker}(\pi' \circ \sigma) = K$, donc $\bar{\sigma}$ est injectif. On en conclut que $\bar{\sigma}$ est un isomorphisme.

5 — Groupe dérivé. Sous-groupe caractéristique

A / Groupe dérivé d'un groupe

Définition (4.36) : Soit G un groupe; à tout couple (x, y) d'éléments de G , on associe l'élément $x^{-1}y^{-1}xy$ noté $[x, y]$.

$[x, y]$ s'appelle le *commutateur* de x et y dans G .

Remarques (4.37) :

1° G abélien $\Leftrightarrow [x, y] = e, \forall (x, y) \in G \times G$.

2° ($H \triangleleft G$ et x ou y dans H) $\Rightarrow [x, y] \in H$.

Définition (4.38) : Etant donné un groupe G , on appelle *groupe dérivé* de G le sous-groupe de G engendré par l'ensemble des commutateurs de G ; on le note $D(G)$.

D'après la remarque (4.37), on a :

G groupe abélien $\Leftrightarrow D(G) = (e)$.

THÉORÈME (4.39). Soit G un groupe; on a :

a) $D(G) \triangleleft G$;

b) si $N \triangleleft G$, alors $\frac{G}{N}$ est un groupe abélien si et seulement si $D(G) \subseteq N$;
en particulier $\frac{G}{D(G)}$ est abélien.

Preuve :

a) Quels que soient x, y, z dans G ,

d'une part :

$$z^{-1}[x, y]z = z^{-1}x^{-1}y^{-1}xyz,$$

d'autre part :

$$\begin{aligned} [z^{-1}xz, z^{-1}yz] &= z^{-1}x^{-1}zz^{-1}y^{-1}zz^{-1}xzz^{-1}yz \\ &= z^{-1}x^{-1}y^{-1}xyz, \end{aligned}$$

d'où $z^{-1}[x, y]z = [z^{-1}xz, z^{-1}yz]$.

On en déduit que $D(G)$ est normal dans G .

$$b) \frac{G}{N} \text{ abélien} \Leftrightarrow \bar{x}\bar{y} = \bar{y}\bar{x}, \forall \bar{x}, \bar{y} \text{ dans } \frac{G}{N}.$$

$$\bar{x}\bar{y} = \bar{y}\bar{x} \Leftrightarrow (yx)^{-1}xy \in N$$

$$\bar{x}\bar{y} = \bar{y}\bar{x} \Leftrightarrow [x, y] \in N,$$

$$\text{d'où } \frac{G}{N} \text{ abélien} \Leftrightarrow D(G) \subseteq N.$$

Groupes dérivés successifs : Etant donné un groupe G , on note $D_2(G)$ le groupe dérivé de $D(G)$ et, d'une façon générale, on pose :

$$D_{i+1}(G) = D(D_i(G)), \quad \forall i \in \mathbb{N},$$

avec $D_0(G) = G$ et $D_1(G) = D(G)$.

$D_i(G)$ s'appelle le i -ème groupe dérivé de G .

D'après le théorème (4.39), on a, pour tout $i \in \mathbb{N}$:

$$D_{i+1}(G) \triangleleft D_i(G) \quad \text{et} \quad \frac{D_i(G)}{D_{i+1}(G)} \text{ abélien.}$$

B / Sous-groupe caractéristique

Définition (4.40) : Un sous-groupe H d'un groupe G est dit *caractéristique* dans G si, pour tout $\alpha \in \text{Aut}(G)$, on a $\alpha(H) = H$.

Notation (4.41) : On écrira $H \sqsubset G$ pour exprimer que H est caractéristique dans G .

Remarques (4.42) :

1° Dans tout groupe G , (e) et G sont des sous-groupes caractéristiques.

2° Dans un groupe G : $H \sqsubset G \Rightarrow H \triangleleft G$.

En effet, si H est invariant par tout $\alpha \in \text{Aut}(G)$, il est en particulier invariant pour tout automorphisme intérieur de G , d'où $H \triangleleft G$ (remarque (4.11) 2°).

PROPOSITION (4.43). Dans tout groupe G , $D(G)$ et $Z(G)$ (le centre de G) sont des sous-groupes caractéristiques.

Preuve : Soit $\alpha \in \text{Aut}(G)$; quels que soient x et y dans G ,

$$\alpha([x, y]) = \alpha(x^{-1}y^{-1}xy)$$

$$\alpha([x, y]) = (\alpha(x))^{-1}(\alpha(y))^{-1}\alpha(x)\alpha(y)$$

$$\alpha([x, y]) = [\alpha(x), \alpha(y)].$$

On en déduit l'inclusion $\alpha(D(G)) \subseteq D(G)$.

Mais $\alpha \in \text{Aut}(G)$ implique $\alpha^{-1} \in \text{Aut}(G)$; le raisonnement précédent appliqué à α^{-1} donne :

$$\alpha^{-1}(D(G)) \subseteq D(G), \quad \text{d'où } D(G) \subseteq \alpha(D(G))$$

et, par suite,

$$\alpha(D(G)) = D(G).$$

Pour tout $a \in Z(G)$ et tout $x \in G$, on a $xa = ax$, d'où $\alpha(x)\alpha(a) = \alpha(a)\alpha(x)$, quel que soit $\alpha \in \text{Aut}(G)$; or, quel que soit $y \in G$, il existe $x \in G$ tel que $y = \alpha(x)$, on en déduit que $y\alpha(a) = \alpha(a)y$, pour tout $y \in G$; par suite, on a $\alpha(Z(G)) \subseteq Z(G)$. Comme dans le cas de $D(G)$, on montre alors que $\alpha(Z(G)) = Z(G)$.

PROPOSITION (4.44). *Soit G un groupe, alors :*

$$a) (H \sqsubset G \text{ et } K \sqsubset H) \Rightarrow K \sqsubset G;$$

$$b) (H \triangleleft G \text{ et } K \sqsubset H) \Rightarrow K \triangleleft G.$$

Preuve :

a) Supposons $H \sqsubset G$ et $K \sqsubset H$; soit $\alpha \in \text{Aut}(G)$.

On a $\alpha(H) = H$, donc la restriction $\alpha|_H$ de α à H est un automorphisme de H , par suite $\alpha|_H(K) = K = \alpha(K)$, d'où $K \sqsubset G$.

b) Soit $H \triangleleft G$ et $K \sqsubset H$; soit $\sigma \in \text{Int}(G)$, alors $\sigma|_H \in \text{Aut}(H)$, par suite $\sigma|_H(K) = K$; on en déduit que $xKx^{-1} = K$, pour tout $x \in G$, d'où $K \triangleleft G$.

COROLLAIRE (4.45). $D_i(G)$ étant le i -ème groupe dérivé d'un groupe G , on a :

$$D_i(G) \sqsubset G, \quad \text{quel que soit } i \in \mathbb{N}.$$

Preuve : Compte tenu de la proposition (4.43), on a :

$$D_1(G) \subset G \quad \text{et} \quad D_2(G) \subset D_1(G).$$

Le *a*) de la proposition (4.44) implique alors $D_2(G) \subset G$.
Raisonnons par récurrence sur i ; supposons $D_i(G) \subset G$ pour un $i \geq 2$ dans \mathbf{N} .

Des propositions précédemment citées, on déduit :

$$D_{i+1}(G) \subset D_i(G) \quad \text{et, par suite,} \quad D_{i+1}(G) \subset G.$$

Remarque (4.46) : Les propriétés des groupes dérivées seront fondamentales dans l'étude des groupes résolubles : chapitre VII.

6 — Sous-groupe maximal.

Sous-groupe normal maximal

Définitions (4.47) : G désigne un groupe *non réduit à un seul élément*.

1° Un sous-groupe M de G est dit *maximal*, s'il est maximal dans l'ensemble des sous-groupes *propres* de G ordonné par l'inclusion.

Autrement dit, M est un *sous-groupe maximal* dans G si et seulement si M est un sous-groupe *propre* de G tel que :

$$M \leq L \leq G \Rightarrow L = M \quad \text{ou} \quad L = G.$$

2° Un sous-groupe N de G est *normal maximal*, s'il est maximal dans l'ensemble des sous-groupes *propres normaux* de G ordonné par l'inclusion.

Autrement dit, N est un *sous-groupe normal maximal* dans G si et seulement si : $N \triangleleft G$, $N \neq G$ et

$$(L \triangleleft G, N \leq L \leq G) \Rightarrow L = N \quad \text{ou} \quad L = G.$$

Exemple (4.48) : On vérifiera facilement que les sous-groupes maximaux de \mathbf{Z} sont les $p\mathbf{Z}$, où p est premier.

Remarque (4.49) : Un groupe $G \neq (e)$ n'admet pas nécessairement de sous-groupe (resp^b sous-groupe normal) maximal, puisque, d'une façon générale, un ensemble ordonné n'admet pas nécessairement un élément maximal. Cependant, *dans le cas où $G \neq (e)$ est fini, alors il existe au moins un sous-groupe maximal dans G , comme le montre la propriété suivante :*

PROPOSITION (4.50). *Si G est un groupe fini tel que $o(G) > 1$, alors tout sous-groupe propre de G est contenu dans un sous-groupe maximal de G .*

Preuve : Soit $H < G$.

— Si H est maximal, il n'y a rien à démontrer.

— Supposons H non maximal; il existe alors $H_1 < G$ tel que $H < H_1 < G$. Si H_1 est maximal, la propriété est démontrée, sinon il existe $H_2 < G$ tel que $H < H_1 < H_2 < G$. Comme précédemment, ou bien H_2 est maximal, ou bien il ne l'est pas et on réitère le raisonnement à partir de H_2 . Le groupe G étant fini, nécessairement au bout d'un nombre fini, k , d'opérations, on aboutit à un sous-groupe $H_k < G$ tel que

$$H < H_1 < H_2 < \dots < H_k < G$$

et H_k maximal.

De façon analogue on prouve que, *dans un groupe fini G , tout sous-groupe normal propre de G est contenu dans un sous-groupe normal maximal de G .*

Remarque (4.51) : La proposition (4.50) peut être démontrée dans le cas d'un groupe $G \neq (e)$ de type fini, grâce à l'axiome de Zorn ⁽¹⁾ [énoncé (4.60); remarque (4.62)].

PROPOSITION (4.52). *N est un sous-groupe normal maximal d'un groupe $G \neq (e)$, si et seulement si $\frac{G}{N}$ est simple.*

⁽¹⁾ Max Zorn (1906-).

Preuve : Soit $N < G$.

N normal maximal dans G

$$\Leftrightarrow [(N < G, N \leq L \leq G \text{ et } L < G) \Rightarrow L = N \text{ ou } L = G]$$

N normal maximal dans G

$$\Leftrightarrow \left[\frac{L}{N} < \frac{G}{N} \Rightarrow \frac{L}{N} = (\bar{e}) \text{ ou } \frac{L}{N} = \frac{G}{N} \right]$$

N normal maximal dans G

$$\Leftrightarrow \frac{G}{N} \text{ simple.}$$

Remarque (4.53) : Dans un groupe simple G , (e) est l'unique sous-groupe normal maximal.

PROPOSITION (4.54). *Soit un groupe $G \neq (e)$ et $K < G$; alors K est un sous-groupe maximal de G , si et seulement si $\frac{G}{K}$ est cyclique d'ordre premier.*

Preuve :

$$K \text{ maximal} \Leftrightarrow (K \leq L \leq G \Rightarrow L = K \text{ ou } L = G)$$

$$(K < G \text{ et } K \text{ maximal}) \Leftrightarrow \left(\frac{L}{K} \leq \frac{G}{K} \Rightarrow \frac{L}{K} = (\bar{e}) \text{ ou } \frac{L}{K} = \frac{G}{K} \right)$$

$$(K < G \text{ et } K \text{ maximal}) \Leftrightarrow \frac{G}{K} \text{ n'a pas d'autre sous-groupe que } (\bar{e}) \text{ et } \frac{G}{K}.$$

Cette dernière condition équivaut à $\frac{G}{K}$ cyclique d'ordre premier (proposition (3.16)).

Remarque (4.55) : Les propositions (4.52) et (4.54) montrent que, dans le cas d'un groupe G non abélien :

$$\left. \begin{array}{l} K \text{ sous-groupe maximal} \\ \text{dans } G \text{ et } K \triangleleft G \end{array} \right\} \Rightarrow \begin{array}{l} K \text{ sous-groupe normal} \\ \text{maximal dans } G \end{array}$$

mais la réciproque est fausse, puisqu'un groupe simple n'est pas nécessairement cyclique d'ordre premier.

Définition (4.56) : Soit un groupe $G \neq (e)$; désignons par \mathcal{M} l'ensemble (éventuellement vide) de ses sous-groupes maximaux et posons :

$$\Phi(G) = \bigcap_{M \in \mathcal{M}} M \quad \text{si } \mathcal{M} \neq \emptyset \quad \text{et} \quad \Phi(G) = G \quad \text{si } \mathcal{M} = \emptyset.$$

$\Phi(G)$ est un sous-groupe de G , appelé *sous-groupe de Frattini* ⁽²⁾ de G . Si $G = (e)$, on pose $\Phi(G) = (e)$.

Remarque (4.57) : Lorsque $\mathcal{M} \neq \emptyset$ et $G \neq (e)$, $\Phi(G)$ est un sous-groupe *propre* de G . $\Phi(G)$ jouera un rôle au chapitre VII, dans la caractérisation des groupes finis nilpotents.

PROPOSITION (4.58). *Quel que soit le groupe G , $\Phi(G)$ est un sous-groupe caractéristique de G .*

Preuve : On considère le cas $\mathcal{M} \neq \emptyset$. Soit $\alpha \in \text{Aut}(G)$;
 $\alpha(\Phi(G)) = \bigcap_{M \in \mathcal{M}} \alpha(M)$.

Montrons que, pour tout $M \in \mathcal{M}$, $\alpha(M) \in \mathcal{M}$. En effet, $\alpha(M) \leq L \leq G$ implique $M \leq \alpha^{-1}(L) \leq G$, d'où $\alpha^{-1}(L) = M$ ou $\alpha^{-1}(L) = G$, c'est-à-dire $L = \alpha(M)$ ou $L = G$.

α étant une bijection, on en déduit que $\{\alpha(M); M \in \mathcal{M}\} = \mathcal{M}$, d'où $\alpha(\Phi(G)) = \Phi(G)$, donc $\Phi(G)$ est caractéristique dans G .

Définition (4.59) : Un ensemble non vide partiellement ordonné est dit *inductif*, si tout sous-ensemble totalement ordonné de E admet un majorant dans E .

Axiome de Zorn (4.60) : Tout ensemble partiellement ordonné inductif a un élément maximal.

(2) G. Frattini (1852-1925).

PROPOSITION (4.61). *Tout groupe de type fini $G \neq (e)$ possède un sous-groupe maximal; pour un tel groupe, on a donc $\Phi(G) \neq G$.*

Preuve : Soit $G \neq (e)$ un groupe de type fini. Soit \mathcal{H} l'ensemble des sous-groupes propres de G ; $(e) \in \mathcal{H}$, donc \mathcal{H} est non vide. D'autre part, \mathcal{H} est partiellement ordonné par l'inclusion. Soit $\{H_\lambda\}_{\lambda \in \Lambda}$ une partie de \mathcal{H} totalement ordonnée par l'inclusion. D'après la proposition (1.27), $H = \bigcup_{\lambda \in \Lambda} H_\lambda$ est un sous-groupe de G .

Vérifions que H est un sous-groupe propre de G .

Supposons $H = G$; si G est engendré par $\{a_1, a_2, \dots, a_n\}$, $n \geq 1$ dans N , alors, pour tout i ($1 \leq i \leq n$), il existe $\lambda_i \in \Lambda$ tel que $a_i \in H_{\lambda_i}$. Or la famille des H_λ étant totalement ordonnée, il existe $\mu \in \Lambda$ tel que $H_{\lambda_i} \leq H_\mu$, quel que soit i ($1 \leq i \leq n$). On en déduit que $G = H_\mu$, d'où une contradiction, puisque H_μ est un sous-groupe propre de G . Par suite, $H \in \mathcal{H}$, donc \mathcal{H} est inductif. D'après l'axiome de Zorn, \mathcal{H} contient un élément maximal, autrement dit, G a un sous-groupe maximal, ce qui implique $\Phi(G) \neq G$.

Remarque (4.62) : Si $G \neq (e)$ est un groupe de type fini, la méthode de démonstration ci-dessus peut être appliquée à l'ensemble \mathcal{H} des sous-groupes propres de G contenant un sous-groupe propre donné; on prouve ainsi que, dans un groupe de type fini, tout sous-groupe propre est contenu dans un sous-groupe maximal.

Exercices Chapitre IV

- 1) Soit G un groupe, démontrer la propriété :

$$(H < G \text{ et } |H| = 2) \Rightarrow H \leq Z(G),$$

$Z(G)$ étant le centre de G .

- 2) G étant un groupe, soient $H < G$ et $\alpha \in \text{Aut}(G)$.

On pose $H' = \alpha(H)$; vérifier que l'on a $H' < G$; en déduire que les groupes $\frac{G}{H}$ et $\frac{G}{H'}$ sont isomorphes. [Utiliser le lemme (4.32).]

- 3) Soient deux groupes G_1, G_2 et $H_1 \triangleleft G_1, H_2 \triangleleft G_2$.

Prouver que l'on a $H_1 \times H_2 \triangleleft G_1 \times G_2$ et $\frac{G_1 \times G_2}{H_1 \times H_2} \simeq \frac{G_1}{H_1} \times \frac{G_2}{H_2}$.

[Utiliser le théorème (4.25)].

- 4) Soit $G = C_2 \times C_4$ (C_2 et C_4 groupes cycliques d'ordre 2 et 4).
Montrer que G a deux sous-groupes H_1 et H_2 tels que

$$H_1 \simeq H_2 \quad \text{et} \quad \frac{G}{H_1} \not\simeq \frac{G}{H_2}$$

et deux sous-groupes K_1 et K_2 tels que

$$\frac{G}{K_1} \simeq \frac{G}{K_2} \quad \text{et} \quad K_1 \not\simeq K_2.$$

- 5) Trouver des groupes *non isomorphes* G_1 et G_2 contenant respectivement des sous-groupes H_1 et H_2 tels que :

$$H_1 \triangleleft G_1, \quad H_2 \triangleleft G_2 \quad \text{et} \quad \frac{G_1}{H_1} \simeq \frac{G_2}{H_2}.$$

[Prendre, par exemple, G_1 et G_2 d'ordre 4.]

- 6) Soit K un corps commutatif; on considère l'ensemble Γ des matrices de la forme

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{où } a, b, c \text{ décrivent } K,$$

0 étant l'élément neutre du groupe $(K, +)$ et 1 l'élément unité du groupe multiplicatif $K^* = K \setminus \{0\}$.

Vérifier que Γ est un sous-groupe de $GL_3(K)$; montrer que l'on a $Z(\Gamma) \simeq K$ et $\frac{\Gamma}{Z(\Gamma)} \simeq K \times K$, où K désigne le groupe $(K, +)$.

[Pour le second isomorphisme utiliser le théorème (4.25).]

- 7) Soit un groupe G et $H \triangleleft G$. Pour tout $x \in G$, on note \bar{x} la classe de x modulo H . Soit S une partie *non vide* de G , on pose

$$\bar{S} = \{\bar{x}; x \in S\} \quad \text{et} \quad \bar{G} = \frac{G}{H}.$$

a) Vérifier que :

1) S engendre $G \Rightarrow \bar{S}$ engendre \bar{G} .

2) $(S \text{ fini et } |S| = m) \Rightarrow |\bar{S}| \leq m$.

b) Montrer que, si S est telle que \bar{S} engendre \bar{G} et si T est une partie génératrice de H , alors $S \cup T$ engendre G .

Prouver que si \bar{S} et T sont finis et tels que $|\bar{S}| = m$, $|T| = n$, alors il existe une partie génératrice S' de G telle que $S' \subseteq S \cup T$ et $|S'| \leq m + n$.

8) Vérifier que A_3 est le seul sous-groupe propre normal de S_3 , autre que e .

9) Dans le groupe symétrique S_4 , vérifier que

$$H = \{e, (1, 2) (3, 4)\}$$

$$\text{et } K = \{e, (1, 2) (3, 4), (1, 3) (2, 4), (1, 4) (2, 3)\}$$

sont des sous-groupes tels que $H \triangleleft K$ et $K < S_4$, mais que H n'est pas normal dans S_4 .

10) a) Ecrire les 12 éléments du groupe alterné A_4 et déterminer leurs ordres.

b) Démontrer que le centre $Z(A_4) = (e)$. [Montrer, en utilisant l'exercice 14, chap. III, que $Z(A_4) \neq (e)$ impliquerait l'existence d'un élément d'ordre 6 dans A_4 .]

c) Vérifier que le groupe A_4 n'a qu'un seul sous-groupe K d'ordre 4; en déduire que l'on a $K \triangleleft A_4$.

[On peut utiliser l'exercice 9 précédent.]

d) Prouver que le groupe A_4 n'a pas de sous-groupe d'ordre 6. [Supposer que A_4 a un sous-groupe K' d'ordre 6; considérer le sous-groupe $K \cap K'$, en déduire une contradiction (utiliser, en particulier, l'exercice 1 ci-dessus).]

11) a) A l'aide de la propriété universelle du groupe quotient (théorème (4.25)), démontrer les propriétés suivantes; les notations sont celles de l'exemple (1.29) et U désigne le groupe multiplicatif des nombres complexes de module 1 (U est appelé *groupe circulaire*)

$$1) \quad \frac{\mathbf{C}}{\mathbf{R}} \simeq \mathbf{R} \quad (\text{isomorphismes de groupes additifs}).$$

$$2) \quad U \simeq \left(\frac{\mathbf{R}}{\mathbf{Z}}, + \right) \quad [\text{considérer } \varphi : \mathbf{R} \rightarrow U, \varphi(a) = e^{2\pi i a}].$$

$$3) \quad \frac{\mathbf{C}^*}{\mathbf{R}_+^*} \simeq U \quad \left[\text{considérer } \varphi : \mathbf{C}^* \rightarrow U, \varphi(z) = \frac{z}{|z|} \right].$$

$$4) \quad \frac{\mathbf{C}^*}{\mathbf{U}} \simeq \mathbf{R}_+^* \simeq \frac{\mathbf{R}^*}{\mathbf{U}_2}, \quad \text{où } \mathbf{U}_2 = \{-1, 1\}.$$

$$5) \quad \frac{\mathbf{R}^*}{\mathbf{R}_+^*} \simeq \mathbf{U}_2 \simeq \frac{\mathbf{Q}^*}{\mathbf{Q}_+^*}$$

$$6) \quad \frac{\mathbf{Q}^*}{\mathbf{U}_2} \simeq \mathbf{Q}_+^*.$$

b) Vérifier que les applications :

$$\begin{aligned} \varphi : \mathbf{C}^* &\rightarrow \mathbf{R}_+^* \times \frac{\mathbf{R}}{\mathbf{Z}} & \text{et} & \quad \psi : \mathbf{C}^* \rightarrow \mathbf{R} \times \frac{\mathbf{R}}{\mathbf{Z}} \\ \rho e^{2\pi i \lambda} &\mapsto (\rho, \bar{\lambda}) & & \quad e^{x+2\pi i y} \mapsto (x, \bar{y}) \end{aligned}$$

sont des isomorphismes de groupes (pour $a \in \mathbf{R}$, $\bar{a} = \text{cl}_{\mathbf{Z}}(a)$).

c) Prouver l'existence des isomorphismes de groupes suivants :

$$\mathbf{C}^* \simeq \left(\frac{\mathbf{C}}{\mathbf{Z}}, + \right) \quad [\text{utiliser le théorème (4.25)}];$$

$$\frac{\mathbf{C}^*}{\mathbf{R}^*} \simeq \frac{\mathbf{U}}{\mathbf{U}_2} \quad [\text{utiliser le lemme (4.32)}].$$

- 12) Soit $\Gamma_\infty = \{z \in \mathbf{C}^*; \exists n \in \mathbf{N}, z^n = 1\}$ (voir exercice 12, chap. I). Vérifier que Γ_∞ est un sous-groupe propre du groupe circulaire \mathbf{U} (exercice 11 ci-dessus).

Tout $z \in \Gamma_\infty$ pouvant s'écrire sous la forme $z = e^{\frac{2k\pi i}{n}}$, où $\frac{k}{n} \in \mathbf{Q}$, démontrer que le groupe Γ_∞ est isomorphe au groupe additif $\frac{\mathbf{Q}}{\mathbf{Z}}$.

En déduire, en tenant compte de l'isomorphisme 2) de l'exercice 11 ci-dessus, que le groupe $\frac{\mathbf{U}}{\Gamma_\infty}$ est isomorphe au groupe additif $\frac{\mathbf{R}}{\mathbf{Q}}$. [Appliquer le 3^e théorème d'isomorphisme (4.36).]

- 13) G étant un groupe, on suppose $H < G$ tel que $\frac{G}{H}$ soit fini d'ordre n . Démontrer les propriétés suivantes :

a) $x^n \in H$, quel que soit $x \in G$.

b) $x \in G$ et $x^k \in H$, avec k entier tel que $(k, n) = 1$, implique $x \in H$.

14) Soit \mathbb{Q} le groupe additif des nombres rationnels.

a) Montrer que pour tout sous-groupe propre, non nul, H de \mathbb{Q} , $\frac{\mathbb{Q}}{H}$ est infini.

[Raisonnement par l'absurde et utiliser l'exercice 13 précédent.]

b) Prouver que, quels que soient les sous-groupes propres et non nuls H et K de \mathbb{Q} , on a $H \cap K \neq (0)$; en déduire que

$$H < \mathbb{Q} \Rightarrow \frac{\mathbb{Q}}{H} \text{ non monogène.}$$

[Pour $H \neq (0)$, considérer $H \cap \mathbb{Z}$.]

15) Soit G un groupe; on suppose que G contient un sous-groupe fini H , d'ordre m tel que $H \triangleleft G$. Pour tout $x \in G$, on note \bar{x} la classe de x modulo H .

Etant donné un entier $n \geq 1$ tel que $(m, n) = 1$, démontrer les propriétés suivantes :

$$a) (x \in G \text{ et } o(x) = n) \Rightarrow \left(o(\bar{x}) = n \text{ dans } \frac{G}{H} \right);$$

$$b) \left(o(\bar{x}) = n \text{ dans } \frac{G}{H} \right) \Rightarrow (\exists y \in \bar{x}, o(y) = n).$$

[Utiliser le théorème de Bezout.]

16) Soit G un groupe *abélien fini* tel que $o(G) = n > 1$.

Soit p un nombre premier divisant n . Démontrer, par récurrence sur n , que G contient un élément d'ordre p .

[Lorsque G contient un sous-groupe propre $H \neq (e)$, vérifier que p divise $o(H)$ ou p divise $o\left(\frac{G}{H}\right)$; dans ce dernier cas, utiliser le b) de l'exercice 15 ci-dessus.]

17) Soient E un ensemble non vide et S_E le groupe symétrique de E (groupe des permutations de E).

Pour tout $\sigma \in E$ on note $s(\sigma)$ le support de σ :

$$s(\sigma) = \{x \in E; \sigma(x) \neq x\}.$$

a) Vérifier les propriétés suivantes, pour σ et τ dans S_E :

$$1) s(\sigma^{-1}) = s(\sigma).$$

$$2) s(\sigma \circ \tau) \subseteq s(\sigma) \cup s(\tau).$$

$$3) s(\sigma \circ \tau \circ \sigma^{-1}) = \sigma(s(\tau)).$$

$$4) s(\sigma) \cap s(\tau) = \emptyset \Rightarrow \sigma \circ \tau = \tau \circ \sigma.$$

b) Si $s(\sigma)$ est une partie finie de E , on dit que σ est à *support fini*; on écrira alors $|s(\sigma)| < \infty$. On pose $S_{(E)} = \{\sigma \in S_E; |s(\sigma)| < \infty\}$.

— Démontrer que $S_{(E)}$ est un sous-groupe normal de S_E .

— Prouver que $S_{(E)} = S_E$ si et seulement si E est fini.

— Si E est un ensemble infini, montrer que $S_{(E)}$ est un groupe infini dont tout élément est d'ordre fini et que $\frac{S_E}{S_{(E)}}$ est un groupe infini.

- 18) a) Vérifier que tout groupe engendré par deux éléments a et b satisfaisant aux conditions : $o(a) = 4$, $b^2 = a^2$ et $ab = ba^3$, s'écrit $\langle a, b \rangle = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

En déduire que le groupe $\langle a, b \rangle$ est isomorphe au groupe des quaternions Q_8 (voir exercice 19, chap. I).

b) En identifiant le groupe Q_8 au groupe $\langle a, b \rangle$ ci-dessus, vérifier que Q_8 n'a qu'un seul élément d'ordre 2.

Déterminer le centre du groupe Q_8 .

c) Prouver que tout sous-groupe de Q_8 est un sous-groupe normal, bien que Q_8 ne soit pas abélien.

- 19) G étant un groupe, prouver que $H \triangleleft G \Rightarrow Z(H) \triangleleft G$.

Montrer, en donnant un exemple, qu'en général $Z(H)$ n'est pas contenu dans $Z(G)$ (voir l'exercice 18 ci-dessus).

- 20) On suppose $n \geq 3$ dans \mathbf{N} et on considère le groupe diédral D_n engendré par a et b tels que : $o(a) = n$ et $o(b) = o(ab) = 2$. On note e l'élément unité de D_n .

a) Montrer que $Z(D_n) = (e)$, si n est impair, et $|Z(D_n)| = 2$, si n est pair.

b) On suppose $n = 2k$, $k \geq 2$; vérifier la propriété :

$$\frac{D_{2k}}{Z(D_{2k})} \simeq D_k.$$

c) Si p est un nombre premier, prouver que le sous-groupe cyclique d'ordre p de D_p est le seul sous-groupe propre normal de D_p , autre que (e) .

- 21) Montrer que, dans un groupe fini G , deux éléments conjugués g et g' ont le même ordre.

- 22) Prouver que les permutations

$$u = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 6 & 1 & 4 \end{pmatrix} \quad \text{et} \quad v = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 1 & 6 \end{pmatrix}$$

sont conjuguées dans S_6 .

23) Déterminer la partition en classes de conjugaison du groupe symétrique S_3 et du groupe des quaternions Q_8 .

24) Soient G un groupe et S une partie non vide de G .

On pose $N = N_G(S)$ et on désigne par $\{x_i\}_{i \in I}$ une famille de représentants des classes à gauche distinctes de G modulo N .

Montrer que $i \neq j$ dans I implique $x_i S x_i^{-1} \neq x_j S x_j^{-1}$ et prouver que la classe de conjugaison de S dans $\mathcal{P}(G)$ est formée par l'ensemble des $x_i S x_i^{-1}$, pour $i \in I$.

25) Soient G un groupe et H un sous-groupe de G .

a) Pour tout $a \in G$, on note σ_a l'automorphisme intérieur de G défini par a .

Montrer que, si $a \in N_G(H)$, alors la restriction σ'_a de σ_a à H est un automorphisme de H .

En considérant l'application : $N_G(H) \rightarrow \text{Aut}(H)$, démontrer

$$a \mapsto \sigma'_a$$

que le groupe $\frac{N_G(H)}{C_G(H)}$ est isomorphe à un sous-groupe de $\text{Aut}(H)$.

b) On suppose que le sous-groupe H est monogène et normal dans G .

— Vérifier que $C_G(H)$ est normal dans G .

— En utilisant l'exercice 17, chap. III, démontrer que le groupe $\frac{G}{C_G(H)}$ est abélien fini et que si H est cyclique d'ordre n ,

alors $o\left(\frac{G}{C_G(H)}\right)$ divise $\varphi(n)$, φ étant la fonction d'Euler ; si H est monogène infini, alors $o\left(\frac{G}{C_G(H)}\right)$ est 1 ou 2.

26) Soient G un groupe et N, H deux sous-groupes de G .

a) On suppose $N \triangleleft G$, $[G : N]$ fini et H fini; on pose $r = [G : N]$ et $s = o(H)$. Montrer que, si r et s sont premiers entre eux, alors $H \subseteq N$.

b) On suppose $N \triangleleft G$, N fini et $[G : H]$ fini; on pose $n = o(N)$ et $m = [G : H]$.

Prouver que, si n et m sont premiers entre eux, alors $N \subseteq H$ (voir l'exercice 2, chap. II).

27) G étant un groupe, pour tout $g \in G$, notons C_g la classe de conjugaison de g dans G .

a) Vérifier que, quel que soit $\alpha \in \text{Aut}(G)$, $\alpha(C_g)$ est la classe de conjugaison d'un élément de G .

b) Soit J l'ensemble des éléments $\alpha \in \text{Aut}(G)$ tels que, pour tout $g \in G$, $\alpha(C_g) = C_g$. Démontrer que J est un sous-groupe normal de $\text{Aut}(G)$, contenant $\text{Int}(G)$.

28) G étant un groupe, on désigne par F l'ensemble des éléments $x \in G$ n'ayant qu'un nombre fini de conjugués dans G . Démontrer que F est un sous-groupe caractéristique dans G .

29) Soit K un sous-groupe caractéristique d'un groupe G .

a) Montrer que, pour tout $\alpha \in \text{Aut}(G)$, il existe un unique $\bar{\alpha} \in \text{Aut}\left(\frac{G}{K}\right)$ tel que $\alpha \circ \pi = \pi \circ \bar{\alpha}$, π étant l'épimorphisme canonique $G \rightarrow \frac{G}{K}$.

b) Vérifier que $\Phi : \text{Aut}(G) \rightarrow \text{Aut}\left(\frac{G}{K}\right)$ est un morphisme de groupes.
 $\alpha \mapsto \bar{\alpha}$

c) Soit H un sous-groupe de G contenant K , démontrer la propriété : $\frac{H}{K} \subset \frac{G}{K} \Rightarrow H \subset G$; vérifier que la réciproque est fautive en considérant, dans le groupe diédral D_4 d'ordre 8, le sous-groupe $K = Z(D_4)$ et le sous-groupe H égal à l'unique sous-groupe d'ordre 4 de D_4 .

30) Soient G un groupe quelconque et Γ un groupe abélien.

1° Démontrer que, pour tout $f \in \text{Hom}(G, \Gamma)$, on a

$$D(G) \subseteq \text{Ker } f;$$

en déduire qu'il existe un unique $\bar{f} \in \text{Hom}\left(\frac{G}{D(G)}, \Gamma\right)$ tel que $\bar{f} \circ \pi = f$, π étant l'épimorphisme canonique $G \rightarrow \frac{G}{D(G)}$.

2° On considère l'application :

$$\Phi : \text{Hom}(G, \Gamma) \rightarrow \text{Hom}\left(\frac{G}{D(G)}, \Gamma\right). \\ f \mapsto \bar{f}$$

Compte tenu de la structure de groupe abélien de $\text{Hom}(G, \Gamma)$ et de $\text{Hom}\left(\frac{G}{D(G)}, \Gamma\right)$ (voir exercice 29, chap. I), prouver que Φ est un isomorphisme de groupes.

31) Soit un groupe G .

1° Etant donné x, y, z dans G , vérifier la relation :

$$[xy, z] = y^{-1}[x, z]y[y, z].$$

2° On pose $Z_1 = Z(G)$; montrer qu'il existe un unique sous-groupe Z_2 de G tel que $Z_1 \subseteq Z_2$, $Z_2 \triangleleft G$ et $\frac{Z_2}{Z_1} = Z\left(\frac{G}{Z_1}\right)$.

3° Etant donné $z \in Z_2$, on considère l'application

$$\begin{aligned}\varphi_z : G &\rightarrow G \\ x &\mapsto [x, z].\end{aligned}$$

Prouver que φ_z est un endomorphisme du groupe G , tel que $\text{Im } \varphi_z \subseteq Z_1$ et $D(G) \subseteq \text{Ker } \varphi_z$ (voir le 1° de l'exercice 30 ci-dessus).

32) Soit G un sous-groupe du groupe symétrique S_n ($n \geq 2$) contenant une permutation impaire.

Montrer que $GA_n = S_n$, A_n étant le groupe alterné de degré n ; en déduire que G contient au moins un sous-groupe normal d'indice 2.

33) Soit G un groupe fini, *non abélien*, d'ordre pair.

Le but de cet exercice est de prouver qu'il existe au moins un élément d'ordre 2 dans G .

a) Prouver que les hypothèses impliquent : $o(G) > 4$.

b) On pose $A = \{x \in G; x^2 = e\}$ et $B = \{x \in G; x^2 \neq e\}$.

Montrer que nécessairement B est non vide (exercice 5, chap. I).

Démontrer que $|B|$ est pair; en conclure que $|A| \geq 2$.

34) Soit p un nombre premier; on pose

$$C_{p^\infty} = \{z \in \mathbb{C}^*; \exists n \in \mathbb{N}, z^{p^n} = 1\}.$$

a) Vérifier que C_{p^∞} est un sous-groupe du groupe Γ_∞ de l'exercice 12 ci-dessus.

b) Pour tout $n \in \mathbb{N}$, on note C_{p^n} le groupe cyclique des racines p^n -ième de l'unité dans \mathbb{C} .

Vérifier que, quel que soit $n \in \mathbb{N}$, on a $C_{p^n} < C_{p^{n+1}}$ et montrer que $C_{p^\infty} = \bigcup_{n \in \mathbb{N}} C_{p^n}$.

Prouver que, pour toute partie infinie I de \mathbb{N} , on a encore :

$$C_{p^\infty} = \bigcup_{n \in I} C_{p^n}.$$

c) Soit D un sous-groupe *propre* de C_{p^∞} .

A tout $z \in D$, on associe le *plus petit entier* $k \in \mathbb{N}$ tel que $z \in C_{p^k}$; on note K la partie de \mathbb{N} ainsi définie.

Montrer que K est une partie finie de \mathbb{N} .

En déduire qu'il existe $m \in \mathbb{N}$ tel que $D = C_{p^m}$.

Quelle propriété peut-on énoncer concernant les sous-groupes de C_{p^∞} ?

d) A tout $n \in \mathbb{N}$, on associe un générateur u_n du groupe C_{p^n} .

Montrer que l'on peut choisir u_n de telle façon que l'on ait

$$u_{n+1}^p = u_n \quad (1)$$

Prouver que l'ensemble $\{u_n; n \in \mathbb{N}\}$, où les u_n vérifient (1), forme une partie génératrice du groupe C_{p^∞} .

e) Soit G un groupe abélien (multiplicatif) ayant une partie génératrice infinie dénombrable : $\{a_n; n \in \mathbb{N}\}$ telle que : $a_0 = e$ et $a_{n+1}^p = a_n$, $\forall n \in \mathbb{N}$.

Vérifier que tout sous-groupe monogène $\langle a_n \rangle$ de G est cyclique d'ordre p^n ; en déduire que G est isomorphe à C_{p^∞} .

f) Soit $n \in \mathbb{N}$; pour tout $z \in C_{p^\infty}$, notons \bar{z} la classe de z modulo C_{p^n} .

Démontrer que dans le groupe quotient $\frac{C_{p^\infty}}{C_{p^n}}$ les classes $\overline{u_{n+j}}$, $j \in \mathbb{N}$, sont distinctes, les u_n formant la famille génératrice de C_{p^∞} définie dans d).

En utilisant e), montrer que, pour tout $n \in \mathbb{N}$, on a : $\frac{C_{p^\infty}}{C_{p^n}} \simeq C_{p^\infty}$.

Remarque : Pour tout p premier, le groupe C_{p^∞} (et tout groupe qui lui est isomorphe) est appelé *p-groupe de Prüfer* (ou groupe *p-quasi-cyclique*).

- 35) On considère le groupe diédral infini, noté D_∞ . Compte tenu des notations et des résultats de l'exercice 31, chapitre III, dans lequel est défini le groupe D_∞ , on rappelle que D_∞ et le groupe des isométries de la droite affine \mathbb{R} formé par l'ensemble des éléments de la forme τ_1^n et $\tau_1^n \circ \sigma_0$, où $n \in \mathbb{Z}$, τ_1 est la translation $x \mapsto x + 1$ et σ_0 est la symétrie $x \mapsto -x$.

On notera e l'élément neutre de D_∞ .

1° Prouver que $H = \langle \tau_1 \rangle$ est l'unique sous-groupe monogène infini de D_∞ tel que $[D_\infty : H] = 2$ et tout élément de $D_\infty \setminus H$ est d'ordre 2.

Montrer que H est normal maximal dans D_∞ .

2° a) Vérifier que tout sous-groupe de H est de la forme $H_n = \langle \tau_1^n \rangle$ où $n \in \mathbb{N}$ et que pour $n \neq 0$ on a $\frac{H}{H_n} \simeq C_n$, groupe cyclique d'ordre n .

b) Démontrer que, pour tout $n \in \mathbb{N}$, on a $H_n \triangleleft D_\infty$. Prouver que $n \geq 2$ implique $\frac{D_\infty}{H_n} \simeq D_n$, où D_n est le groupe diédral d'ordre $2n$ et que, pour $n = 1$, on a $\frac{D_\infty}{H_1} \simeq C_2$.

c) Vérifier que, pour tout sous-groupe H' d'ordre 2, de D_∞ , on a $D_\infty = HH'$.

3° Soit K un sous-groupe de D_∞ tel que $K \not\subseteq H$.

a) Montrer que $D_\infty = HK$; en déduire que $[K : K \cap H] = 2$.

b) Démontrer que $K \cap H \neq (e)$ implique $K \simeq D_\infty$. [Utiliser le 1°.]

c) Justifier l'existence d'un unique $n \in \mathbb{N}$ tel que $K \cap H = H_n$.

d) Vérifier que tout sous-groupe propre de D_∞ est isomorphe, soit à \mathbb{Z} , soit à C_2 , soit à D_∞ .

4° Pour $n \geq 1$ dans \mathbb{N} , on note \mathcal{K}_n l'ensemble des sous-groupes K de D_∞ tels que $K \not\subseteq H$ et $K \cap H = H_n$. Démontrer que $\text{card}(\mathcal{K}_n) = n$.

5° Soit $K \in \mathcal{K}_n$ ($n \geq 1$). Démontrer que :

$$K \triangleleft D_\infty \Leftrightarrow n = 1 \text{ ou } n = 2.$$

— En déduire que les seuls sous-groupes normaux de D_∞ sont les sous-groupes de H et deux sous-groupes d'indice 2, isomorphes à D_∞ .

— Quelles sont, à un isomorphisme près, les images homomorphes de D_∞ , autres que D_∞ et (e) ?

36) Soit un groupe $G \neq (e)$.

a) Soit $H \leq M < G$, avec $H \triangleleft G$; démontrer que $\frac{M}{H}$ est maximal dans $\frac{G}{H}$ si et seulement si M est maximal dans G .

b) Montrer que tout sous-groupe propre de \mathbb{Z} est contenu dans un sous-groupe maximal de \mathbb{Z} .

Etant donné $n > 1$ dans \mathbb{N} , déterminer les sous-groupes maximaux de $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

c) Prouver que le groupe $(\mathbb{Q}, +)$ n'a pas de sous-groupe maximal (utiliser l'exercice 14 ci-dessus).

d) Vérifier que le groupe C_{p^∞} (exercice 34 ci-dessus) n'a pas de sous-groupe maximal.

- 37) Soit un corps K ; pour $n \geq 2$ dans \mathbb{N} , on note G le groupe linéaire général $GL(n, K)$, S le groupe linéaire spécial $SL(n, K)$ (voir exemple (1.63)) et H le sous-groupe de G formé par l'ensemble des matrices diagonales de G . \mathbb{Z}_2 et \mathbb{Z}_3 désignent, respectivement, les corps à 2 et 3 éléments.

a) Vérifier que $D(G) = S$, si $n > 2$ et $K \neq \mathbb{Z}_2$.

Pour $n = 2$ et $K = \mathbb{Z}_2$, déterminer S et $D(G)$ et montrer ainsi, que $S \neq D(G)$ (voir l'exercice 22, chap. I).

b) Démontrer que $C_G(H) = H$, si $n \geq 2$ et $K \neq \mathbb{Z}_2$; en déduire que $Z(G) = \{\lambda I_n; \lambda \in K^*\}$, I_n étant la matrice unité de G ; en conclure que $Z(G) \simeq K^*$.

Comparer alors les groupes $Z(G)$ et $\frac{G}{D(G)}$.

c) K étant différent de \mathbb{Z}_2 , on suppose $n > 2$ ou $K \neq \mathbb{Z}_3$.

Prouver que $C_G(H \cap S) = H$; en déduire que $C_G(S) = Z(G)$; en conclure que $Z(S) = Z(G) \cap S = \{\lambda I_n; \lambda \in K^*, \lambda^n = 1\}$.

- 38) a) On suppose que M est un sous-groupe maximal d'un groupe G ; démontrer que :

$$Z(G) \leq M \quad \text{ou} \quad D(G) \leq M.$$

[Montrer que $Z(G) \not\leq M \Rightarrow M < G$.]

b) Vérifier que, dans tout groupe G , on a $D(G) \cap Z(G) \leq \Phi(G)$, $\Phi(G)$ étant le sous-groupe de Frattini de G (définition (4.56)).

CHAPITRE V

Groupe opérant sur un ensemble

1 — Notion de groupe opérant sur un ensemble

A / Définition. Généralités

Définition (5.1) : Soit G un groupe multiplicatif d'élément unité e . Soit E un ensemble *non vide*. On dit que G *opère à gauche sur E* , si E est muni d'une loi de composition externe à gauche, à opérateurs dans G ; c'est-à-dire qu'il existe une application :

$$\begin{aligned} G \times E &\rightarrow E \\ (g, x) &\mapsto g.x \end{aligned}$$

satisfaisant aux deux conditions suivantes :

$$\forall (g_1, g_2) \in G \times G, \quad \forall x \in E, \quad g_1 g_2.x = g_1.(g_2.x) \quad (1)$$

$$\forall x \in E, \quad e.x = x \quad (2)$$

Remarque (5.2) : On définit de façon analogue la notion de groupe *opérant à droite* sur un ensemble (non vide).

Dans la suite (sauf indication contraire), nous conviendrons de dire qu'un groupe G opère sur un ensemble E , si G opère à gauche sur E .

Dans ce cas, E sera appelé un G -ensemble (un G -ensemble sera toujours non vide).

PROPOSITION (5.3). *Soit G un groupe opérant sur un ensemble E .*

1° *Pour tout $g \in G$, l'application $\gamma_g : E \rightarrow E$ est une permutation de E .*

$$x \mapsto g.x$$

2° S_E désignant le groupe des permutations de E , l'application

$\gamma : G \rightarrow S_E$ est un morphisme de groupes et $\text{Ker } \gamma$ est appelé : noyau de l'action de G sur E .

$$g \mapsto \gamma_g$$

Preuve :

1° Montrons que $\gamma_g \in S_E$, c'est-à-dire que γ_g est une bijection.

γ_g est surjective, car, pour tout $x \in E$, $x = \gamma_g(g^{-1}x)$.

γ_g est injective; en effet, soient x et y dans E tels que $\gamma_g(x) = \gamma_g(y)$, c'est-à-dire $g \cdot x = g \cdot y$,

alors $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y)$, d'où $x = y$.

2° Soient g_1 et g_2 dans G ; pour tout $x \in E$,

$$\gamma_{g_1} \circ \gamma_{g_2}(x) = g_1 \cdot (g_2 \cdot x) = g_1 g_2 \cdot x = \gamma_{g_1 g_2}(x);$$

donc $\gamma_{g_1} \circ \gamma_{g_2} = \gamma_{g_1 g_2}$,

ce qui prouve que γ est un morphisme de groupes.

Remarque (5.4) : D'après ce qui précède, à toute action de G sur un ensemble E , correspond un morphisme de groupes, γ , de G dans S_E .

Réciproquement, à tout $\lambda \in \text{Hom}(G, S_E)$, on peut associer l'action de G sur E définie par :

$$G \times E \rightarrow E$$

$$(g, x) \mapsto \lambda(g)(x).$$

On a en effet, quels que soient g_1 et g_2 dans G et x dans E :

$$\lambda(g_1 g_2)(x) = (\lambda(g_1) \circ \lambda(g_2))(x) = \lambda(g_1)(\lambda(g_2)(x))$$

et $\lambda(e)(x) = \text{id}_E(x) = x$.

B / Exemples classiques

G désigne un groupe multiplicatif.

Exemple (5.5) : G opère sur G par translation à gauche.

On sait que, pour tout $g \in G$, la translation à gauche τ_g est une permutation de G et que $G \rightarrow S_G$ est un morphisme de groupes

$$g \mapsto \tau_g$$

(lemme 1.77); par suite, $G \times G \rightarrow G$ définit une action de G sur lui-même.

$$(g, x) \mapsto gx$$

Exemple (5.6) : G opère sur $\mathcal{P}(G)$ par translation à gauche.

$\mathcal{P}(G)$ désigne l'ensemble des parties de G .

L'application $G \times \mathcal{P}(G) \rightarrow \mathcal{P}(G)$, où $gS = \{gx; x \in S\}$ si

$$(g, S) \mapsto gS$$

$S \neq \emptyset$ et $g\emptyset = \emptyset$, vérifie, en effet, les conditions (1) et (2) de la définition (5.1).

Exemple (5.7) : Soit H un sous-groupe de G ; alors G opère par translation à gauche, sur l'ensemble $\left(\frac{G}{H}\right)_g$ des classes à gauche de G modulo H .

En effet, posons $Q_H = \left(\frac{G}{H}\right)_g$, Q_H est une partie non vide de $\mathcal{P}(G)$; vérifions que la correspondance

$$\begin{aligned} G \times Q_H &\rightarrow Q_H \\ (g, xH) &\mapsto gxH \end{aligned}$$

est une application.

Supposons $xH = yH$, donc $y^{-1}x \in H$; pour tout $g \in G$, $(gy)^{-1}gx = y^{-1}g^{-1}gx = y^{-1}x$ appartient à H , d'où $gxH = gyH$. Ainsi G opère sur Q_H par translation à gauche.

Exemple (5.8) : G opère sur G par conjugaison.

En effet, l'application : $G \times G \rightarrow G$ satisfait aux conditions (1) et (2) de la définition (5.1).

$$(g, x) \mapsto gxg^{-1}$$

La permutation de G associée à tout $g \in G$ est, dans ce cas, l'automorphisme intérieur $\sigma_g : x \mapsto gxg^{-1}$ et, d'après la proposition (5.3), $\sigma : G \rightarrow S_G$ est un morphisme de groupes.

$$g \mapsto \sigma_g$$

PROPOSITION (5.9). *Soit $\text{Int}(G)$ le groupe des automorphismes intérieurs d'un groupe G ; on a alors :*

$$\text{Int}(G) \simeq \frac{G}{Z(G)}, \quad \text{où } Z(G) \text{ est le centre de } G.$$

Preuve : Pour le morphisme $\sigma : G \rightarrow S_G$, on a

$$g \mapsto \sigma_g$$

$$\text{Im } \sigma = \text{Int}(G) \quad \text{et} \quad \text{Ker } \sigma = \{g \in G; \sigma_g = \text{id}_G\};$$

$$\text{d'où} \quad g \in \text{Ker } \sigma \Leftrightarrow gxg^{-1} = x, \quad \forall x \in G$$

$$g \in \text{Ker } \sigma \Leftrightarrow gx = xg, \quad \forall x \in G;$$

par suite $\text{Ker } \sigma = Z(G)$.

D'après le 1^{er} théorème d'isomorphisme, on a donc

$$\text{Int}(G) \simeq \frac{G}{Z(G)}.$$

Exemple (5.10) : G opère sur $\mathcal{P}(G)$ par conjugaison.

Comme précédemment, l'application

$$\begin{aligned} G \times \mathcal{P}(G) &\rightarrow \mathcal{P}(G) \\ (g, S) &\mapsto gSg^{-1} \end{aligned}$$

satisfait aux conditions (1) et (2) de la définition (5.1).

$gSg^{-1} = \sigma_g(S)$, où σ_g est l'automorphisme intérieur de G défini par g . (Si $S = \emptyset$, $gSg^{-1} = \emptyset$, quel que soit $g \in G$.)

Exemple (5.11) : Soient E un ensemble non vide et S_E son groupe symétrique; alors, l'application :

$$\begin{aligned} S_E \times E &\rightarrow E \\ (\sigma, x) &\mapsto \sigma(x) \end{aligned}$$

satisfait aux conditions (1) et (2) de la définition (5.1); on dit que S_E opère « de façon naturelle » sur E .

En particulier, pour tout entier $n \geq 1$, S_n opère de façon naturelle sur $N_n = \{1, 2, \dots, n\}$, ou sur tout ensemble $X = \{x_1, x_2, \dots, x_n\}$ de cardinal n , par

$$\begin{aligned} S_n \times X &\rightarrow X \\ (\sigma, x_i) &\mapsto x_{\sigma(i)}. \end{aligned}$$

2 — Sous-groupe d'isotropie ou stabilisateur. Orbite

A / Définitions. Exemples

Soit G un groupe opérant sur un ensemble E , grâce à l'application :

$$\begin{aligned} G \times E &\rightarrow E \\ (g, x) &\mapsto g \cdot x. \end{aligned}$$

1° A tout $x \in E$, on associe

$$G_x = \{g \in G; g \cdot x = x\} \quad (3)$$

On vérifie facilement que G_x est un sous-groupe de G .

G_x est formé des éléments de G qui « laissent fixe » l'élément x de E .

Définition (5.12) : E étant un G -ensemble, le sous-groupe G_x de G , associé à tout $x \in E$ et défini ci-dessus, est appelé *sous-groupe d'isotropie de x* ou *stabilisateur de x* (nous utiliserons généralement la seconde appellation, qui, dans certains ouvrages, se traduit par la notation $Stab_G(x)$).

2° On considère dans E la relation binaire ρ_G définie par :

$$x \rho_G y \Leftrightarrow \exists g \in G, y = g \cdot x \quad (4)$$

Les conditions (1) et (2) de la définition (5.1) impliquent que ρ_G est une relation d'équivalence dans E .

Définition (5.13) : E étant un G -ensemble, la classe d'équivalence modulo ρ_G d'un élément x de E est appelée *orbite de x suivant G* ou *G -orbite de x* (nous adopterons, en général, la seconde appellation).

La G -orbite d'un élément x de E sera notée Ω_x :

$$\Omega_x = \{g \cdot x; g \in G\} \quad (5)$$

Exemples (5.14) :

1° G opère sur G par translation à gauche ; pour tout $x \in G$, on a

$$G_x = \{g \in G; gx = x\}, \quad \text{donc } G_x = \{e\}$$

$$\Omega_x = \{gx; g \in G\} = Gx, \quad \text{donc } \Omega_x = G.$$

2° G opère sur G par conjugaison; pour tout $x \in G$,

$$G_x = \{g \in G; gxg^{-1} = x\} = C_G(x),$$

le centralisateur de x dans G .

$$\Omega_x = \{gxg^{-1}; g \in G\} = (\text{classe de conjugaison de } x \text{ dans } G).$$

On en déduit que ρ_G coïncide, dans ce cas, avec la relation de conjugaison dans G .

3° G opère sur $\mathcal{P}(G)$ par conjugaison, alors pour $S \in \mathcal{P}(G)$ et $S \neq \emptyset$,

$$G_S = \{g \in G; gSg^{-1} = S\} = N_G(S),$$

le normalisateur de S dans G .

$$\Omega_S = \{gSg^{-1}; g \in G\}$$

= (classe de conjugaison de S dans $\mathcal{P}(G)$)

$$G_\emptyset = G \quad \text{et} \quad \Omega_\emptyset = \{\emptyset\}.$$

ρ_G coïncide avec la relation de conjugaison dans $\mathcal{P}(G)$.

4° Soit $\sigma \in S_n$ ($n > 1$ dans \mathbb{N}). Supposons $o(\sigma) = r$ dans le groupe S_n et posons $G = \langle \sigma \rangle$.

En considérant G comme opérant de façon naturelle sur $N_n = \{1, 2, \dots, n\}$, on a, pour tout $i \in N_n$:

$$\Omega_i = \{\sigma^k(i); 1 \leq k \leq r\}.$$

Ω_i coïncide avec ce que l'on a appelé, dans le chapitre III, la σ -orbite de i .

En effet, la relation d'équivalence ρ_G n'est autre, ici, que la relation \mathcal{R}_σ (voir chap. III).

5° Soit $H \leq G$; dans l'action de G , par translation à gauche, sur $\mathcal{Q}_H = \left(\frac{G}{H} \right)_o$, pour toute classe à gauche xH , on a

$$G_{xH} = xHx^{-1}.$$

En effet,

$$g \in G_{xH} \Leftrightarrow gxH = xH$$

$$g \in G_{xH} \Leftrightarrow gx \in xH$$

$$g \in G_{xH} \Leftrightarrow g \in xHx^{-1}.$$

PROPOSITION (5.15). Soient un groupe G et $H \leq G$; alors le noyau de l'action de G sur $Q_H = \left(\frac{G}{H}\right)_g$ est $\bigcap_{x \in G} xHx^{-1}$ et c'est le plus grand sous-groupe de G , normal dans G et contenu dans H .

Preuve : Le noyau de l'action de G sur Q_H est $\text{Ker } \gamma$, où γ est le morphisme de groupes : $G \rightarrow S_{Q_H}$

$$g \mapsto \gamma_g,$$

tel que $\gamma_g(xH) = gxH$, quel que soit $xH \in Q_H$.

On a donc $\text{Ker } \gamma = \{g \in G; \gamma_g = \text{id}_{Q_H}\}$; par suite,

$$g \in \text{Ker } \gamma \Leftrightarrow gxH = xH, \quad \forall xH \in Q_H$$

$$\text{d'où } g \in \text{Ker } \gamma \Leftrightarrow g \in \bigcap_{x \in G} G_{xH}.$$

Alors, $G_{xH} = xHx^{-1}$ implique $\text{Ker } \gamma = \bigcap_{x \in G} xHx^{-1}$.

Le noyau d'un morphisme de groupe étant un sous-groupe normal, on a $\text{Ker } \gamma \triangleleft G$; d'autre part, $g \in \text{Ker } \gamma$ implique, en particulier, $gH = H$, d'où $\text{Ker } \gamma \subseteq H$.

Supposons $N < G$ et $N \subseteq H$; pour tout $x \in G$, on a alors $N = xNx^{-1} \subseteq xHx^{-1}$, d'où $N \subseteq \text{Ker } \gamma$.

Remarque (5.16) : Les notations étant celles de la proposition (5.15) :

1° $H \triangleleft G \Rightarrow \text{Ker } \gamma = H$.

2° Si G est un groupe simple, alors, quel que soit $H < G$, G est isomorphe à un sous-groupe de S_{Q_H} , donc à un sous-groupe de $S_{[G:H]}$.

En effet, $H \neq G$, implique, dans ce cas, $\text{Ker } \gamma = (e)$; γ est injectif, donc $G \simeq \text{Im } \gamma$.

PROPOSITION (5.17). Si G est un groupe fini d'ordre $n > 1$, contenant un sous-groupe propre H tel que $[G:H] = k > 1$ et n ne divise pas $k!$, alors G n'est pas simple.

Preuve : Si G était simple, d'après la remarque (5.16) 2°, G serait isomorphe à un sous-groupe de $S_{[G:H]}$ qui est d'ordre $k!$, donc n diviserait $k!$, ce qui est contraire à l'hypothèse.

B / Propriétés des stabilisateurs et des orbites

THÉORÈME (5.18). *Soit E un G -ensemble ; alors, quels que soient x et y dans E , on a*

$$x\rho_G y \Rightarrow G_x \text{ et } G_y \text{ conjugués dans } \mathcal{P}(G).$$

Preuve : On suppose que G opère sur E par l'application

$$G \times E \rightarrow E$$

$$(g, x) \mapsto g.x$$

$$x\rho_G y \Leftrightarrow \exists g \in G, y = g.x,$$

montrons alors que $G_y = gG_x g^{-1}$.

Soit $g' \in G_y$, on a $y = g'.y$, d'où $g.x = g'.(g.x)$ et par suite $x = g^{-1}g'g.x$. On en déduit que $g^{-1}g'g \in G_x$, donc $g' \in gG_x g^{-1}$, ce qu'implique $G_y \subseteq gG_x g^{-1}$. Réciproquement, soit $g_1 \in gG_x g^{-1}$, alors :

$$g^{-1}g_1g \in G_x \Rightarrow g^{-1}g_1g.x = x,$$

d'où $g_1g.x = gx$, c'est-à-dire $g_1.y = y$.

On a donc $g_1 \in G_y$, par suite $gG_x g^{-1} \subseteq G_y$.

G_y est donc conjugué de G_x par g .

THÉORÈME (5.19). *E étant un G -ensemble, pour tout $x \in E$, on a :*

$$|\Omega_x| = [G : G_x] \quad (6)$$

$|\Omega_x|$ désignant le cardinal de Ω_x .

Preuve : On suppose que G opère à gauche sur E .

Pour démontrer (6), montrons qu'il existe une bijection de Ω_x sur $\left(\frac{G}{G_x}\right)_o$.

$$\Omega_x = \{g.x; g \in G\}; \text{ posons } Q_x = \left(\frac{G}{G_x}\right)_o = \{gG_x; g \in G\}.$$

$$\text{Soit } \lambda : \Omega_x \rightarrow Q_x \\ g.x \mapsto gG_x$$

- λ est une application : en effet, supposons $g \cdot x = g' \cdot x$; on a alors $x = g^{-1} g' \cdot x$, donc $g^{-1} g' \in G_x$, ce qui implique $g G_x = g' G_x$;
- la définition de λ implique sa surjectivité;
- λ est injective : en effet,

$$g_1 G_x = g_2 G_x \Rightarrow g_1^{-1} g_2 \in G_x$$

$$g_1^{-1} g_2 \in G_x \Rightarrow g_1^{-1} g_2 \cdot x = x,$$

$$\text{donc } g_1 G_x = g_2 G_x \Rightarrow g_1 \cdot x = g_2 \cdot x.$$

En conclusion, λ est une bijection, d'où l'égalité (6).

COROLLAIRE (5.20). Soit G un groupe considéré comme opérant sur $\mathcal{P}(G)$ par conjugaison; pour tout $S \in \mathcal{P}(G)$, on a :

$$|\Omega_S| = [G : N_G(S)] \quad (7)$$

COROLLAIRE (5.21). Soit E un ensemble fini et G un groupe opérant sur E . Si $\{x_i\}_{1 \leq i \leq r}$ est une famille de représentants des G -orbites distinctes, alors :

$$|E| = \sum_{i=1}^r [G : G_{x_i}] \quad (8)$$

Preuve : E étant fini, chaque G -orbite est un ensemble fini et le nombre des G -orbites est fini. Si $\{x_i\}_{1 \leq i \leq r}$ est une famille de représentants des G -orbites distinctes de E , les Ω_{x_i} ($1 \leq i \leq r$) forment une partition de E , d'où

$$|E| = \sum_{i=1}^r |\Omega_{x_i}|.$$

L'application de la formule (6) donne alors $|E| = \sum_{i=1}^r [G : G_{x_i}]$.

COROLLAIRE (5.22). Soit G un groupe fini considéré comme opérant sur lui-même par conjugaison.

Si $\{x_i\}_{1 \leq i \leq r}$ est une famille de représentants des classes de conjugaison distinctes dans G :

$$o(G) = \sum_{i=1}^r [G : C_G(x_i)] \quad (9)$$

où $C_G(x_i)$ est le centralisateur de x_i dans G .

La relation (9) est appelée « *équation aux classes* » du groupe fini G , elle s'obtient en appliquant (8) au cas de l'action du groupe fini G sur lui-même, par conjugaison.

Remarques (5.23) : Soit G un groupe considéré comme opérant sur lui-même *par conjugaison*; $Z(G)$ étant son centre :

$$x \in Z(G) \quad \Leftrightarrow \quad C_G(x) = G,$$

c'est-à-dire

$$x \in Z(G) \quad \Leftrightarrow \quad [G : C_G(x)] = 1,$$

ou encore,

$$x \in Z(G) \quad \Leftrightarrow \quad \Omega_x = \{x\}.$$

Définition (5.24) : Si E est un G -ensemble, toute G -orbite réduite à un seul élément sera dite *ponctuelle*.

THÉORÈME (5.25). *Soit G un groupe fini de centre $Z(G)$.*

Soit $\{x_i\}_{1 \leq i \leq k}$ une famille de représentants des classes de conjugaison distinctes et non ponctuelles de G , alors :

$$o(G) = o(Z(G)) + \sum_{i=1}^k [G : C_G(x_i)] \quad (10)$$

Preuve : On remarque que, si G est abélien, toutes les classes de conjugaison sont ponctuelles et $G = Z(G)$, la formule (10) est vérifiée.

Supposons G non abélien; $Z(G) \neq G$ implique qu'il existe des classes de conjugaison non ponctuelles dans G .

Soit, comme dans le corollaire (5.22), $\{x_i\}_{1 \leq i \leq r}$ une famille de représentants des classes de conjugaison distinctes de G ; alors (en changeant éventuellement l'ordre des indices) il existe k ($1 \leq k < r$) tel que

$$x_i \notin Z(G) \quad \text{pour } 1 \leq i \leq k$$

$$\text{et} \quad x_i \in Z(G) \quad \text{pour } k+1 \leq i \leq r.$$

La relation (10) s'obtient alors à partir de (9), en remplaçant $[G : C_G(x_i)]$ par 1 pour $k + 1 \leq i \leq r$, et chaque classe de conjugaison de $x_i \in Z(G)$ étant ponctuelle, nécessairement $r - k = o(Z(G))$.

Remarque (5.26) : Les hypothèses et les notations étant celles du théorème (5.25), en désignant par Ω_{x_i} la classe de conjugaison de x_i pour $1 \leq i \leq k$, la formule (10) s'écrit :

$$o(G) = o(Z(G)) + \sum_{i=1}^k |\Omega_{x_i}| \quad (11)$$

et l'égalité $|\Omega_{x_i}| = [G : C_G(x_i)]$ implique que le cardinal de la classe de conjugaison d'un élément quelconque de G divise l'ordre du groupe G .

THÉORÈME (5.27). *Si G est un groupe fini d'ordre p^n , p étant un nombre premier et $n \geq 1$ dans \mathbf{N} , alors le centre de G n'est pas réduit à l'élément neutre.*

Preuve : Si G est abélien, $Z(G) = G$ et l'hypothèse $n \geq 1$ implique $G \neq (e)$. Supposons G non abélien; la formule (10) implique

$$o(Z(G)) = p^n - \sum_{i=1}^k [G : C_G(x_i)],$$

avec $[G : C_G(x_i)] > 1$ pour tout i ($1 \leq i \leq k$).

Or chaque $[G : C_G(x_i)]$ divise $o(G) = p^n$; on en déduit que p divise $\sum_{i=1}^k [G : C_G(x_i)]$ et, par suite, p divise $o(Z(G))$; d'où $o(Z(G)) > 1$.

COROLLAIRE (5.28). *Si p est un nombre premier, alors tout groupe fini d'ordre p^2 est abélien.*

Preuve : Soit G un groupe d'ordre p^2 ; d'après le théorème (5.27), on a $Z(G) \neq (e)$; alors,

soit $o(Z(G)) = p^2$, donc G est abélien;

soit $o(Z(G)) = p$ et dans ce cas $\frac{G}{Z(G)}$ est d'ordre premier p , donc cyclique, ce qui implique G abélien, d'après la proposition (4.13).

Définition (5.29) : On dit qu'un groupe G opère transitivement sur un ensemble E , si E n'a qu'une seule G -orbite (qui est nécessairement E); autrement dit, si :

$$\forall (x, y) \in E \times E, \quad \exists g \in G, \quad y = g \cdot x.$$

Dans ce cas, on dit que E est un G -ensemble homogène, ou que G est transitif sur E .

Dans le cas contraire, on dit que G opère intransitivement sur E , ou que G est intransitif sur E .

Remarque (5.30) : Compte tenu de la définition (5.29), pour qu'un groupe G opère transitivement sur un ensemble E , il faut et il suffit qu'il existe $x \in E$ tel que $\Omega_x = E$.

Exemple (5.31) : Les exemples (5.14) montrent que :

- 1) G opère transitivement sur G , par translation à gauche;
- 2) Si $G \neq (e)$, G opère intransitivement sur G , par conjugaison;
- 3) Si $G \neq (e)$, G opère intransitivement sur $\mathcal{P}(G)$, par conjugaison;
- 4) E étant un G -ensemble, quel que soit $x \in E$, G opère transitivement sur la G -orbite de x .

PROPOSITION (5.32). G étant un groupe, quel que soit $H \leq G$, G opère transitivement par translation à gauche sur l'ensemble $Q_H = \left(\frac{G}{H} \right)_g$.

De plus, si E est un G -ensemble homogène, alors il existe $H \leq G$ tel que E soit équipotent à Q_H .

Preuve : D'après l'exemple (5.7), G opère sur Q_H par l'application :

$$\begin{aligned} G \times Q_H &\rightarrow Q_H \\ (g, xH) &\mapsto gxH. \end{aligned}$$

$H \in Q_H$ et $\Omega_H = \{gH; g \in G\} = Q_H$, par suite, G opère transitivement sur Q_H . Soit E un G -ensemble homogène; on a $E = \Omega_x$, quel que soit $x \in E$.

D'autre part, d'après le théorème (5.19), Ω_x est équipotent à $\left(\frac{G}{G_x} \right)_g$, d'où E équipotent à Q_{G_x} .

Définition (5.33) : Soit G un groupe opérant sur un ensemble E . On dit que G opère *fidèlement* sur E , si

$$(g \in G \text{ et } g.x = x, \forall x \in E) \Rightarrow g = e;$$

autrement dit, si le morphisme de groupes $\gamma : G \rightarrow S_E$, tel que $\gamma_g(x) = g.x$ pour tout $x \in E$, est *injectif*. $g \mapsto \gamma_g$

Remarque (5.34) : Si G opère fidèlement sur un ensemble E , alors G est isomorphe à un sous-groupe de S_E .

Exemple (5.35) :

1° G opère fidèlement sur G , par translation à gauche.

2° G n'opère pas fidèlement sur G , par conjugaison.

3 — Sous-ensemble des points fixes d'un G -ensemble

Définition (5.36) : Soit G un groupe opérant sur un ensemble E ; la partie de E définie par :

$$E_G = \{x \in E; g.x = x, \forall g \in G\} \quad (12)$$

est appelée *sous-ensemble des points fixes* du G -ensemble E . (E_G est noté $\text{Fix}_E(G)$, dans certains ouvrages.)

Remarques (5.37) :

1° Compte tenu de (12), il est immédiat que :

$$E_G = \{x \in E; G_x = G\} \quad (13)$$

$$\text{d'où } E_G = \{x \in E; \Omega_x = \{x\}\} \quad (14)$$

2° E_G peut être vide. En particulier, si $|E| \neq 1$ et si $G \neq (e)$ opère transitivement sur E , alors $E_G = \emptyset$.

Exemples (5.38) :

1° G opère sur G par conjugaison :

$$\Omega_x = \{x\} \Leftrightarrow x \in Z(G) \text{ (remarque (5.23))}$$

donc $G_G = Z(G)$.

2° Considérons $G \leq S_4$ et G opérant de façon naturelle sur $E = \{1, 2, 3, 4\}$.

— Si $G = \langle (1, 2, 3) \rangle$, alors $E_G = \{4\}$.

— Si $G = \langle (1, 2)(3, 4) \rangle$, alors $E_G = \emptyset$.

Remarque (5.39) : Si un groupe G opère sur un ensemble E , si K est un sous-groupe de G , alors K opère sur E par la restriction de l'action de G :

$$\begin{aligned} K \times E &\rightarrow E \\ (k, x) &\mapsto k.x. \end{aligned}$$

— Si, pour $x \in E$, K_x désigne le stabilisateur de x dans K et G_x le stabilisateur de x dans G , alors :

$$K_x = G_x \cap K \quad (15)$$

Par ailleurs, $E_K = \{x \in E; K_x = K\}$, d'où

$$x \in E_K \Leftrightarrow K \leq G_x \quad (16)$$

— Si G opère fidèlement sur E , alors tout sous-groupe de G opère fidèlement sur E .

— Par contre, Si G opère transitivement sur E , un sous-groupe de G peut opérer intransitivement sur E .

En effet, on sait que, si H est un sous-groupe de G , G opère transitivement sur $Q_H = \left(\frac{G}{H}\right)_o$.

Considérons l'action sur Q_H d'un sous-groupe K de G .

K opère transitivement sur Q_H si et seulement si :

$$Q_H = \{gH; g \in G\} = \{kH; k \in K\} \quad (17)$$

(17) équivaut à : $(\forall g \in G, \exists k \in K, gH = kH)$.

On en déduit que K opère transitivement sur Q_H si et seulement si $G = KH$.

Les deux lemmes suivants seront à la base de la démonstration du second théorème de Sylow (chap. VI).

LEMME (5.40). Soit G un groupe fini d'ordre p^n , p étant un nombre premier et $n \geq 1$ dans \mathbb{N} . Si G opère sur un ensemble fini E , alors :

$$|E_G| \equiv |E| \pmod{p}.$$

Preuve : $x \in E_G \Leftrightarrow \Omega_x = \{x\}$ (relation 14).

$|E_G|$ est donc égal au nombre des G -orbites ponctuelles de E . Soient $\{\Omega_{x_i}\}_{1 \leq i \leq k}$ les G -orbites non ponctuelles de E ($k \in \mathbb{N}$); on a :

$$|E| = |E_G| + \sum_{i=1}^k |\Omega_{x_i}|.$$

Pour tout i ($1 \leq i \leq k$), $|\Omega_{x_i}| = [G : G_{x_i}]$ et $|\Omega_{x_i}| \neq 1$; on en déduit que $|\Omega_{x_i}|$ divise p^n et est de la forme p^{n_i} , $n_i \geq 1$ dans \mathbb{N} ; par suite $|E| - |E_G|$ est un multiple de p , d'où $|E_G| \equiv |E| \pmod{p}$.

LEMME (5.41). *Soient deux sous-groupes H et K d'un groupe G tels que $[G : H] = r$ ($r \in \mathbb{N}^*$) et $o(K) = p^n$, p étant un nombre premier ne divisant pas r et $n \geq 1$ dans \mathbb{N} ; alors K est contenu dans un conjugué de H .*

Preuve : Posons $E = \left(\frac{G}{H}\right)_o$; E est un ensemble fini de cardinal r . Considérons le groupe K comme opérant par translation à gauche sur E ; E_K étant l'ensemble des points fixes du K -ensemble E , d'après le lemme (5.40) :

$$|E_K| \equiv r \pmod{p}.$$

p ne divise pas r , par suite, on a $E_K \neq \emptyset$.

L'application de la relation (16), vue plus haut, donne :

$$xH \in E_K \Leftrightarrow K \leq G_{xH},$$

où G_{xH} est le stabilisateur de xH dans l'action de G sur E ; or $G_{xH} = xHx^{-1}$ (exemple (5.14) 5°), d'où

$$K \leq xHx^{-1}.$$

4 — Produit semi-direct

a) *Préliminaires :* Soient deux groupes H et N . Si H opère sur N par l'application :

$$\begin{aligned} H \times N &\rightarrow N \\ (h, x) &\mapsto h.x, \end{aligned}$$

nous poserons

$$h.x = x^h \quad (18)$$

Compte tenu de cette notation, les conditions (1) et (2) de la définition (5.1) s'écrivent :

$$\forall (h_1, h_2) \in H \times H, \forall x \in N, \quad x^{h_1 h_2} = (x^{h_2})^{h_1} \quad (1')$$

$$\forall x \in N, \quad x^e = x \quad (2')$$

Soit φ le morphisme du groupe H dans le groupe symétrique S_N , associé à l'action de H sur N :

$$\varphi : H \rightarrow S_N$$

$$h \mapsto \varphi_h,$$

où $\varphi_h(x) = x^h$, quel que soit $x \in N$.

Si, pour tout $h \in H$, $\varphi_h \in \text{Aut}(N)$, alors l'action de H sur N vérifie la condition supplémentaire :

$$\forall (x, y) \in N \times N, \forall h \in H, \quad (xy)^h = x^h y^h \quad (C)$$

Réciproquement, toute action de H sur N vérifiant la condition (C) est telle que, pour tout $h \in H$, $\varphi_h \in \text{Aut}(N)$, c'est-à-dire que :

La condition (C) équivaut à : $\text{Im } \varphi \leq \text{Aut}(N)$.

Exemple (5.42) :

1° Soit G un groupe considéré comme opérant sur lui-même par conjugaison :

$$G \times G \rightarrow G$$

$$(g, x) \mapsto gxg^{-1}.$$

Compte tenu des notations générales ci-dessus, pour g et x dans G , on a $\varphi_g(x) = x^g = gxg^{-1}$; φ_g est l'automorphisme intérieur de G défini par g .

La condition (C) est donc vérifiée.

On remarquera que l'action de G sur G par translation à gauche ne vérifie pas la condition (C), puisqu'une translation de G n'est pas un automorphisme, en général.

2° Soient A un anneau unitaire et U_A le groupe multiplicatif des éléments inversibles de A ; $(A, +)$ désignant le groupe additif abélien A , considérons l'application :

$$\begin{aligned} U_A \times (A, +) &\rightarrow (A, +) \\ (u, a) &\mapsto a^u = ua. \end{aligned}$$

Quels que soient a, a_1, a_2 dans A , quels que soient u, u_1, u_2 dans U_A , on a

$$u_1(u_2 a) = (u_1 u_2) a; \quad 1a = a$$

et
$$u(a_1 + a_2) = ua_1 + ua_2.$$

Ainsi le groupe U_A opère sur le groupe $(A, +)$ et cette action vérifie la condition (C).

3° N étant un groupe, soit $H \leq \text{Aut}(N)$; H opère sur N par :

$$\begin{aligned} H \times N &\rightarrow N \\ (h, x) &\mapsto x^h = h(x); \end{aligned}$$

$\varphi_h = h$, donc la condition (C) est vérifiée. Cette action est dite *action naturelle* de H sur N .

b) Produit semi-direct d'un sous-groupe normal par un autre sous-groupe.

Définition (5.43) : Etant donné un groupe G et deux sous-groupes H et N , on dira que G est *produit semi-direct de N par H* si :

- i) $N < G$
- ii) $G = NH$
- iii) $N \cap H = (e)$.

S'il en est ainsi, la condition $N < G$ implique que G opère sur N par conjugaison et par restriction, H opère sur N par conjugaison. Le morphisme φ associé à cette action est tel que, pour tout $h \in H$, φ_h est la restriction à N de l'automorphisme intérieur de G défini par h ; N étant normal dans G , $\varphi_h \in \text{Aut}(N)$.

On remarque de plus que, quels que soient x, y dans N et h, k dans H , on peut écrire dans $G = NH$:

$$xhyk = (xhyh^{-1})hk$$

$$xhyk = x\varphi_h(y)hk,$$

ou, en posant $hyh^{-1} = y^h$,

$$xhyk = xy^h hk \quad (19)$$

Définition (5.44) : Etant donné un groupe G et $N < G$, s'il existe un sous-groupe H de G , tel que G est produit semi-direct de N par H , alors H est appelé *complément* de N dans G .

Dans ce cas, l'application du second théorème d'isomorphisme (théorème (4.34)) donne $\frac{G}{N} \simeq H$.

Exemple (5.45) :

Soit D_n le groupe diédral d'ordre $2n$, engendré par a et b tels que $o(a) = n \geq 3$, $o(b) = 2$ et $o(ab) = 2$ (théorème (3.74)). Posons $\Gamma_n = \langle a \rangle$ et $\Gamma_2 = \langle b \rangle$; on a $\Gamma_n < D_n$, puisque $[D_n : \Gamma_n] = 2$, $D_n = \Gamma_n \Gamma_2$ et $\Gamma_n \cap \Gamma_2 = \langle e \rangle$, donc D_n est produit semi-direct de Γ_n par Γ_2 . On rappelle que D_2 est isomorphe au groupe de Klein $C_2 \times C_2$.

c) Produit semi-direct de groupes.

Soient H et N deux groupes; la donnée d'un morphisme $\varphi \in \text{Hom}(H, \text{Aut}(N))$ détermine une action de H sur N définie par :

$$\begin{aligned} H \times N &\rightarrow N \\ (h, x) &\mapsto \varphi_h(x), \end{aligned}$$

où φ_h désigne l'image de h par φ (voir remarque (5.4)); cette action vérifie nécessairement la condition (C), dans laquelle, selon la notation (18), $x^h = \varphi_h(x)$.

Considérons alors l'ensemble $N \times H$ muni de la loi de composition (multiplicative) telle que :

$$(x, h)(y, k) = (xy^h, hk), \quad (20)$$

quels que soient x, y dans N et h, k dans H .

Définition (5.46) : Compte tenu des données et des notations ci-dessus, l'ensemble $N \times H$ muni de la loi de composition (20) est noté $N \times_{\varphi} H$ et est appelé : *produit semi-direct de N par H relativement à φ* .

PROPOSITION (5.47). *Quels que soient les groupes H et N , pour tout $\varphi \in \text{Hom}(H, \text{Aut}(N))$, $N \times_{\varphi} H$ est un groupe non abélien, en général.*

Preuve : La formule (20) montre que la loi de composition qu'elle définit dans $N \times H$ est non commutative, en général.

Associativité : Soient x, y, z dans N et h, k, l dans H :

$$[(x, h)(y, k)](z, l) = (xy^h, hk)(z, l)$$

$$[(x, h)(y, k)](z, l) = (xy^h z^{hk}, hkl).$$

D'autre part :

$$(x, h)[(y, k)(z, l)] = (x, h)(yz^k, kl)$$

$$(x, h)[(y, k)(z, l)] = (xy^h z^{hk}, hkl), \text{ d'après (1'),}$$

$$\text{d'où } [(x, h)(y, k)](z, l) = (x, h)[(y, k)(z, l)].$$

Élément unité : Notons 1 l'élément unité de H et e celui de N ; quel que soit $(x, h) \in N \times H$, on a

$$(x, h)(e, 1) = (e, 1)(x, h) = (x, h),$$

donc $(e, 1)$ est élément unité dans $N \times_{\varphi} H$.

Inverse : Soit $(x, h) \in N \times H$, vérifions qu'il existe (y, k) dans $N \times H$ tel que :

$$(x, h)(y, k) = (y, k)(x, h) = (e, 1) \quad (21)$$

(21) équivaut à :

$$\text{et } \left. \begin{array}{l} xy^h = yx^k = e, \text{ dans } N \\ hk = kh = 1, \text{ dans } H \end{array} \right\}$$

On en déduit $k = h^{-1}$ et $y = (x^{-1})^{h^{-1}}$, d'où

$$(x, h)^{-1} = ((x^{-1})^{h^{-1}}, h^{-1}) \quad (22)$$

PROPOSITION (5.48). Soit $G = N \times_{\varphi} H$, alors les applications

$$\begin{array}{ll} \alpha : H \rightarrow G & \text{et} \quad \beta : N \rightarrow G \\ h \mapsto (e, h) & x \mapsto (x, 1) \end{array}$$

sont des monomorphismes de groupes.

Si $H' = \text{Im } \alpha$ et $N' = \text{Im } \beta$, alors G est produit semi-direct du sous-groupe N' par le sous-groupe H' .

En identifiant H à H' et N à N' au moyen des morphismes α et β , on obtient, dans G :

$$\varphi_h(x) = x^h = h x h^{-1},$$

quels que soient $x \in N$ et $h \in H$.

Preuve : On vérifie facilement que α et β sont des monomorphismes de groupes. Montrons que G est produit semi-direct de N' par H' .

— $N' \triangleleft G$: Soient $(x, 1) \in N'$ et $(y, k) \in G$,

$$(y, k)(x, 1)(y, k)^{-1} = (y x^k y^{-1}, 1) \text{ appartient à } N'.$$

— $G = N' H'$: $N' \triangleleft G$ implique que $N' H'$ est un sous-groupe de G (proposition (4.18)) et, d'autre part, tout $(x, h) \in G$ s'écrit $(x, h) = (x, 1)(e, h)$.

— $N' \cap H' = \langle (e, 1) \rangle$:

$$(x, h) \in N' \Leftrightarrow h = 1$$

$$(x, h) \in H' \Leftrightarrow x = e,$$

d'où $(x, h) \in N' \cap H' \Rightarrow (x, h) = (e, 1)$.

Identifier H à H' et N à N' au moyen de α et β revient à remplacer dans G , (e, h) par h et (e, x) par x , en posant, d'autre part, $(e, 1) = 1 = e$; dans ces conditions $(x, h) = (x, 1)(e, h)$ s'écrit simplement xh et la multiplication dans G se trouve définie par :

$$x h y k = x y^h h k \quad (23)$$

quels que soient x, y dans N et h, k dans H .

En particulier, pour tout $x \in N$ et tout $h \in H$, on obtient (en écrivant $h x h^{-1} = 1 h x h^{-1}$) :

$$\varphi_h(x) = x^h = h x h^{-1} \quad (24)$$

Remarque (5.49) : Si $\varphi \in \text{Hom}(H, \text{Aut}(N))$ est tel que $\varphi(h) = \text{id}_N$, quel que soit $h \in H$, alors $N \times_{\varphi} H = N \times H$, groupe produit direct de N et H .

Exemples (5.50) :

1° Soient C_2 et C_n deux groupes cycliques d'ordres respectifs 2 et $n \geq 3$.

Posons

$$C_n = \langle a \rangle, \quad C_2 = \langle b \rangle \quad \text{où } b^2 = 1$$

et soit $\varphi : C_2 \rightarrow \text{Aut}(C_n)$

tel que $\varphi_1 = \text{id}_{C_n}$ et $\varphi_b(x) = x^{-1}$, quel que soit $x \in C_n$

C_n étant abélien, φ_b est un automorphisme et φ est alors un morphisme de groupes.

De la proposition (5.48), on déduit que $C_n \times_{\varphi} C_2$ s'identifie au groupe diédral D_n (voir exemple (5.45)).

2° Soit N un groupe et $H = \text{Aut}(N)$. Si ϵ désigne l'application identique de $\text{Aut}(N)$, alors le groupe :

$$N \times_{\epsilon} \text{Aut}(N)$$

est appelé l'*holomorphe de N* et est noté $\text{Hol}(N)$.

Selon la proposition (5.48), en identifiant N à un sous-groupe de $\text{Hol}(N)$, on obtient $N \triangleleft \text{Hol}(N)$ et, quels que soient $x \in N$ et $g \in \text{Aut}(N)$, on a, dans $\text{Hol}(N)$,

$$g(x) = x^g = gxg^{-1},$$

car $g = \epsilon(g)$. On en déduit que tout automorphisme de N s'obtient par la restriction à N d'un automorphisme intérieur de $\text{Hol}(N)$.

Remarque (5.51) :

1° L'intérêt de la notion de produit semi-direct de groupes est de fournir une méthode de construction de nouveaux groupes, à partir de groupes connus et c'est ainsi que l'on peut mettre en évidence l'existence de certaines familles de groupes (voir, par exemple, l'exercice 23, chap. V).

2° L'exemple du groupe diédral considéré comme produit semi-direct de groupes cycliques montre qu'un produit semi-direct de groupes abéliens n'est pas, en général, abélien.

Remarque (5.52) : Par analogie avec le cas d'un groupe H opérant sur un groupe N , de telle sorte que le morphisme $\varphi : H \rightarrow S_N$ associé à cette action vérifie la condition $\text{Im } \varphi \leq \text{Aut}(N)$ (voir les préliminaires de ce paragraphe), on peut envisager l'action d'un groupe G opérant sur un ensemble E muni d'une structure algébrique autre que celle de groupe. En particulier, si E est

un espace vectoriel, si G opère sur E de telle sorte que le morphisme $\rho : G \rightarrow S_E$ associé à cette action vérifie la condition $\text{Im } \rho \leq \text{GL}(E)$, alors le couple (ρ, E) , où ρ est considéré comme morphisme de groupes de G dans $\text{GL}(E)$, définit ce qu'on appelle *une représentation linéaire de G* (à rapprocher de la notion de représentation matricielle d'un groupe, considérée dans l'exercice 25, chap. I).

La théorie de la représentation linéaire des groupes ne sera pas développée dans ce livre; signalons, cependant, que cette théorie a fourni de puissantes méthodes de démonstration pour l'étude des groupes (en particulier des groupes finis) et qu'elle s'est révélée avoir, aussi, des applications dans certains domaines de la physique et en chimie structurale, ce qui en a renforcé l'intérêt (voir par exemple [66] et [55]).

Exercices Chapitre V

- 1) a, b, c étant des nombres réels, soit

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}; ac \neq 0 \right\}.$$

Vérifier que G est un sous-groupe de $\text{GL}(2, \mathbb{R})$ et que G opère sur \mathbb{R} par l'application

$$\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, x \right) \mapsto \frac{ax + b}{c}.$$

Déterminer le noyau de l'action de G sur \mathbb{R} , ainsi que le stabilisateur et la G -orbite de 0.

- 2) Soit G un groupe fini opérant sur un ensemble fini E .

a) On suppose que l'action de G sur E est telle que $E_G = \emptyset$, E_G étant l'ensemble des points fixes de E .

Si $|G| = 15$ et $|E| = 17$, trouver le nombre de G -orbites et le cardinal de chacune d'elles.

b) Montrer que, si $|G| = 33$ et $|E| = 19$, alors nécessairement E_G est non vide.

- 3) Soit G un sous-groupe du groupe symétrique S_4 ; on considère G comme opérant de façon naturelle sur $N_4 = \{1, 2, 3, 4\}$.

Pour chacun des groupes G suivants, déterminer la décomposition de N_4 en G -orbites et le stabilisateur de chaque élément de N_4 .

$$G = \langle (1, 2, 3) \rangle; \quad G = \langle (1, 2), (3, 4) \rangle; \quad G = A_4.$$

- 4) Soit $G = GL(2, \mathbb{R})$; $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \text{ réels, } ad - bc \neq 0 \right\}$.

Soit $\mathbb{R}^2 = \{(x, y); x, y \text{ réels}\}$.

A tout couple d'éléments $\left((x, y), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)$ de $\mathbb{R}^2 \times G$ on associe le produit de matrices $(x, y) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ax + cy, bx + dy)$.

a) Prouver que le groupe G opère ainsi, à droite, sur l'espace vectoriel \mathbb{R}^2 .

b) Soit \mathcal{D} l'ensemble des droites de l'espace vectoriel \mathbb{R}^2 .

$$D \in \mathcal{D} \Leftrightarrow D = \{(ax, \beta x); x \in \mathbb{R}, \alpha \text{ et } \beta \text{ fixés dans } \mathbb{R}\}.$$

Vérifier que G opère à droite sur \mathcal{D} .

Si $D = (2x, x)$ déterminer G_D et Ω_D .

c) Soit H le sous-groupe de G engendré par les matrices $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

— Vérifier que H est un groupe fini d'ordre 8.

— On considère H comme opérant à droite sur \mathcal{D} .

Pour $D = (2x, x)$, trouver H_D et la H -orbite de D .

- 5) Soit Γ le sous-groupe de $GL(2, \mathbb{R})$ défini par :

$$\Gamma = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}; a > 0, b > 0 \right\}.$$

On considère Γ comme opérant à droite sur l'espace vectoriel \mathbb{R}^2 (voir l'exercice 4 ci-dessus).

Déterminer les stabilisateurs $\Gamma_{(0,0)}$, $\Gamma_{(1,1)}$, $\Gamma_{(0,1)}$.

Trouver toutes les Γ -orbites de \mathbb{R}^2 et vérifier ainsi qu'il y en a 9.

- 6) L'objet de cet exercice est de prouver que le groupe alterné A_n est simple pour $n \geq 5$.

1° Soit $n \geq 2$ dans N ; on note C_r l'ensemble des r -cycles du groupe symétrique S_n ($2 \leq r \leq n$). Vérifier les propriétés suivantes :

- a) Le groupe S_n opère transitivement, par conjugaison sur C_r .
 b) Si $2 \leq r \leq n-2$, alors A_n opère aussi transitivement par conjugaison sur C_r (voir exercices 24 et 26, chap. III).

2° Soit $n \geq 5$ dans N . On suppose qu'il existe un sous-groupe H de A_n tel que $H \neq (e)$ et $H \triangleleft A_n$.

a) Montrer que, pour prouver la simplicité de A_n , il suffit de démontrer que H contient un 3-cycle.

Le but des questions qui suivent est donc de mettre en évidence l'existence d'un 3-cycle dans H .

b) Soient $\alpha \in A_n$ et $\sigma \in H$.

Vérifier que $\alpha^{-1} \sigma \alpha \sigma^{-1} \in H$; si $\alpha = (i, j, k)$, écrire $\alpha^{-1} \sigma \alpha \sigma^{-1}$ sous forme d'un produit de deux 3-cycles.

c) Soient $\tau \in H \setminus \{e\}$ et $i \in \text{supp}(\tau)$. On pose $j = \tau(i)$. Soit $k \in N_n \setminus \{i, j, \tau^{-1}(i)\}$; on pose $l = \tau(k)$.

En considérant $\alpha^{-1} \sigma \alpha \sigma^{-1}$ où $\alpha = (i, j, k)$, démontrer que H contient une permutation $\sigma \neq e$ telle que $|\text{supp}(\sigma)| \leq 5$.

Montrer que cette permutation σ est nécessairement : un 3-cycle, ou un 5-cycle, ou un produit de deux transpositions dont les supports sont disjoints.

En conclure que H contient un 3-cycle. [Dans le second cas, en posant $\sigma = (i, j, k, l, m)$ et $\alpha = (i, j, k)$, calculer $\alpha^{-1} \sigma \alpha \sigma^{-1}$; dans le troisième cas, poser $\sigma = (i, j)(k, l)$, en tenant compte de l'hypothèse $n \geq 5$, considérer $\beta = (i, j, m)$ où $m \in N_n \setminus \{i, j, k, l\}$ et calculer $\beta^{-1} \sigma \beta \sigma^{-1}$.]

- 7) Soit G un sous-groupe du groupe symétrique S_n ($n \geq 2$).

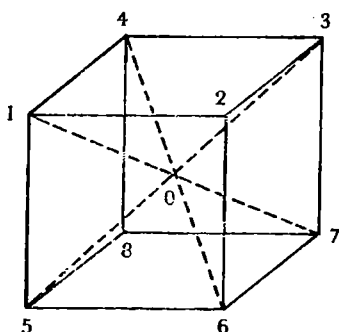
On suppose que G opère transitivement de façon naturelle sur $N_n = \{1, 2, \dots, n\}$.

a) Soit $H \triangleleft G$; H opère aussi de façon naturelle sur N_n .

Montrer que les H -orbites de N_n sont toutes de même cardinal.

b) Prouver que, si n est un nombre premier, alors H opère transitivement sur N_n .

- 8) Soit C un cube considéré comme solide indéformable et dont les sommets seront notés 1, 2, ..., 8 :



On appelle « groupe de symétries » du cube le groupe G des isométries de l'espace affine euclidien de dimension 3, qui conservent le cube.

On remarque que G peut être identifié à un sous-groupe du groupe symétrique S_8 .

$$a) \text{ Vérifier que } \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}$$

$$\text{et } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 3 & 1 & 5 & 8 & 4 \end{pmatrix}$$

définissent deux isométries appartenant à G .

b) Soit $H = \langle \alpha, \beta \rangle$ le sous-groupe de G engendré par α et β ; on considère H comme opérant de façon naturelle sur l'ensemble des sommets de C .

Déterminer la H -orbite de 1.

En déduire que G opère transitivement sur l'ensemble des sommets de C .

c) On remarquera que tout $\gamma \in G$ est une permutation des quatre diagonales a, b, c, d de C [$a = (1,7)$, $b = (2,8)$, $c = (3,5)$, $d = (4,6)$].

Déterminer alors, le stabilisateur G_1 de 1 dans l'action de G sur l'ensemble des sommets du cube.

[Vérifier que G_1 est le groupe engendré par la rotation d'angle $\frac{2\pi}{3}$ autour de a .]

En tenant compte du résultat de la question *b)*, trouver l'ordre du groupe G . En conclure que G s'identifie au groupe S_4 .

9) (Application des lemmes (5.40) et (5.41).)

a) Soit G un groupe fini; soit $H < G$ tel que $o(H) = p^r$, où p est un nombre premier, $r \geq 1$ dans N et p divise $[G:H]$.

On pose $E = \left(\frac{G}{H}\right)_g$ et on considère l'action de H par translation à gauche sur E ; E_H désignant l'ensemble des points fixes du H -ensemble E , prouver que

$$xH \in E_H \Leftrightarrow x \in N_G(H).$$

En déduire que p divise $[N_G(H) : H]$.

b) On suppose que $o(G) = p^n$, $n > 0$ dans N . Vérifier que :

$$H < G \Rightarrow H < N_G(H).$$

En conclure que, si $o(H) = p^{n-1}$, alors H est normal dans G .

10) Soit G un groupe opérant sur un ensemble E , par l'application

$$G \times E \rightarrow E$$

$$(g, x) \mapsto gx.$$

Pour $X \in \mathcal{P}(E)$, ensemble des parties de E , on pose

$$G_X = \{g \in G; gx = x, \forall x \in X\}$$

et $G_X^* = \{g \in G; gX = X\}.$

Prouver que a) $G_{gX} = gG_X g^{-1}$ et $G_{gX}^* = gG_X^* g^{-1}$

b) G_X et G_X^* sont des sous-groupes de G tels que $G_X \triangleleft G_X^*$.

c) Soit $x \in E$, posons $X = \Omega_x$, la G -orbite de x .

Montrer que, dans ce cas, on a $G_X \triangleleft G$ et que G_X est le noyau de l'action de G sur $X = \Omega_x$; en déduire que $\frac{G}{G_X}$ est isomorphe à un sous-groupe du groupe symétrique S_X .

11) (Application de l'exercice précédent.)

Soit G un groupe fini. On suppose que G opère *fidèlement* sur un ensemble fini E . Soit k le nombre des G -orbites de E , que l'on note X_1, X_2, \dots, X_k .

Pour tout i ($1 \leq i \leq k$), on pose

$$n = |X_i| \quad \text{et} \quad G_i = G_{X_i} = \{g \in G; gx = x, \forall x \in X_i\}.$$

D'après le c) de l'exercice 10, on a $G_i \triangleleft G$.

Pour tout i ($1 \leq i \leq k$) on note π_i l'épimorphisme canonique $G \rightarrow \frac{G}{G_i}$. En considérant :

$$\varphi = G \rightarrow \frac{G}{G_1} \times \frac{G}{G_2} \times \dots \times \frac{G}{G_k}$$

$$x \mapsto (\pi_1(x), \pi_2(x), \dots, \pi_k(x)).$$

Prouver que G est isomorphe à un sous-groupe de

$$S_{n_1} \times S_{n_2} \times \dots \times S_{n_k}.$$

- 12) Soient G un groupe fini et H un sous-groupe de G tel que $[G : H] = n$. Prouver que G contient un sous-groupe K tel que $K \triangleleft G$, $K \subseteq H$ et $[G : K]$ divise $n!$.
- 13) Soit G un groupe fini considéré comme opérant sur lui-même par conjugaison. Soit k le nombre des classes de conjugaison de G . On suppose $G \neq (e)$ et on désigne par p le plus petit nombre premier divisant l'ordre de G . Démontrer que $k > \frac{o(G)}{p}$ implique $Z(G) \neq (e)$.
- 14) L'objet de cet exercice est la détermination du nombre des classes de conjugaison du groupe symétrique S_n ($n \geq 2$).

Soit $\sigma \in S_n$ décomposé en un produit de cycles disjoints :

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_t \quad \text{tels que} \quad \sum_{i=1}^t \text{long } \gamma_i = n \quad (\text{remarque (3.58)}).$$

On pose $n_i = \text{long } \gamma_i$ ($1 \leq i \leq t$).

a) Vérifier qu'il est toujours possible d'écrire $\sigma = \gamma_1 \gamma_2 \dots \gamma_t$ de telle façon que l'on ait $1 \leq n_1 \leq n_2 \leq \dots \leq n_t$.

Ainsi tout $\sigma \in S_n$ détermine une suite d'entiers positifs (n_1, n_2, \dots, n_t) telle que $n_1 \leq n_2 \leq \dots \leq n_t$ et $\sum_{i=1}^t n_i = n$. Une telle suite est appelée une *partition* de n .

b) γ et γ' étant deux cycles dans S_n , prouver que :

$$\gamma \text{ et } \gamma' \text{ sont conjugués dans } S_n \Leftrightarrow \text{long } \gamma = \text{long } \gamma'.$$

En déduire que deux permutations σ et σ' sont conjuguées dans S_n si et seulement si elles déterminent la même partition de n .

En conclure que le nombre des classes de conjugaison de S_n est égal au nombre des partitions de n , noté $p(n)$. (Ce nombre $p(n)$

définit une fonction arithmétique $p: \mathbb{N}^* \rightarrow \mathbb{N}^*$ bien connue en théorie des nombres [36]. On pourra vérifier en particulier que $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$, $p(6) = 11$.

15) Soient r et n dans \mathbb{N} tels que $2 \leq r \leq n$.

a) Vérifier que dans S_n , une permutation σ commute avec le r -cycle $\gamma = (1, 2, \dots, r)$, si et seulement si $\sigma = \gamma^k \circ \tau$, où $k \in \{1, 2, \dots, r\}$, $\tau \in S_n$ et laisse fixe $1, 2, \dots, r$. [Voir exercice 24, chap. III.]

Quel est le nombre des permutations qui commutent avec γ ?

b) Démontrer que le nombre de r -cycles dans S_n est $\frac{1}{r} \frac{n!}{(n-r)!}$.

16) Soit $n \geq 4$ dans \mathbb{N} .

a) Quelle est la forme des éléments qui commutent avec $(1, 2) (3, 4)$ dans S_n ?

b) Quel est le nombre de conjugués de $(1, 2) (3, 4)$ dans S_n ?

17) (Formule de Burnside ⁽¹⁾ [10].)

a) Principe de dénombrement : soient X et Y deux ensembles finis et soit $S \subseteq X \times Y$ on pose

$$S(a, \cdot) = \{(x, y) \in S; x = a\} \quad \text{et} \quad S(\cdot, b) = \{(x, y) \in S; y = b\}.$$

Vérifier que les familles $\{S(a, \cdot); a \in X\}$ et $\{S(\cdot, b); b \in Y\}$ forment deux partitions de S , en déduire que

$$|S| = \sum_{a \in X} |S(a, \cdot)| = \sum_{b \in Y} |S(\cdot, b)|.$$

b) Soit G un groupe fini opérant sur un ensemble fini E , par l'application :

$$\begin{aligned} G \times E &\rightarrow E \\ (g, x) &\mapsto gx. \end{aligned}$$

On note t le nombre des G -orbites de E et pour tout $g \in G$, on pose

$$F(g) = \{x \in E; gx = x\}.$$

⁽¹⁾ William Snow Burnside, mathématicien américain (1852-1927).

— Soit $S = \{(g, x) \in G \times E; gx = x\}$; compte tenu de a), vérifier que $S(g, \cdot) = F(g)$ et $S(\cdot, x) = G_x$ (stabilisateur de x) et en déduire que

$$\sum_{g \in G} |F(g)| = \sum_{i=1}^t \sum_{x \in \Omega_{x_i}} |G_x|,$$

où les Ω_{x_i} ($1 \leq i \leq t$) sont les G -orbites de E .

— Prouver alors que

$$\sum_{g \in G} |F(g)| = \sum_{i=1}^t |\Omega_{x_i}| |G_{x_i}|;$$

en conclure que

$$\sum_{g \in G} |F(g)| = t |G| \quad (\text{formule de Burnside}).$$

c) Ecrire la formule ci-dessus, dans le cas où G opère transitivement sur E .

- 18) Soit G un groupe fini opérant *transitivement* sur un ensemble fini E (les notations sont celles de l'exercice 17).

a) Démontrer que le nombre des G_x -orbites de E est indépendant de x ; on note r ce nombre.

b) Compte tenu des résultats de l'exercice précédent, vérifier que

$$r |G| = \sum_{x \in E} \sum_{g \in G_x} |F(g)| = \sum_{g \in G} \sum_{x \in F(g)} |F(g)|,$$

en conclure que :

$$r |G| = \sum_{g \in G} |F(g)|^2.$$

- 19) Soit G un groupe opérant sur un ensemble E ; on dit que G est k -transitif sur E , $k \geq 1$ dans \mathbb{N} , si, quels que soient les k -tuples ordonnés (x_1, x_2, \dots, x_k) et (y_1, y_2, \dots, y_k) , chacun d'eux étant formé d'éléments distincts dans E , il existe $g \in G$ tel que, pour tout i ($1 \leq i \leq k$), $gx_i = y_i$.

a) Vérifier que, si G est k -transitif sur E , $k \geq 2$, alors, G est 1-transitif sur E , c'est-à-dire transitif sur E .

b) Pour $k \geq 2$, prouver que G est k -transitif sur E , si et seulement si, quel que soit $x \in E$, G_x est $(k-1)$ -transitif sur $E \setminus \{x\}$.

c) On suppose que le groupe G et l'ensemble E sont *finis* et que G opère k -transitivement sur E , $k \geq 2$.

— A l'aide des résultats des exercices 17 et 18 précédents, montrer que

$$|G| = \sum_{g \in G} |F(g)| \quad \text{et} \quad 2|G| = \sum_{g \in G} |F(g)|^2.$$

— Si $|E| = n$, démontrer que $|G|$ est divisible par $n(n-1) \dots (n-k+1)$. [On pourra partir de l'égalité $|G| = n|G_x|$.]

20) Pour $n \geq 2$ dans N , on considère le groupe symétrique S_n opérant de façon naturelle sur $N_n = \{1, 2, \dots, n\}$.

a) Prouver que S_n est n -transitif sur N_n .

b) Démontrer que pour $n \geq 3$, A_n est $(n-2)$ -transitif sur N_n . [Procéder par récurrence sur n et vérifier, en considérant les $(n-1)$ -tuples $(1, 2, \dots, n-2, n-1)$ et $(1, 2, \dots, n-2, n)$, que A_n n'est pas $(n-1)$ -transitif sur N_n .]

21) a) Pour $n \geq 2$ dans N , on pose $Z_n = \frac{Z}{nZ}$; vérifier que l'on a

$D_n \simeq Z_n \times_{\varphi} Z_2$, où φ est un morphisme de groupes de Z_2 dans $\text{Aut}(Z_n)$, que l'on précisera (voir exemple (5.50)).

b) D_{∞} désignant le groupe diédral infini (exercice 35, chap. IV), montrer que l'on a $D_{\infty} \simeq Z \times_{\varphi} Z_2$, où le morphisme $\varphi \in \text{Hom}(Z_2, \text{Aut}(Z))$ est à préciser.

22) N_1 et N_2 étant des groupes, prouver que :

$$N_1 \simeq N_2 \Rightarrow \text{Hol}(N_1) \simeq \text{Hol}(N_2)$$

(voir exemples (5.50) et exercice 32, chap. I).

23) N étant un groupe, soit $H \leq \text{Aut}(N)$. On considère l'action naturelle de H sur N et on note i l'injection canonique de H dans $\text{Aut}(N)$.

a) Vérifier que $N \times_i H$ est un sous-groupe de $\text{Hol}(N)$.

b) Compte tenu des exercices 21 ci-dessus et 17, chap. IV, montrer que, pour $n \geq 3$, D_n est isomorphe à un sous-groupe de $\text{Hol}(Z_n)$ et que D_{∞} est isomorphe à $\text{Hol}(Z)$.

24) G étant un groupe, soit $\lambda \in \text{End}(G)$ tel que $\lambda \circ \lambda = \lambda$. Si $K = \text{Ker } \lambda$ et $L = \text{Im } \lambda$, démontrer que G est produit semi-direct de K par L .

Vérifier que K est le sous-groupe normal de G engendré par $\{g\lambda(g^{-1}), g \in G\}$.

25) Soit $H = \langle h \rangle$ un groupe cyclique d'ordre 4 et $N = \langle x \rangle$ un groupe cyclique d'ordre $2n$, $n \geq 2$ dans N .

a) Vérifier qu'il existe un unique morphisme

$$\varphi \in \text{Hom}(H, \text{Aut}(N)) \quad \text{tel que } \varphi_h(x) = x^h = x^{-1},$$

quel que soit $x \in N$. On pose alors $G = N \rtimes_{\varphi} H$.

b) $Z(G)$ désignant le centre du groupe G , démontrer les propriétés :

$$Z(G) = \langle x^n \rangle \times \langle h^2 \rangle \simeq C_2 \times C_2 \quad \text{et} \quad \frac{G}{Z(G)} \simeq D_n.$$

c) Soit $K = \langle x^n h^2 \rangle$; vérifier que $K \triangleleft G$.

$$\text{On pose } \bar{G} = \frac{G}{K}, \quad \bar{H} = \frac{HK}{K}, \quad \bar{N} = \frac{NK}{K}.$$

Prouver que \bar{H} , \bar{N} , \bar{G} sont tels que :

$$\bar{H} \leq \bar{G} \quad \text{et} \quad \bar{H} \simeq C_4; \quad \bar{N} < \bar{G} \quad \text{et} \quad \bar{N} \simeq C_{2n};$$

$$\bar{G} = \bar{N}\bar{H}, \quad |\bar{N} \cap \bar{H}| = 2, \quad |\bar{G}| = 4n.$$

Le groupe \bar{G} ainsi défini est appelé : *groupe dicyclique d'ordre $4n$* .

d) Soit $\overline{Z(G)} = \frac{Z(G)}{K}$; montrer que $\overline{Z(G)} = Z(\bar{G})$.

Déterminer l'ordre de $Z(\bar{G})$; en conclure que \bar{G} est non abélien.

$$\text{Prouver que } \frac{\bar{G}}{Z(\bar{G})} \simeq \frac{G}{Z(G)}.$$

e) Vérifier que \bar{G} n'a qu'un seul élément d'ordre 2; en déduire que $\bar{G} \not\simeq D_{2n}$.

Prouver que $n = 2$ implique $\bar{G} \simeq Q_8$ (groupe des quaternions).

f) On note désormais Q_{4n} le groupe dicyclique d'ordre $4n$ ($n \geq 2$). Compte tenu des résultats précédents, vérifier que, dans $\bar{G} = Q_{4n}$, on peut identifier \bar{N} à N et \bar{H} à H ; en déduire que Q_{4n} peut être considéré comme engendré par deux éléments x et h tels que :

$$o(x) = 2n, \quad o(h) = 4, \quad x^n h^{-2} = e, \quad x^{-1} = hxh^{-1}.$$

26) Soit E un espace vectoriel non nul; S_E , $L(E)$, $GL(E)$ désignent, respectivement, le groupe symétrique, l'anneau des endomorphismes linéaires et le groupe linéaire général de E .

a) Pour $f \in L(E)$ et $a \in E$, on note $(f; a)$ l'application :

$$(f; a) : E \rightarrow E$$

$$x \mapsto f(x) + a.$$

Prouver que $(f; a) \in S_E$, si et seulement si $f \in GL(E)$.

b) Soit $\mathcal{A}(E) = \{(f; a); f \in GL(E), a \in E\}$.

— Vérifier que l'on a $\mathcal{A}(E) \leq S_E$ et $GL(E) \leq \mathcal{A}(E)$.

$\mathcal{A}(E)$ est le groupe affine de E .

— Soit $\mathcal{E}(E)$ l'ensemble des translations de E :

$$\mathcal{E}(E) = \{(e; a); e = \text{id}_E, a \in E\}.$$

Prouver les propriétés : $\mathcal{E}(E) \triangleleft \mathcal{A}(E)$ et $\mathcal{E}(E) \simeq (E, +)$.

c) On identifie $\mathcal{E}(E)$ à $(E, +)$ en posant $(e; a) = a$ et on écrit fa à la place de $(f; a)$; démontrer alors que $\mathcal{A}(E)$ est produit semi-direct de $(E, +)$ par $GL(E)$.

- 27) Etant donné deux groupes G et G' opérant, respectivement, sur deux ensembles E et E' , on dira que les actions de G sur E et G' sur E' sont *équivalentes*, s'il existe un isomorphisme θ de G sur G' et une bijection λ de E sur E' , tels que :

$$\theta(g) \cdot \lambda(x) = \lambda(g \cdot x), \quad \text{quels que soient } g \in G \text{ et } x \in E.$$

1° On suppose que les actions de G sur E et G' sur E' sont équivalentes; vérifier les propriétés suivantes :

a) quel que soit $x \in E$:

$$[G_x = \text{Stab}_G(x) \text{ et } G'_{\lambda(x)} = \text{Stab}_{G'}(\lambda(x))] \Rightarrow G_x \simeq G'_{\lambda(x)};$$

b) G transitif sur $E \Leftrightarrow G'$ transitif sur E' .

$$G \text{ transitif sur } E \Rightarrow G_x \simeq G'_y, \quad \forall (x, y) \in E \times E';$$

c) G opère fidèlement sur $E \Leftrightarrow G'$ opère fidèlement sur E' .

2° Soit G un groupe opérant *fidèlement* sur un ensemble E . Soit λ une bijection de E sur un ensemble E' . On note γ le morphisme de groupes de G dans S_E associé à l'action de G sur E :

$$\gamma : G \rightarrow S_E$$

$$g \mapsto \gamma_g, \quad \gamma_g(x) = g \cdot x, \quad \forall x \in E.$$

Vérifier que, pour tout $g \in G$, $\lambda \circ \gamma_g \circ \lambda^{-1} \in S_{E'}$ et que l'application :

$$\varphi : G \rightarrow S_{E'}$$

$$g \mapsto \lambda \circ \gamma_g \circ \lambda^{-1}$$

est un monomorphisme de groupes.

On pose $G' = \text{Im } \varphi$; montrer que l'action de G sur E est équivalente à l'action naturelle de G' sur E' .

CHAPITRE VI

Groupes finis. Théorèmes de Sylow

G étant un groupe fini d'ordre m , d'après le théorème de Lagrange (chap. II), tout sous-groupe de G a un ordre qui divise m . Par contre, si d est un entier positif divisant m , il n'existe pas nécessairement un sous-groupe de G , d'ordre d . Par exemple, le groupe alterné A_4 , d'ordre 12, n'a pas de sous-groupe d'ordre 6 (exercice 10, chap. IV).

Cependant, nous allons voir dans ce chapitre que, grâce au premier théorème de Sylow, on peut affirmer que, si le diviseur d de m est une puissance d'un nombre premier, alors le groupe G a au moins un sous-groupe d'ordre d . Le second théorème de Sylow donnera une indication sur le nombre de certains de ces sous-groupes.

Ces théorèmes, démontrés en 1872, sont fondamentaux en théorie des groupes finis.

1 — Théorèmes de Sylow

A / Premier théorème de Sylow ⁽¹⁾

THÉORÈME (6.1). *Soient G un groupe fini et p un nombre premier divisant l'ordre de G . Si $o(G) = sp^n$, avec s non divisible par p , alors pour tout entier r ($1 \leq r \leq n$), il existe un sous-groupe de G d'ordre p^r .*

⁽¹⁾ Peter Ludwig Mejdell Sylow, mathématicien suédois (1832-1918).

On connaît plusieurs démonstrations de ce théorème; celle qui est donnée ici date de 1959 [75], elle utilise la notion de groupe opérant sur un ensemble et s'appuie sur la remarque préliminaire suivante :

Remarque (6.2) : D'une façon générale, pour a et b entiers positifs, notons C_a^b le nombre de combinaisons de a éléments b à b . Autrement dit, si X est un ensemble fini de cardinal a , le nombre des parties de X de cardinal b est C_a^b . D'après un résultat d'analyse combinatoire [16] :

$$C_a^b = \frac{a(a-1) \dots (a-b+1)}{b!} = \frac{a!}{b!(a-b)!} \quad (1)$$

Compte tenu des notations du théorème (6.1), démontrons que pour tout entier r ($1 \leq r \leq n$), on a

$$C_{sp^n}^{pr} = \lambda p^{n-r}, \text{ où } \lambda \text{ est un entier non divisible par } p \quad (2)$$

D'après (1),

$$C_{sp^n}^{pr} = \frac{sp^n}{p^r} \cdot \frac{sp^n - 1}{1} \cdot \frac{sp^n - 2}{2} \dots \frac{sp^n - (p^r - 1)}{p^r - 1}$$

$$C_{sp^n}^{pr} = sp^{n-r} \cdot \frac{sp^n - 1}{1} \dots \frac{sp^n - (p^r - 1)}{p^r - 1}$$

$C_{sp^n}^{pr}$ étant un entier, il suffit de prouver que chaque fraction $\frac{sp^n - k}{k}$ est égale à une fraction irréductible dont ni le dénominateur, ni le numérateur n'est divisible par p .

Pour tout k ($1 \leq k \leq p^r - 1$), on peut écrire :

$$k = qp^\alpha, \text{ avec } 0 \leq \alpha \leq r \text{ et } q \text{ non divisible par } p \text{ dans } \mathbf{N},$$

$$\text{alors } \frac{sp^n - k}{k} = \frac{sp^n - qp^\alpha}{qp^\alpha} = \frac{sp^{n-\alpha} - q}{q};$$

p ne divise pas q , donc p ne divise pas $sp^{n-\alpha} - q$, ce qui implique la relation (2).

Preuve du théorème (6.1) : Etant donné un entier r ($1 \leq r \leq n$), notons \mathcal{F} l'ensemble des parties de G , de cardinal p^r .

D'après la remarque (6.2), \mathcal{F} est un ensemble fini de cardinal $C_{p^n}^{p^r}$ et en tenant compte de (2), on a

$$|\mathcal{F}| = \lambda p^{n-r}, \quad \text{où } \lambda \text{ est un entier, non divisible par } p.$$

Si $A \in \mathcal{F}$, pour tout $g \in G$, $|gA| = |A| = p^r$; par suite, G opère sur \mathcal{F} par translation à gauche.

Soit $\{A_i\}_{1 \leq i \leq k}$ une famille de représentants des G -orbites distinctes de \mathcal{F} ; le corollaire (5.21) implique :

$$|\mathcal{F}| = \sum_{i=1}^k [G : G_{A_i}],$$

où, pour tout i ($1 \leq i \leq k$), G_{A_i} est le stabilisateur de A_i dans G ; par suite, on a :

$$\sum_{i=1}^k [G : G_{A_i}] = \lambda p^{n-r}, \quad \lambda \text{ entier non divisible par } p.$$

On en déduit qu'il existe au moins un entier h ($1 \leq h \leq k$) tel que p^{n-r+1} ne divise pas $[G : G_{A_h}]$.

Posons alors $H = G_{A_h}$.

$$o(G) = sp^n \Rightarrow sp^n = o(H) [G : H].$$

Par hypothèse, p^{n-r+1} ne divise pas $[G : H]$, donc,

$$[G : H] = s' p^\alpha, \quad \text{où } s' \text{ divise } s \text{ et } 0 \leq \alpha \leq n - r, \text{ dans } \mathbf{N}.$$

En posant $s = s' s''$, on a $o(H) = s'' p^{n-\alpha}$;

$$0 \leq \alpha \leq n - r \Rightarrow r \leq n - \alpha \leq n,$$

par suite, p^r divise $o(H)$, d'où $p^r \leq o(H)$.

D'autre part, $H = G_{A_h}$, où $A_h \in \mathcal{F}$. Quels que soient g et g' dans G_{A_h} , on a

$$gA_h = g'A_h = A_h$$

et $g \neq g'$ implique $gx \neq g'x$, quel que soit $x \in A_h$.

On en déduit que $|G_{A_h}| \leq |A_h| = p^r$, c'est-à-dire $o(H) \leq p^r$, ce qui conduit à la conclusion : $o(H) = p^r$.

En appliquant le théorème (6.1) dans le cas $r = 1$, puis dans le cas $r = n$, on obtient les deux résultats suivants :

COROLLAIRE (6.3). (Théorème de Cauchy ⁽²⁾) :

G étant un groupe fini, si p est un nombre premier divisant l'ordre de G , alors G a au moins un élément d'ordre p .

COROLLAIRE (6.4). *Si G est un groupe fini d'ordre sp^n , où p est un nombre premier ne divisant pas s , alors G contient au moins un sous-groupe d'ordre p^n .*

Remarque (6.5) : Chronologiquement, le résultat de Cauchy a précédé celui de Sylow et on peut en trouver une démonstration directe dans [39], par exemple.

Définition (6.6) :

1° Si G est un groupe fini, on dit que G est un p -groupe, si $o(G) = p^n$, où p est un nombre premier et $n \in \mathbb{N}$.

2° Etant donné un groupe fini G et un nombre premier p divisant $o(G)$, un sous-groupe H de G est un p -sous-groupe de G , si $o(H) = p^r$, $r \geq 0$ dans \mathbb{N} .

3° Si G est un groupe fini d'ordre sp^n , où p est un nombre premier ne divisant pas s , alors tout sous-groupe d'ordre p^n de G est appelé : p -sous-groupe de Sylow de G .

B / Second théorème de Sylow

THÉORÈME (6.7). *Soient G un groupe fini et p un nombre premier divisant l'ordre de G ; alors,*

- 1° *tout p -sous-groupe de G est contenu dans un p -sous-groupe de Sylow de G ;*
- 2° *les p -sous-groupes de Sylow de G sont conjugués;*
- 3° *le nombre des p -sous-groupes de Sylow de G est congru à 1 modulo p et divise l'ordre de G .*

(²) Augustin-Louis Cauchy, mathématicien français (1789-1857).

La démonstration [61] que nous donnons de ce théorème s'appuie sur les lemmes (5.40), (5.41), et sur le suivant :

LEMME (6.8). *G étant un groupe fini, si S est un p-sous-groupe de Sylow de G, alors S est l'unique p-sous-groupe de $N_G(S)$.*

Preuve : Posons $o(G) = p^n s$, p ne divisant pas s .

On remarque que S est un p -sous-groupe de Sylow de tout sous-groupe de G contenant S; en particulier, S est un p -sous-groupe de Sylow de $N_G(S)$. Si $o(N_G(S)) = p^n s'$ et si K est un p -sous-groupe de Sylow de $N_G(S)$, on a $[N_G(S) : K] = s'$, p ne divisant pas s' . De l'application du lemme (5.41), avec $H = S$, on déduit qu'il existe $x \in N_G(S)$ tel que

$$K \leq xSx^{-1};$$

alors, $xSx^{-1} = S$ et $o(K) = o(S)$ implique $K = S$.

Preuve du théorème (6.7) : Comme ci-dessus, on pose $o(G) = p^n s$, p ne divisant pas s .

1° Soit H un p -sous-groupe de G; si S est un p -sous-groupe de Sylow de G, on a $[G : S] = s$; d'après le lemme (5.41) : il existe $x \in G$ tel que $H \leq xSx^{-1}$; mais $o(xSx^{-1}) = o(S)$, donc xSx^{-1} est un p -sous-groupe de Sylow de G.

2° Si S et S' sont deux p -sous-groupes de Sylow de G, le raisonnement ci-dessus montre qu'il existe $x \in G$ tel que $S' \leq xSx^{-1}$; xSx^{-1} étant un p -sous-groupe de Sylow de G, on a nécessairement $S' = xSx^{-1}$.

3° Soit \mathcal{S} l'ensemble des p -sous-groupes de Sylow de G. D'après le résultat précédent, G opère transitivement par conjugaison sur \mathcal{S} . Notons Ω_s la classe de conjugaison d'un élément $S \in \mathcal{S}$, alors :

$$|\mathcal{S}| = |\Omega_s| = [G : N_G(S)];$$

par suite, $|\mathcal{S}|$ divise $o(G)$ et, plus précisément, $|\mathcal{S}|$ divise $[G : S] = s$ puisque $[G : N_G(S)]$ divise $[G : S]$.

D'autre part, S opère sur \mathcal{S} par conjugaison; si \mathcal{S}_s désigne l'ensemble des points fixes du S-ensemble \mathcal{S} , d'après le lemme (5.40), on a

$$|\mathcal{S}| \equiv |\mathcal{S}_s| \pmod{p}.$$

$$\text{Or, } S' \in \mathcal{S}_S \Leftrightarrow S' = yS'y^{-1}, \quad \forall y \in S$$

$$S' \in \mathcal{S}_S \Leftrightarrow S \leq N_G(S').$$

Mais, d'après le lemme (6.8), $N_G(S')$ ne contient qu'un seul p -sous-groupe de Sylow S' ; on en déduit que

$$|\mathcal{S}_S| = 1, \quad \text{d'où } |\mathcal{S}| \equiv 1 \pmod{p}.$$

En résumé et en vue des applications pratiques, on retiendra que, si $o(G) = p^n s$, p premier ne divisant pas s et si n_p est le nombre des p -sous-groupes de Sylow de G , alors :

$$n_p \equiv 1 \pmod{p} \quad \text{et } n_p \text{ divise } s \tag{3}$$

Les propriétés suivantes sont la conséquence directe du 2° du théorème (6.7) :

COROLLAIRE (6.9). *Un groupe fini G a un unique p -sous-groupe de Sylow S , si et seulement si S est normal dans G .*

En particulier, dans un groupe fini abélien G , pour tout nombre premier p divisant l'ordre de G , il n'existe qu'un seul p -sous-groupe de Sylow.

2 — Quelques applications des théorèmes de Sylow

Le résultat suivant sera utilisé dans l'étude des groupes nilpotents finis (chap. VII).

LEMME (6.10) (G. Frattini). *Soit H un sous-groupe fini et normal d'un groupe G . Soit S un p -sous-groupe de Sylow de H , alors $G = HN_G(S)$.*

Preuve : Soit $g \in G$, alors $gSg^{-1} \leq gHg^{-1} = H$, et $|gSg^{-1}| = |S|$; par suite, gSg^{-1} est un p -sous-groupe de Sylow de H , donc est conjugué de S dans H , c'est-à-dire qu'il existe $h \in H$ tel que $gSg^{-1} = hSh^{-1}$, d'où $S = h^{-1}gSg^{-1}h$.

On en déduit que $h^{-1}g \in N_G(S)$, donc $g \in HN_G(S)$, par suite $G = HN_G(S)$.

COROLLAIRE (6.11). Soient G un groupe fini et S un p -sous-groupe de Sylow de G ; alors pour H , sous-groupe de G , on a :

$$N_G(S) \leq H \Rightarrow N_G(H) = H.$$

Preuve : $N_G(S) \leq H \leq G \Rightarrow S \leq H \leq G$.

S étant un p -sous-groupe de Sylow de G , S est aussi un p -sous-groupe de Sylow de H . D'autre part, on a $H < N_G(H)$; en appliquant le lemme (6.10) à H considéré comme sous-groupe de $N_G(H)$, on obtient :

$$N_G(H) = HN_G(S)$$

et $N_G(S) \leq H$ implique alors $N_G(H) = H$.

THÉORÈME (6.12). Soit G un groupe fini tel que $o(G) = pq$, où p et q sont deux nombres premiers distincts, tels que $q \not\equiv 1 \pmod{p}$; alors G a un unique p -sous-groupe de Sylow.

Preuve : Soit n_p le nombre des p -sous-groupes de Sylow de G ; d'après le second théorème de Sylow, on a $n_p \equiv 1 \pmod{p}$ et n_p divise $[G : S] = q$; l'hypothèse $q \not\equiv 1 \pmod{p}$ implique donc $n_p = 1$.

Remarque (6.13) : Si G est un groupe fini, non abélien, d'ordre p^n , où p est premier, alors G n'est pas simple.

En effet, d'après le théorème (5.27), le centre de G est un sous-groupe propre, différent de (e) et normal dans G .

PROPOSITION (6.14). Si G est un groupe simple, fini, non abélien et si p premier divise $o(G)$, alors le nombre n_p des p -sous-groupes de Sylow de G est plus grand que 1.

Preuve : Soit S un p -sous-groupe de Sylow de G ; on a $S \neq (e)$ et, d'après la remarque (6.13), S est nécessairement un sous-groupe propre de G . Si S était l'unique p -sous-groupe de Sylow de G , S serait normal dans G (corollaire (6.9)), ce qui est impossible, car G est simple; par suite on a $n_p > 1$.

PROPOSITION (6.15). *Si G est un groupe fini d'ordre pq , où p et q sont deux nombres premiers distincts, alors G n'est pas simple.*

Preuve : On peut supposer $p > q$; alors $q - 1$ n'est pas divisible par p ; d'après le théorème (6.12), G a un unique p -sous-groupe de Sylow S ; on a

$$(e) < S < G \quad \text{et} \quad S \triangleleft G \quad (\text{corollaire (6.9)}),$$

donc G n'est pas simple.

PROPOSITION (6.16). *Soient p et q deux nombres premiers distincts tels que $p \not\equiv 1 \pmod{q}$ et $q \not\equiv 1 \pmod{p}$; alors tout groupe d'ordre pq est cyclique.*

Preuve : Soit G un groupe fini tel que $o(G) = pq$. D'après le théorème (6.12) G a un unique p -sous-groupe de Sylow S et un unique q -sous-groupe de Sylow T ; on a $S < G$ et $T < G$.

S et T sont d'ordres premiers, donc ils sont cycliques; posons

$$S = \langle x \rangle \quad \text{et} \quad T = \langle y \rangle.$$

p et q étant premiers entre eux, $S \cap T = (e)$.

Montrons que x et y commutent :

$$[x, y] = x^{-1}y^{-1}xy,$$

alors $(S < G \text{ et } T < G) \Rightarrow [x, y] \in S \cap T$,

d'où $[x, y] = e$ et, par suite, $xy = yx$.

On en déduit que l'ordre de xy est pq , d'où $G = \langle xy \rangle$.

PROPOSITION (6.17). *Soit p un nombre premier impair. Si G est un groupe fini d'ordre $2p$, alors on a :*

$$G \simeq C_{2p} \quad \text{ou} \quad G \simeq D_p \quad (\text{groupe diédral}).$$

Preuve : p premier impair implique $p > 2$; $2 \not\equiv 1 \pmod{p}$, donc G a un unique p -sous-groupe de Sylow $S \simeq C_p$.

Le nombre n_2 des 2-sous-groupes de Sylow de G est congru à 1 modulo 2 et divise p , donc $n_2 = 1$ ou $n_2 = p$:

- si $n_2 = 1$, on vérifie que : $G \simeq C_p \times C_2 = C_{2p}$.
- si $n_2 = p$, S étant le p -sous-groupe de Sylow de G , soit $y \in G \setminus S$, alors :

$$(o(G) = 2p \text{ et } y \notin S) \Rightarrow o(y) = 2.$$

G a un unique sous-groupe cyclique S d'ordre $p > 2$, tel que $[G : S] = 2$ et tout élément de $G \setminus S$ est d'ordre 2 ; on en déduit que le groupe G d'ordre $2p$ est isomorphe au groupe diédral D_p .

THÉORÈME (6.18). *Soit un groupe fini $G \neq (e)$, tel que $o(G) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $k \geq 1$ dans \mathbf{N} , les p_i ($1 \leq i \leq k$) étant des nombres premiers distincts et les α_i des entiers strictement positifs. Si, pour tout i ($1 \leq i \leq k$), G a un unique p_i -sous-groupe de Sylow P_i , alors :*

$$G = P_1 P_2 \dots P_k \simeq \prod_{1 \leq i \leq k} P_i \quad (4)$$

Preuve : Pour tout i ($1 \leq i \leq k$), on a $P_i \triangleleft G$ (corollaire (6.9)) ; on en déduit que $H = P_1 P_2 \dots P_k$ est un sous-groupe normal de G et on vérifie que, d'après la proposition (1.88), H est isomorphe au produit direct des p_i -groupes P_i ($1 \leq i \leq k$) ; alors :

$$H \simeq \prod_{1 \leq i \leq k} P_i \Rightarrow o(H) = \prod_{1 \leq i \leq k} o(P_i) \Rightarrow o(H) = o(G),$$

d'où la relation (4).

COROLLAIRE (6.19). *Si $G \neq (e)$ est un groupe abélien fini, d'ordre $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $k \geq 1$ dans \mathbf{N} , les p_i ($1 \leq i \leq k$) étant des nombres premiers distincts et les α_i des entiers positifs non nuls, alors G est isomorphe au produit direct de ses p_i -sous-groupes de Sylow distincts.*

Remarque (6.20) : Si la loi de composition d'un groupe abélien fini $G \neq (e)$ est notée additivement, la relation (4) s'écrit :

$$G = P_1 \oplus P_2 \oplus \dots \oplus P_k.$$

Exercices Chapitre VI

- 1) Montrer que, si n est impair, alors tout sous-groupe de Sylow du groupe diédral D_n , d'ordre $2n$, est cyclique.
- 2) Déterminer les 2-sous-groupes de Sylow du groupe symétrique S_4 et vérifier que chacun d'eux est isomorphe au groupe diédral D_4 . [Remarquer que tout sous-groupe d'ordre 4 de S_4 est contenu dans un 2-sous-groupe de Sylow de S_4 .]
- 3) Prouver que tout sous-groupe d'ordre 35 est cyclique.
- 4) Montrer qu'un groupe d'ordre 42 n'est pas simple.
- 5) Soit G un groupe fini d'ordre 56. On note, respectivement, n_7 et n_2 le nombre des 7-sous-groupes de Sylow et celui des 2-sous-groupes de Sylow de G .
 - a) Vérifier que $n_7 = 1$ ou $n_7 = 8$.
 - b) Dans le cas où $n_7 = 8$, déterminer le nombre des éléments d'ordre 7 dans G et calculer n_2 .
 - c) Montrer que, dans tous les cas, G n'est pas simple.
- 6) Démontrer qu'il n'existe pas de groupe simple d'ordre 300. [G étant un groupe d'ordre 300, dans le cas où le nombre des 5-sous-groupes de Sylow H de G est plus grand que 1, considérer $[G : N_G(H)]$ et utiliser la remarque (5.16), chap. V, 2°.]
- 7) Soit G un groupe fini d'ordre $p^2 q$, où p et q sont deux nombres premiers distincts, tels que $p^2 \not\equiv 1 \pmod{q}$ et $q \not\equiv 1 \pmod{p}$. Démontrer que G est abélien. [On montrera que $G = H_p H_q$ où H_p et H_q sont, respectivement, un p -sous-groupe de Sylow et un q -sous-groupe de Sylow de G .]
- 8) Soit G un groupe fini d'ordre $p^2 q$, où p et q sont des nombres premiers distincts. Soit n_p (resp^t n_q) le nombre des p -sous-groupes (resp^t q -sous-groupes) de Sylow de G .
 En vue de prouver que $n_p = 1$ ou $n_q = 1$, on fait l'hypothèse contraire, c'est-à-dire que l'on suppose $n_p > 1$ et $n_q > 1$.
 - a) Montrer que :

$$n_p > 1 \Rightarrow q > p$$
 et

$$n_q > 1 \Rightarrow n_q = p \text{ ou } n_q = p^2.$$

b) En considérant le nombre des éléments d'ordre q dans G , montrer que $n_q = p$ implique $p > q$ et $n_q = p^2$ implique $n_p = 1$.

En déduire que nécessairement $n_p = 1$ ou $n_q = 1$; en conclure que le groupe G n'est pas simple.

- 9) Soit G un groupe d'ordre $p^n q$, où p et q sont des nombres premiers distincts et $n > 1$ dans \mathbb{N} . On suppose que G a un q -sous-groupe de Sylow Q tel que $N_G(Q) = Q$. Démontrer qu'il existe alors un unique p -sous-groupe de Sylow; en conclure que G n'est pas simple.
- 10) Soit G un groupe d'ordre pqr , où p, q, r sont des nombres premiers distincts. On suppose $p > q > r$ et on note, respectivement, n_p, n_q, n_r , le nombre des p -sous-groupes, q -sous-groupes, r -sous-groupes de Sylow de G .

a) En considérant les nombres d'éléments d'ordre, respectivement, p, q, r , dans G , démontrer l'inégalité :

$$pqr \geq n_p(p-1) + n_q(q-1) + n_r(r-1) + 1 \quad (1)$$

b) Prouver que l'hypothèse $n_p > 1, n_q > 1, n_r > 1$ implique : $n_p = qr, n_q \geq p, n_r \geq q$.

Montrer que ces résultats sont en contradiction avec l'inégalité (1); en conclure que le groupe G n'est pas simple.

- 11) 1° Soient G un groupe fini et H un sous-groupe de G tel que $[G : H] = p$, où p est le plus petit nombre premier divisant l'ordre de G . Soit K le noyau de l'action de G par translation à gauche sur $\left(\frac{G}{H}\right)_o$.

a) Justifier les propriétés suivantes :

- $[H : K]$ divise $p!$;
- si $[H : K] > 1$ et si q est un nombre premier divisant $[H : K]$, alors $q \geq p$.

b) Prouver que les deux propriétés précédentes sont contradictoires.

En déduire que H est normal dans G .

2° Soit G un groupe d'ordre 399.

a) Vérifier que G a un sous-groupe d'ordre 19, normal dans G .

b) Prouver que G a au moins un sous-groupe cyclique d'ordre 133, normal dans G [utiliser 1°].

Démontrer, alors, que G est un groupe cyclique.

- 12) Soit G un groupe; soit K un sous-groupe fini et normal de G . Si H est un p -sous-groupe de Sylow de K , normal dans K , prouver que H est normal dans G .
- 13) Soient G un groupe fini et $H \leq G$. Soit S' un p -sous-groupe de Sylow de H , prouver qu'il existe un p -sous-groupe de Sylow S de G tel que $S' = S \cap H$.

- 14) *Notations* : le cardinal d'un ensemble fini E est noté $|E|$, de même l'ordre d'un groupe fini G est noté $|G|$.

Soient p un nombre premier et G un groupe fini d'ordre $p^n s$, où $n \in \mathbb{N}^*$ et p ne divise pas s .

Le but de cet exercice est de prouver que *pour tout entier k , tel que $1 \leq k \leq n$, le nombre des sous-groupes de G d'ordre p^k est congru à 1 modulo p* ; d'après le second théorème de Sylow on sait que la propriété est vraie pour $k = n$, on supposera donc ici $1 \leq k < n$.

On pose $m = p^{n-k} s$, donc $|G| = p^k m$. Soit E l'ensemble des parties de G ayant p^k éléments.

1° a) Vérifier que G opère sur E par translation à gauche; pour $A \in E$, on note G_A le stabilisateur de A .

b) Montrer que, pour $A \in E$, G_A opère par translation à gauche sur A .

Vérifier que la G_A -orbite d'un élément $a \in A$ est la classe à droite de a modulo G_A . En déduire que, pour tout $A \in E$, $|G_A|$ divise p^k .

2° On pose

$$E_0 = \{A \in E; |G_A| = p^k\} \text{ et } E'_0 = \{B \in E; |G_B| = p^l, l < k\}.$$

a) Soient $B \in E'_0$ et Ω_B la G -orbite de B , relativement à l'action de G sur E , par translation à gauche.

Montrer que pm divise $|\Omega_B|$; en déduire que :

$$|E| \equiv |E_0| \pmod{pm}.$$

b) Soit $A \in E_0$ et $a \in A$; G_A étant le stabilisateur de A , considéré dans 1°, démontrer que

$$G_A a = A.$$

c) Soit H un sous-groupe d'ordre p^k de G et Hx une classe à droite modulo H , dans G .

Soit G_{Hx} le stabilisateur de Hx , dans l'action de G sur E , par translation à gauche.

Démontrer que $G_{Hx} = H$; en déduire que $Hx \in E_0$.

3° On désigne par λ le nombre des sous-groupes de G d'ordre p^k ; montrer que :

$$|E_0| = \lambda m;$$

en conclure que $\lambda \equiv \frac{|E|}{m} \pmod{p}$.

4° En remarquant que la classe de congruence de λ modulo p ne dépend pas de G , mais seulement de son ordre p^n et de l'entier k ($1 \leq k < n$), démontrer que λ est congru à 1 modulo p [prendre G cyclique d'ordre p^n].

15) (Application de l'exercice 14 ci-dessus.)

C_p désignant un groupe cyclique d'ordre premier p , déterminer le nombre des sous-groupes d'ordre p du groupe $G = C_p \times C_p$.

Dans le cas où $p = 3$, expliciter tous les sous-groupes d'ordre 3 de $C_3 \times C_3$.

16) Déterminer (à un isomorphisme près) tous les groupes finis d'ordre $n \leq 15$.

(Pour $k \geq 2$ dans N , C_k désigne un groupe cyclique d'ordre k et D_k un groupe diédral d'ordre $2k$; Q_8 est le groupe des quaternions.)

On note G un groupe quelconque d'ordre $n \leq 15$.

a) Considérer les cas $n = p$ (premier), $n = 2p$ (p premier impair), $n = pq$, p et q premiers tels que $p \not\equiv 1 \pmod{q}$ et $q \not\equiv 1 \pmod{p}$ [voir propositions (6.16) et (6.17)].

b) Montrer que $n = p^2$ (p premier) implique :

$$G \simeq C_{p^2} \quad \text{ou} \quad G \simeq C_p \times C_p.$$

[Considérer un sous-groupe H d'ordre p de G et le sous-groupe de G engendré par un élément $x \in G \setminus H$.]

c) Cas $n = 8$:

— Vérifier que, si G est abélien, alors G est isomorphe à C_8 , ou $C_2 \times C_4$, ou $C_2 \times C_2 \times C_2$.

[Considérer les 3 cas : il existe un élément d'ordre 8; il n'existe pas d'élément d'ordre 8, mais il existe un élément d'ordre 4; il n'existe pas d'élément d'ordre 4.]

— On suppose G non abélien; montrer que G a nécessairement un élément d'ordre 4 (exercice 5, chap. I).

Soit $a \in G$, un élément d'ordre 4; on pose $N = \langle a \rangle$. Prouver que $N \triangleleft G$ et en déduire que $b \in G \setminus N$ implique $b^2 \in N$ et plus précisément $b^2 = e$ ou $b^2 = a^2$. Démontrer alors, que :

$$(b^2 = e \Rightarrow G \simeq D_4) \quad \text{et} \quad (b^2 = a^2 \Rightarrow G \simeq Q_8).$$

d) Pour $n = 12$, soient, respectivement, n_2 et n_3 le nombre de 2-sous-groupes et des 3-sous-groupes de Sylow de G .

— Vérifier que les couples (n_2, n_3) éventuellement possibles sont $(1, 1)$, $(1, 4)$, $(3, 1)$, $(3, 4)$.

— Montrer que le cas $(n_2, n_3) = (3, 4)$ est impossible [considérer, en particulier, le nombre des éléments d'ordre 3].

— Cas $(n_2, n_3) = (1, 1)$: prouver que G est isomorphe à $C_4 \times C_3$, ou $C_2 \times C_2 \times C_3$ et qu'à un isomorphisme près il n'y a pas d'autre groupe abélien d'ordre 12.

— Cas $(n_2, n_3) = (1, 4)$: Soit N le 2-sous-groupe de Sylow de G ; prouver que nécessairement : $N \simeq C_2 \times C_2$.

Soit H un 3-sous-groupe de Sylow de G ; montrer que G est produit semi-direct de N par H .

En posant $N = \{e, a, b, ab\}$, où $a^2 = b^2 = e$ et $H = \{e, c, c^2\}$, démontrer que $ab = ba$, $ac = cb$, $bc = cab$, $abc = ca$; en déduire que $G \simeq A_4$ (voir exercice 10, chap. IV).

[On pourra écrire la table de multiplication de G .]

— Cas $(n_2, n_3) = (3, 1)$: Soit K le 3-sous-groupe de Sylow de G .

On pose $K = \{e, c, c^2\}$. Soit S un 2-sous-groupe de Sylow de G .

1) Si $S \simeq C_4$, on pose $S = \{e, a, a^2, a^3\}$; K étant normal dans G et G étant non abélien, vérifier les relations : $aca^{-1} \neq c$, $ca = ac^2$, $c^2a = ac$; en déduire que :

$$G = \{e, a, a^2, a^3, c, c^2, ac, a^2c, a^3c, ac^2, a^2c^2, a^3c^2\}.$$

Démontrer que G peut être considéré comme engendré par $x = a^2c$ et a , qui vérifient :

$$o(x) = 6, \quad o(a) = 4, \quad x^3a^{-2} = e, \quad x^{-1} = axa^{-1}.$$

En conclure que $G \simeq Q_{12}$ (groupe dicyclique d'ordre 12; voir exercice 25, chap. V).

2) Si $S \simeq C_2 \times C_2$, on pose $S = \{e, a, b, ab\}$, où $a^2 = b^2 = e$.

K étant normal dans G et G étant non abélien, prouver qu'il existe $x \in S$ tel que $xcx^{-1} \neq c$; on suppose que $x = a$. On pose $H = K \langle a \rangle$; vérifier que H est un sous-groupe de G , produit semi-direct de K par $\langle a \rangle$. En déduire que $H \simeq D_8$ (voir chap. V).

Démontrer qu'il existe $y \in S \setminus H$ tel que $ycy^{-1} = c$. (Si $bc b^{-1} = c$, on prend $y = b$; si $(ab)c(ab)^{-1} = c$, on prend $y = ab$.)

Prouver que, quel que soit $h \in H$, on a $hy = yh$; en déduire que $G = H \langle y \rangle \simeq D_8 \times C_2$.

Démontrer que $G \simeq D_8$.

e) En conclusion de l'étude précédente, on pourra écrire un tableau récapitulatif de la forme :

Ordre du groupe	1	2	3	...	15
Nombre de groupes commutatifs	1				
Nombre de groupes non commutatifs	0				
Nombre total de groupes	1				

17) Dans le groupe $GL(2, \mathbb{C})$, on considère les matrices

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^2 \end{pmatrix},$$

où $i^2 = -1$, $\varepsilon^3 = 1$, $\varepsilon \neq 1$.

a) Soit Γ le sous-groupe de $GL(2, \mathbb{C})$ engendré par A et B .

Démontrer que Γ est isomorphe au groupe dicyclique Q_{12} (exercice 25, chap. V), donc isomorphe au groupe G d'ordre 12, correspondant, dans l'exercice 16, ci-dessus, au cas $(n_2, n_3) = (3, 1)$ et $S \simeq C_4$.

b) Déterminer tous les sous-groupes cycliques de Γ , ou du groupe G de l'exercice 16, qui lui est isomorphe; en déduire que tous les sous-groupes du groupe dicyclique Q_{12} sont cycliques.

18) G étant un groupe fini, soient $H \triangleleft G$ et p un nombre premier divisant $[G : H]$. Démontrer que Σ est un p -sous-groupe de Sylow de $\frac{G}{H}$, si et seulement s'il existe un p -sous-groupe de Sylow S de G , tel que $\Sigma = \frac{SH}{H}$.

19) Un groupe fini G sera dit *hypercyclique* si tout sous-groupe de Sylow de G est cyclique.

1° Trouver des exemples de groupes hypercycliques non cycliques.

2° Prouver que tout sous-groupe et tout quotient d'un groupe fini hypercyclique est hypercyclique [utiliser les exercices 13 et 18 ci-dessus].

3° Démontrer que tout groupe abélien hypercyclique est cyclique.

4° Soit G un groupe fini hypercyclique non abélien, d'ordre $p^n s$, où p est premier, $n \geq 1$ et p ne divise pas s .

a) Si H et H' sont deux p -sous-groupes de G d'ordre p^r ($1 \leq r \leq n$), montrer que H et H' sont conjugués dans G .

b) Soit $N < G$ et $H \leq G$. On pose :

$$d = \text{PGCD}(|N|, |H|) \quad \text{et} \quad l = \text{PPCM}(|N|, |H|).$$

Si $d = p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}$, où les p_i ($1 \leq i \leq k$) sont des nombres premiers distincts et les δ_i des entiers positifs (non nuls), montrer que, pour tout i ($1 \leq i \leq k$), $p_i^{\delta_i}$ divise $|N \cap H|$.

En déduire que $|N \cap H| = d$ et $|NH| = l$.

c) Démontrer que $N < G$ implique N caractéristique dans G .

20) Soit p un nombre premier divisant l'ordre d'un groupe fini G ; soit n_p le nombre des p -sous-groupes de Sylow de G , on suppose $n_p > 1$.

On désigne par \mathcal{D} l'ensemble des p -sous-groupes H de G qui sont contenus dans au moins deux p -sous-groupes de Sylow de G , *distincts*. \mathcal{D} est non vide, car \mathcal{D} contient (e).

1° L'ensemble \mathcal{D} étant ordonné par l'inclusion, justifier l'existence, dans \mathcal{D} , d'au moins un élément *maximal* D . On pose $N = N_G(D)$.

2° a) Vérifier que p divise l'ordre de N .

b) Soient P et P' deux p -sous-groupes de Sylow de G , distincts, contenant D . Démontrer les relations : $D < N \cap P$ et $D < N \cap P'$ (voir exercice 9, chap. V).

c) Montrer qu'il existe des p -sous-groupes de Sylow Q et Q' de N tels que

$$N \cap P \leq Q \quad \text{et} \quad N \cap P' \leq Q'.$$

— Prouver que $D = Q \cap Q'$.

— En conclure que le nombre des p -sous-groupes de Sylow de N est plus grand que 1.

21) Soit G un groupe fini d'ordre $p^n s$, où p est premier, $n \geq \lambda$ et p ne divise pas s . On note E_p l'ensemble des p -sous-groupes de Sylow de G .

1° Soit $P = \bigcap_{S \in E_p} S$ prouver que P est un p -sous-groupe de G , normal dans G .

2° Soit \mathcal{S}_{E_p} le groupe symétrique de E_p . On sait que G opère sur E_p par conjugaison, on note γ le morphisme : $G \rightarrow \mathcal{S}_{E_p}$ défini par cette action.

a) Comparer $\text{Ker } \gamma$ et $\bigcap_{S \in E_p} N_G(S)$.

b) Prouver que le sous-groupe P , défini dans 1°, est l'unique p -sous-groupe de Sylow de $\text{Ker } \gamma$.

Dans toutes les questions qui suivent, on suppose $|E_p| = 1 + p$. S étant fixé dans E_p , on pose $S = S_0$ et on note S_1, S_2, \dots, S_p les autres éléments de E_p .

3° On considère S comme opérant sur E_p , par conjugaison. On note S_{S_i} le stabilisateur de S_i dans S , $0 \leq i \leq p$.

a) Quel est le sous-groupe S_{S_0} ? Vérifier que $i \neq 0$ implique $S_{S_i} \neq S$.

b) Déterminer le nombre des S -orbites de E_p et expliciter chacune d'elles.

En déduire que, pour $1 \leq i \leq p$, l'ordre du sous-groupe S_{S_i} est indépendant de i et calculer cet ordre.

c) Comparer S_{S_i} et $S \cap S_i$, pour $1 \leq i \leq p$. En déduire que $o(P) \leq p^{n-1}$.

4° a) Compte tenu de l'hypothèse $|E_p| = 1 + p$, montrer que :

$$o(G) = p^n(1 + p)r, \quad \text{où } r \text{ divise } s.$$

En déduire que : $o(N_G(S)) = p^n r$, quel que soit $S \in E_p$, et que $o(\text{Ker } \gamma) = p^m r'$, où r' divise r et $m \leq n-1$ dans N .

b) En considérant $[G : \text{Ker } \gamma]$, calculer m et en déduire $o(P)$.

En conclure que $P = S_i \cap S_j$, quels que soient $i \neq j$, $0 \leq i \leq p$, $0 \leq j \leq p$.

22) Soit G un groupe simple, d'ordre 60.

a) Calculer le nombre des 5-sous-groupes de Sylow de G ; en déduire que G a 24 éléments d'ordre 5.

b) Prouver que G n'a pas de sous-groupe d'ordre 15.

[Montrer que l'existence d'un sous-groupe d'ordre 15 impliquerait G isomorphe à un sous-groupe du groupe symétrique S_4 .]

c) Démontrer que G a 20 éléments d'ordre 3.

23) Soit G un groupe fini d'ordre $p^n s$, où p est premier, p ne divise pas s et $n \geq 1$ dans N .

a) Montrer que, si G est simple, alors p^n divise $(s-1)!$ (voir remarque (5.16) 2°).

b) Prouver qu'il n'existe pas de groupe simple d'ordre $2^n \times 5$, avec $n \geq 4$.

24) a) Prouver que, pour $2 \leq n \leq 4$, le groupe symétrique S_n n'a pas de sous-groupe simple, non abélien.

[Pour $n = 4$, voir la proposition (6.15) et l'exercice 23 ci-dessus.]

b) Vérifier que, si G est un groupe fini, simple, non abélien, alors : $H < G \Rightarrow [G : H] \geq 5$.

25) Soit $n \geq 5$ dans \mathbb{N} .

a) Montrer que : $(H < S_n, H \neq (e) \text{ et } H \neq S_n) \Rightarrow H = A_n$.
En déduire que $(H < S_n \text{ et } [S_n : H] = 2) \Rightarrow H = A_n$.

b) Soit $H < A_n$ tel que $[A_n : H] = n$.

En application de l'exercice 27, chapitre V, prouver que l'action de A_n sur $\left(\frac{A_n}{H}\right)_o$ définie par $(\alpha, \sigma H) \mapsto \alpha \sigma H$, quels que soient $\alpha \in A_n$ et $\sigma H \in \left(\frac{A_n}{H}\right)_o$, est équivalente à l'action naturelle d'un sous-groupe J de S_n sur $\{1, 2, \dots, n\}$. Vérifier que, nécessairement, $J = A_n$ (utiliser a)) et en considérant une bijection de $\left(\frac{A_n}{H}\right)_o$ sur $\{1, 2, \dots, n\}$, prouver que :

$$\text{Stab}_{A_n}(\sigma H) \simeq \text{Stab}_{A_n}(k), \forall \sigma H \in \left(\frac{A_n}{H}\right)_o, \forall k \in \{1, 2, \dots, n\};$$

en conclure que H est isomorphe à A_{n-1} .

c) Soit G un groupe simple, d'ordre 60.

— Soit S un 5-sous-groupe de Sylow de G ; prouver que $[G : N_G(S)] = 6$ (voir l'exercice 22 ci-dessus).

En déduire que G est isomorphe à un sous-groupe H de S_6 .

— Prouver que $H \leq A_6$ [montrer que, si H contenait une permutation impaire, alors H contiendrait un sous-groupe d'indice 2].

— Calculer $[A_6 : H]$; en conclure que G est isomorphe à A_5 .

(On peut démontrer, plus généralement, que si G est un groupe fini, non abélien et simple, d'ordre au plus égal à 100, alors G est isomorphe à A_5 [61].)

26) a) Prouver que le groupe des automorphismes intérieurs de S_3 est isomorphe à S_3 (voir proposition (5.9)).

Vérifier que tout automorphisme de S_3 est une permutation de $\{(1, 2), (2, 3), (1, 3)\}$; en déduire que $\text{Aut}(S_3) \simeq S_3$ et que $\text{Aut}(S_3) = \text{Int}(S_3)$.

b) Vérifier que le groupe symétrique S_4 a quatre 3-sous-groupes de Sylow, que l'on déterminera et que l'on notera P_i , $1 \leq i \leq 4$.

Montrer que tout automorphisme de S_4 est une permutation de l'ensemble $E = \{P_i; 1 \leq i \leq 4\}$.

Prouver que $\text{Int}(S_4) \simeq S_4$, en déduire que $\text{Aut}(S_4) \simeq S_4$ et $\text{Aut}(S_4) = \text{Int}(S_4)$.

[Les propriétés ci-dessus sont des cas particuliers d'un résultat plus général [10].]

CHAPITRE VII

Suites de composition

Dans ce chapitre, nous démontrons le *théorème de Jordan-Hölder* et nous introduisons deux classes importantes de groupes : celle des *groupes résolubles* et celle des *groupes nilpotents*. Toute cette étude repose sur la notion de *suite de composition*.

1 — Théorème de Jordan-Hölder

A / *Suites de composition*

Nous désignons par G un groupe quelconque.

Définition (7.1) : On appellera *suite de composition* de G toute chaîne finie de sous-groupes G_i ($0 \leq i \leq n$, $n \in \mathbf{N}^*$), du type :

$$G = G_0 \geq G_1 \geq \dots \geq G_i \geq G_{i+1} \geq \dots \geq G_n = (e) \quad (1)$$

dans laquelle on a $G_{i+1} < G_i$, quel que soit i ($0 \leq i \leq n-1$).

Les groupes $\frac{G_i}{G_{i+1}}$ sont appelés *quotients* de la suite de composition et n est sa *longueur* (n = nombre des quotients de la suite).

Si, dans (1), on a $G_i \neq G_{i+1}$, quel que soit i ($0 \leq i \leq n-1$), on dit que la suite de composition est *strictement décroissante*.

Remarque (7.2) :

1° Une suite de composition, selon la définition (7.1), est appelée par certains auteurs : « suite normale ». Nous avons préféré réserver cette dernière appellation aux suites de composition telles que chaque G_i est normal dans G (définition (7.24)).

2° Tout groupe G a au moins une suite de composition : $G \geq (e)$.

3° Une généralisation de la définition (7.1) est la suivante :

Définition (7.3) : H étant un sous-groupe de G , on appellera *suite de composition de G vers H* toute chaîne finie de sous-groupes H_i ($0 \leq i \leq n$, $n \in \mathbf{N}^*$), de la forme :

$$G = H_0 \geq H_1 \geq \dots \geq H_i \geq H_{i+1} \geq \dots \geq H_n = H \quad (2)$$

dans laquelle, pour tout i ($0 \leq i \leq n-1$), on a $H_{i+1} \triangleleft H_i$.

Les $\frac{H_i}{H_{i+1}}$ sont les *quotients* de la suite et n est sa *longueur*.

Définitions (7.4) : Soient Σ et Σ' deux suites de composition de G :

$$\Sigma : \quad G = G_0 \geq G_1 \geq \dots \geq G_n = (e)$$

$$\Sigma' : \quad G = K_0 \geq K_1 \geq \dots \geq K_p = (e).$$

1° On dit que Σ' est un *raffinement* de Σ , si $p \geq n$ et si la suite Σ est extraite de Σ' ; c'est-à-dire s'il existe n entiers positifs : $j_0 < j_1 < \dots < j_n \leq p$ tels que, pour tout i ($0 \leq i \leq n$), $G_i = K_{j_i}$. On pourra alors écrire : $\Sigma \subseteq \Sigma'$.

S'il existe un entier $j \in \{0, 1, \dots, p\}$ tel que $K_j \neq G_i$, quel que soit i ($0 \leq i \leq n$), on dit que Σ' est un *raffinement propre* de Σ ; dans ce cas, on a nécessairement $p > n$ et on écrira $\Sigma \subset \Sigma'$.

2° On dit que les suites de compositions Σ et Σ' sont *équivalentes*, si $n = p$ et s'il existe une permutation σ des entiers $0, 1, 2, \dots, n-1$, telle que, pour tout i ($0 \leq i \leq n-1$) :

$$\frac{G_i}{G_{i+1}} \simeq \frac{K_{\sigma(i)}}{K_{\sigma(i)+1}}.$$

On exprimera l'équivalence des deux suites de composition par la notation : $\Sigma \sim \Sigma'$.

Remarque (7.5) : Toute suite extraite d'une suite de composition telle que Σ' n'est pas, en général, une suite de composition; car, pour $l > j + 1$, on n'a pas nécessairement $K_l \triangleleft K_j$.

THÉORÈME (7.6) (Schreier ⁽¹⁾). Soient Σ_1 et Σ_2 deux suites de composition d'un groupe G ; il existe alors deux suites de compositions Σ'_1 et Σ'_2 de G telles que :

$$\Sigma_1 \subseteq \Sigma'_1, \quad \Sigma_2 \subseteq \Sigma'_2 \quad \text{et} \quad \Sigma'_1 \sim \Sigma'_2.$$

La démonstration de ce théorème s'appuie sur le lemme suivant :

LEMME (7.7) (Zassenhaus ⁽²⁾). Soient H , H' , K et K' des sous-groupes de G tels que $H' < H$ et $K' < K$; on a alors :

$$H'(H \cap K') \triangleleft H'(H \cap K), \quad K'(H' \cap K) \triangleleft K'(H \cap K) \quad (3)$$

$$\text{et} \quad \frac{H'(H \cap K)}{H'(H \cap K')} \simeq \frac{K'(H \cap K)}{K'(H' \cap K)} \quad (4)$$

Preuve : Des propriétés des sous-groupes normaux (chap. IV) on déduit les résultats suivants :

$$K' \triangleleft K \Rightarrow H \cap K' \triangleleft H \cap K$$

$$\text{et} \quad H' \triangleleft H \Rightarrow H' \cap K \triangleleft H \cap K,$$

$$\text{d'où} \quad H'(H \cap K') \triangleleft H'(H \cap K) \quad \text{et} \quad K'(H' \cap K) \triangleleft K'(H \cap K),$$

ainsi que :

$$(H \cap K')(H' \cap K) \triangleleft H \cap K.$$

Pour démontrer (4), on va prouver que chacun des quotients de cette relation est isomorphe à $\frac{H \cap K}{(H \cap K')(H' \cap K)}$; pour cela, considérons la correspondance :

$$\varphi : H'(H \cap K) \rightarrow \frac{H \cap K}{(H \cap K')(H' \cap K)}$$

$$xy \mapsto \bar{y}$$

$x \in H'$, $y \in H \cap K$ et \bar{y} est la classe de y modulo $(H \cap K')(H' \cap K)$.

⁽¹⁾ O. Schreier, mathématicien allemand (1901-1929).

⁽²⁾ H. J. Zassenhaus, mathématicien américain, d'origine allemande (lemme publié en 1934 [77]).

Vérifions que φ est une *application* : supposons $x' \in H'$, $y' \in H \cap K$ tels que $x'y' = xy$; on a alors $x^{-1}x' = yy'^{-1}$, donc $yy'^{-1} \in H' \cap K$ et par suite $\bar{y} = \bar{y}'$; d'où $\varphi(x'y') = \varphi(xy)$.

La définition de φ implique sa *surjectivité*. D'autre part, φ est un *morphisme de groupes* :

Soient x, x' dans H' et y, y' dans $H \cap K$,

$$xyx'y' = xyx'y'^{-1}yy' \quad \text{et} \quad (H' \triangleleft H, y \in H) \Rightarrow yx'y^{-1} \in H';$$

en posant $x_1 = yx'y^{-1}$ on a $xyx'y' = xx_1yy'$, d'où

$$\varphi(xyx'y') = \varphi(xx_1yy') = \overline{yy'} = \bar{y}\bar{y}';$$

par suite, $\varphi(xyx'y') = \varphi(xy)\varphi(x'y')$.

Déterminons $\text{Ker } \varphi$: soient $x \in H'$, $y \in H \cap K$,

$$xy \in \text{Ker } \varphi \Leftrightarrow y \in (H \cap K')(H' \cap K)$$

d'où $\text{Ker } \varphi = H'(H \cap K')$, car $H' \cap K \leq H'$.

En appliquant le 1^{er} théorème d'isomorphisme, on obtient :

$$\frac{H'(H \cap K)}{H'(H \cap K')} \simeq \frac{H \cap K}{(H \cap K')(H' \cap K)} \quad (5)$$

De la même façon, on montrerait que $\frac{K'(H \cap K)}{K'(H' \cap K)}$ est isomorphe au second quotient de la relation (5), d'où le lemme.

Démonstration du théorème (7.6) de Schreier

Soient :

$$\Sigma_1: \quad G = G_0 \geq G_1 \geq \dots \geq G_n = (e)$$

$$\Sigma_2: \quad G = H_0 \geq H_1 \geq \dots \geq H_p = (e).$$

Quels que soient i ($1 \leq i \leq n$) et j ($1 \leq j \leq p$), posons :

$$G_{ij} = G_i(G_{i-1} \cap H_j) \quad \text{et} \quad H_{ji} = H_j(H_{j-1} \cap G_i) \quad (6)$$

Les G_{ij} sont des sous-groupes de G , car on a $G_i \triangleleft G_{i-1}$ et $G_{i-1} \cap H_j \leq G_{i-1}$; il en est de même pour les H_{ji} .

On a $G_{ip} = G_i$, $H_{jn} = H_j$ et quels que soient i ($1 \leq i \leq n$) et j ($1 \leq j \leq p$),

$$G_{i-1} \geq G_{i1} \geq G_{i2} \geq \dots \geq G_{ip} = G_i \quad (7)$$

$$H_{j-1} \geq H_{j1} \geq H_{j2} \geq \dots \geq H_{jn} = H_j \quad (8)$$

on remarque que l'on peut écrire $G_{i-1} = G_{i0}$ et $H_{j-1} = H_{j0}$ et, compte tenu du lemme (7.7) de Zassenhaus, on a

$$G_{ij} \triangleleft G_{i,j-1}, \quad H_{ji} \triangleleft H_{j,i-1} \quad (9)$$

et
$$\frac{G_{i,j-1}}{G_{ij}} \simeq \frac{H_{j,i-1}}{H_{ji}} \quad (10)$$

Soit Σ'_1 la chaîne décroissante de sous-groupes de G , obtenue à partir de Σ , en intercalant entre G_{i-1} et G_i les sous-groupes G_{ij} ($1 \leq j \leq p$) comme dans (7), pour tout i tel que $1 \leq i \leq n$; d'après (9), Σ'_1 est une suite de composition de G , sa longueur est np et c'est un raffinement de Σ_1 .

On construit de même un raffinement Σ'_2 de Σ_2 en intercalant entre H_{j-1} et H_j les sous-groupes H_{ji} ($1 \leq i \leq n$), comme dans (8); Σ'_2 est aussi de longueur np .

Σ'_1 et Σ'_2 sont donc de même longueur et, compte tenu de (10), on a $\Sigma'_1 \sim \Sigma'_2$.

B / Théorème de Jordan-Hölder ⁽⁸⁾

Définition (7.8) : Une suite de composition d'un groupe G sera appelée *suite de Jordan-Hölder* si tous les quotients de la suite sont des groupes simples. Cette appellation sera justifiée par le théorème (7.12) de Jordan-Hölder.

PROPOSITION (7.9). *Une suite de composition de G est une suite de Jordan-Hölder si et seulement si elle est strictement décroissante et n'admet aucun raffinement propre.*

Preuve : Soit

$$\Sigma: \quad G = G_0 \geq G_1 \geq \dots \geq G_i \geq G_{i+1} \geq \dots \geq G_n = (e).$$

⁽⁸⁾ C.-M. Jordan, mathématicien français (1838-1922); O. Hölder, mathématicien allemand (1859-1937).

$\frac{G_i}{G_{i+1}}$ simple $\Leftrightarrow G_{i+1} \neq G_i$ et G_{i+1} normal maximal dans G , d'après la proposition (4.52). Cette dernière condition est équivalente à : quel que soit i ($0 \leq i \leq n-1$), il n'existe aucun sous-groupe H tel que $G_i > H > G_{i+1}$ et $H \triangleleft G_i$, d'où le résultat énoncé.

Remarques (7.10) :

1° Si Σ est une suite de Jordan-Hölder de G alors toute suite de composition Σ' équivalente à Σ est encore une suite de Jordan-Hölder de G .

En effet, tout quotient de Σ' est isomorphe à un quotient de Σ , donc il est simple.

2° Tout groupe n'admet pas nécessairement une suite de Jordan-Hölder. Par exemple, \mathbf{Z} n'admet pas de suite de Jordan-Hölder. En effet, si on considère une suite de composition strictement décroissante de \mathbf{Z} :

$$\mathbf{Z} > k_1 \mathbf{Z} > k_2 \mathbf{Z} > \dots > k_n \mathbf{Z} > (0) \quad (11)$$

on peut toujours construire un raffinement propre de (11) en intercalant, par exemple, $2k_n \mathbf{Z}$ entre $k_n \mathbf{Z}$ et (0) .

Nous montrons que tout groupe fini a une suite de Jordan-Hölder, mais il existe des groupes infinis qui ont une suite de Jordan-Hölder (exercice 5, chap. VII).

Notons cependant qu'un groupe abélien n'a une suite de Jordan-Hölder que s'il est fini et différent de (e) .

En effet, supposons qu'un groupe abélien G ait une suite de Jordan-Hölder :

$$G = G_0 > G_1 > \dots > G_n = (e).$$

Tous les quotients de la suite sont abéliens simples, donc ils sont cycliques d'ordre premier (proposition (4.9)).

Pour tout i ($0 \leq i \leq n-1$) posons $p_i = [G_i : G_{i+1}]$, les p_i sont des nombres premiers et

$$[G : G_n] = |G| = p_0 p_1 \dots p_{n-1},$$

donc G est fini.

3° Tout groupe simple G admet une unique suite de composition strictement décroissante, qui est une suite de Jordan-Hölder : $G = G_0 > G_1 = (e)$.

PROPOSITION (7.11). *Tout groupe fini $G \neq (e)$ admet une suite de Jordan-Hölder.*

Preuve : Soit un groupe fini $G \neq (e)$. Un groupe simple ayant une suite de Jordan-Hölder, on suppose G non simple. Soit \mathcal{H} l'ensemble des sous-groupes *propres normaux* de G ; cet ensemble est non vide et fini, car G est fini. Toute chaîne strictement croissante de sous-groupes de G appartenant à \mathcal{H} est donc finie, par suite \mathcal{H} contient au moins un élément maximal H_1 ; donc $\frac{G}{H_1}$ est simple.

Si H_1 est simple, alors $G > H_1 > (e)$ est une suite de Jordan-Hölder de G .

Si H_1 n'est pas simple, on considère l'ensemble non vide et fini \mathcal{H}_1 des sous-groupes propres et normaux de H_1 . Le raisonnement vu plus haut montre que \mathcal{H}_1 contient au moins un élément maximal H_2 , donc $\frac{H_1}{H_2}$ est simple.

Si H_2 est simple, alors $G > H_1 > H_2 > (e)$ est une suite de Jordan-Hölder, sinon on réitère la méthode précédente. Le nombre des sous-groupes de G étant fini, nécessairement, au bout d'un nombre fini, k , d'opérations on obtient un sous-groupe H_k simple de G tel que :

$$G > H_1 > H_2 > \dots > H_{k-1} > H_k > (e)$$

est une suite de Jordan-Hölder de G .

THÉORÈME (7.12) (Jordan-Hölder). *Etant donné un groupe G admettant une suite de Jordan-Hölder, alors :*

- 1° *toute suite de composition strictement décroissante de G admet un raffinement qui est une suite de Jordan-Hölder ;*
- 2° *deux suites de Jordan-Hölder quelconques de G sont équivalentes.*

Preuve :

1° Par hypothèse, G admet une suite de Jordan-Hölder que nous notons Σ_0 .

Soit, d'autre part, Σ une suite de composition strictement décroissante de G . D'après le théorème de Schreier, Σ et Σ_0 admettant des

raffinements équivalents, Σ' et Σ'_0 , respectivement. Mais Σ_0 n'ayant pas de raffinement propre, Σ'_0 est identique à Σ_0 , d'où $\Sigma' \sim \Sigma_0$ et Σ' est donc une suite de Jordan-Hölder (remarque (7.10) 1°).

2° Compte tenu des notations précédentes, si Σ est aussi une suite de Jordan-Hölder de G , alors le raffinement Σ' de Σ est identique à Σ , d'où $\Sigma \sim \Sigma_0$.

Remarques (7.13) :

1° Dans le cas des groupes finis, on peut démontrer directement le théorème de Jordan-Hölder, sans utiliser le lemme de Zassenhaus, ni le théorème de Schreier [41].

3° D'après le théorème (7.12), pour un groupe G admettant une suite de Jordan-Hölder, deux telles suites quelconques ont la même longueur.

Définition (7.14) :

- a) un groupe G admettant une suite de Jordan-Hölder de longueur n est dit de *longueur finie* n ;
- b) un groupe $G \neq (e)$ n'admettant pas de suite de Jordan-Hölder est dit de *longueur infinie*;
- c) $G = (e)$ sera, par convention, de *longueur 0*.

Remarque (7.15) : Un groupe est simple si et seulement s'il est de longueur 1.

Exemples (7.16) : Pour le groupe symétrique S_4 ,

$$S_4 > A_4 > (e) \tag{12}$$

est une suite de composition, mais ce n'est pas une suite de Jordan-Hölder, car A_4 n'est pas simple.

D'après les résultats des exercices 9 et 10 (chap. IV), $K = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ est normal dans A_4 et $H = \{e, (1, 2)(3, 4)\}$ est normal dans K , on en déduit un raffinement de (12) :

$$S_4 > A_4 > K > H > (e) \tag{13}$$

tel que $o\left(\frac{S_4}{A_4}\right) = 2$, $o\left(\frac{A_4}{K}\right) = 3$, $o\left(\frac{K}{H}\right) = 2$ et $o(H) = 2$; donc (13) est une suite de Jordan-Hölder et S_4 est un groupe de longueur 4.

Par contre, A_5 étant simple (exercice 6, chap. V), $S_5 > A_5 > (e)$ est une suite de Jordan-Hölder et S_5 est un groupe de longueur 2.

PROPOSITION (7.17). Soit $H \triangleleft G$, alors :

$$\left(H \text{ et } \frac{G}{H} \text{ sont de longueur finie} \right) \Rightarrow G \text{ est de longueur finie}$$

et $\text{long}(G) = \text{long}(H) + \text{long}\left(\frac{G}{H}\right).$

Preuve : Soit

$$H = H_0 > H_1 > \dots > H_{r-1} > H_r = (e)$$

une suite de Jordan-Hölder de H

et $\frac{G}{H} = \frac{G_0}{H} > \frac{G_1}{H} > \dots > \frac{G_{s-1}}{H} > \frac{G_s}{H} = (\bar{e})$

une suite de Jordan-Hölder de $\frac{G}{H}$.

$$\frac{G_{i+1}}{H} \triangleleft \frac{G_i}{H} \Leftrightarrow G_{i+1} < G_i, \text{ dans } G.$$

D'autre part, pour tout i ($0 \leq i \leq s-1$), on a

$$\frac{\frac{G_i}{H}}{\frac{G_{i+1}}{H}} \simeq \frac{G_i}{G_{i+1}}, \text{ donc } \frac{G_i}{G_{i+1}} \text{ est simple;}$$

de plus $G_s = H$, par suite,

$$G = G_0 > G_1 > \dots > G_{s-1} > H > H_1 > \dots > H_r = (e)$$

est une suite de Jordan-Hölder de G et sa longueur est $r + s$.

PROPOSITION (7.18). *Quel que soit le nombre premier p , tout p -groupe fini G , d'ordre p^n , est de longueur n et tous les quotients d'une suite de Jordan-Hölder de G sont d'ordre p .*

Preuve :

- si $n = 1$, la propriété est vérifiée (voir remarques (7.10) et (7.15));
- supposons $n > 1$;
- si le groupe G est abélien, d'après le 1^{er} théorème de Sylow, il existe un sous-groupe G_1 de G , d'ordre p^{n-1} ;

$$G \text{ abélien} \Rightarrow G_1 < G \quad \text{et} \quad o\left(\frac{G}{G_1}\right) = p.$$

De même G_1 étant abélien d'ordre p^{n-1} , il existe un sous-groupe G_2 de G_1 , d'ordre p^{n-2} et tel que $o\left(\frac{G_1}{G_2}\right) = p$.

Ainsi, de proche en proche on construit une suite de composition strictement décroissante de G , de longueur n (car $o(G_n) = p^0 = 1$), telle que chacun de ses quotients est d'ordre p , donc simple.

— Supposons G non abélien et raisonnons par récurrence sur n ; $Z(G)$ étant le centre de G , d'après le théorème (5.27), on a $Z(G) \neq (e)$, donc $o(Z(G)) = p^k$ avec $1 \leq k \leq n - 1$. Soit x un élément d'ordre p de $Z(G)$; x existe d'après le théorème de Sylow. Posons $H = \langle x \rangle$.

$$H \leq Z(G) \Rightarrow H \triangleleft G \quad (\text{exemple (4.12) } 3^\circ)$$

$$o(H) = p \Rightarrow o\left(\frac{G}{H}\right) = p^{n-1}.$$

Compte tenu de l'hypothèse de récurrence, $\frac{G}{H}$ est un groupe de longueur $n - 1$ et tous les quotients d'une suite de Jordan-Hölder de $\frac{G}{H}$ sont d'ordre p .

D'autre part, H est d'ordre p , donc H est de longueur 1; d'après la proposition (7.17), G est de longueur n .

De plus, la démonstration de la proposition (7.17) montre que,

si $\frac{G}{H} > \frac{G_1}{H} > \dots > \frac{G_{n-2}}{H} > \frac{G_{n-1}}{H} = (\bar{e})$ est une suite de Jordan-Hölder de $\frac{G}{H}$, alors :

$$G > G_1 > \dots > G_{n-2} > H > (e) \quad (14)$$

est une suite de Jordan-Hölder de G ; on en déduit que tous les quotients de cette suite sont d'ordre p .

COROLLAIRE (7.19). *Tout p -groupe fini d'ordre p^n a au moins un sous-groupe maximal normal d'ordre p^{n-1} .*

En effet, dans (14), on a $G_1 < G$ et $o\left(\frac{G}{G_1}\right) = p$ premier, donc G_1 est maximal dans G (proposition (4.54)).

Remarque (7.20) :

1° Si un groupe infini G est de longueur finie, alors un sous-groupe de G n'est pas nécessairement de longueur finie (exercice 5, chap. VII).

2° G et G' étant deux groupes, on voit aisément que

$$G \simeq G' \Rightarrow \text{long}(G) = \text{long}(G'),$$

mais la réciproque est fausse.

Par exemple, d'après la proposition (7.18), les groupes d'ordre 4, C_4 et $C_2 \times C_2$ sont de longueur 2, mais ils ne sont pas isomorphes.

2 — Groupes résolubles

A / Définitions et propriétés générales

Etant donné un groupe G , les groupes dérivés successifs de G , définis au paragraphe 5 du chapitre IV, forment une chaîne décroissante de sous-groupes de G :

$$G = D_0(G) \geq D_1(G) \geq \dots \geq D_i(G) \geq D_{i+1}(G) \geq \dots$$

Définition (7.21) : Un groupe G est dit *résoluble* s'il existe un entier $n \geq 0$ tel que $D_n(G) = (e)$.

Conséquences de la définition (7.21) :

Si $G \neq (e)$ est résoluble et si n désigne le plus petit entier positif tel que $D_n(G) = (e)$, alors, pour tout i ($0 \leq i \leq n-1$), on a $D_i(G) > D_{i-1}(G)$, car

$$D_i(G) = D_{i+1}(G) \Rightarrow D_j(G) = D_i(G), \quad \forall j \geq i.$$

D'autre part, d'après le théorème (4.39), on a

$$D_{i+1}(G) \triangleleft D_i(G), \quad \forall i (0 \leq i \leq n-1);$$

on en déduit que

$$G = D_0(G) > D_1(G) > \dots > D_n(G) = (e) \quad (15)$$

est une suite de composition de G .

Remarque (7.22) :

1° Tout groupe abélien G est résoluble, car, pour un tel groupe, $D(G) = D_1(G) = (e)$.

2° L'appellation groupe « résoluble » provient du fait qu'en théorie de Galois ⁽⁴⁾ de tels groupes permettent de caractériser les équations polynomiales « résolubles par radicaux » ([68], [44]).

THÉORÈME (7.23). Si G est un groupe résoluble, alors tout sous-groupe de G et tout quotient de G est résoluble.

Preuve : Par hypothèse, il existe $n \in \mathbb{N}$ tel que $D_n(G) = (e)$.

— Soit H un sous-groupe de G .

$$H \leq G \Rightarrow D(H) \leq D(G)$$

$$D(H) \leq D(G) \Rightarrow D_2(H) \leq D_2(G).$$

⁽⁴⁾ Evariste Galois, mathématicien français (1811-1832).

Ainsi, de proche en proche, on obtient $D_n(H) \leq D_n(G) = (e)$, d'où $D_n(H) = (e)$; H est donc résoluble.

— Soit $N \triangleleft G$; notons π l'épimorphisme canonique : $G \rightarrow \frac{G}{N}$ et posons $\bar{x} = \pi(x)$, pour tout $x \in G$.

Tout commutateur de $\frac{G}{N}$ est l'image par π d'un commutateur de G , car

$$\bar{x}^{-1} \bar{y}^{-1} \bar{x} \bar{y} = \pi(x^{-1} y^{-1} xy).$$

On en déduit que $D\left(\frac{G}{N}\right) = \pi(D(G))$.

De même, on a $D_2\left(\frac{G}{N}\right) = \pi(D_2(G))$ et de proche en proche on obtient :

$$D_n\left(\frac{G}{N}\right) = \pi(D_n(G)) = (\bar{e}),$$

d'où $\frac{G}{N}$ résoluble.

Définition (7.24) : Une suite de composition d'un groupe G :

$$G = G_0 \geq G_1 \geq \dots \geq G_n = (e)$$

est appelée *suite normale* si, pour tout i ($0 \leq i \leq n$), on a $G_i \triangleleft G$.

THÉORÈME (7.25). Pour un groupe G , les propriétés suivantes sont équivalentes :

- 1) G est résoluble ;
- 2) G admet une suite normale dont tous les quotients sont abéliens ;
- 3) G admet une suite de composition dont tous les quotients sont abéliens.

Preuve : On suppose $G \neq (e)$.

— Si G est résoluble, soit n le plus petit entier positif tel que $D_n(G) = (e)$. Dans la suite de composition (15), chaque quotient $\frac{D_i(G)}{D_{i+1}(G)}$ est abélien, d'après le théorème (4.39); d'autre

part, on a $D_i(G) \triangleleft G$, d'après le corollaire (4.45). On en déduit que 1) \Rightarrow 2).

— Compte tenu de la définition d'une suite normale, 2) \Rightarrow 3).

— Montrons que 3) \Rightarrow 1). Par hypothèse, G a une suite de composition (que l'on peut supposer strictement décroissante) :

$$G = H_0 > H_1 > \dots > H_{n-1} > H_n = (e)$$

telle que, pour tout i ($0 \leq i \leq n-1$), $\frac{H_i}{H_{i+1}}$ est abélien.

D'après le théorème (4.39),

$$\frac{G}{H_1} \text{ abélien} \Rightarrow D_1(G) \leq H_1.$$

$$D_1(G) \leq H_1 \Rightarrow D_2(G) \leq D(H_1)$$

et
$$\frac{H_1}{H_2} \text{ abélien} \Rightarrow D(H_1) \leq H_2,$$

on en déduit : $D_2(G) \leq H_2$.

Ainsi, de proche en proche, on montre que, pour tout i ($1 \leq i \leq n$), on a $D_i(G) \leq H_i$; en particulier, $D_n(G) \leq H_n = (e)$ implique $D_n(G) = (e)$, donc G est résoluble.

COROLLAIRE (7.26). *Les seuls groupes simples résolubles sont les groupes cycliques d'ordre premier.*

Preuve : Si G est un groupe simple, sa seule suite de composition strictement décroissante est : $G > (e)$; alors, d'après le théorème (7.25), si G est résoluble, il est abélien; par suite G est cyclique d'ordre premier (proposition (4.9)).

COROLLAIRE (7.27). *Pour $n \geq 5$, le groupe symétrique S_n n'est pas résoluble.*

Preuve : Si, pour $n \geq 5$, le groupe S_n était résoluble, d'après le théorème (7.23), le groupe alterné A_n serait résoluble; or on sait que, pour $n \geq 5$, le groupe A_n est simple (exercice 6, chap. V) et non abélien, donc non résoluble d'après le corollaire (7.26).

Remarque (7.28) : Pour $2 \leq n \leq 4$, S_n est résoluble. En effet :

- pour $n = 2$, $S_2 \simeq C_2$, résoluble d'après le corollaire (7.26);
- pour $n = 3$, la suite de composition $S_3 > A_3 > (e)$ a tous ses quotients abéliens, car $\frac{S_3}{A_3} \simeq C_2$ et $A_3 \simeq C_3$;
- pour $n = 4$, S_4 a une suite de Jordan-Hölder (13), dont tous les quotients sont abéliens (voir l'exemple (7.16)).

On notera que cette suite n'est pas une suite normale, car H n'est pas normal dans S_4 (exercice 9, chap. IV).

THÉORÈME (7.29). *Un groupe $G \neq (e)$ est résoluble si et seulement s'il contient un sous-groupe normal propre N , tel que N et $\frac{G}{N}$ sont résolubles.*

Preuve :

— Si G est résoluble, alors la suite (15) est au moins de longueur 1. Le sous-groupe $D_1(G) = D(G) \neq G$ est normal dans G et $\frac{G}{D(G)}$ est un groupe abélien, donc résoluble.

— Réciproquement, supposons que le groupe G contienne un sous-groupe normal propre N , tel que N et $\frac{G}{N}$ soient résolubles; alors, d'après le théorème (7.25), N et $\frac{G}{N}$ ont, respectivement, des suites de composition :

$$N = K_0 \geq K_1 \geq \dots \geq K_r = (e)$$

$$\frac{G}{N} = \frac{G_0}{N} \geq \frac{G_1}{N} \geq \dots \geq \frac{G_s}{N} = (\bar{e})$$

dont tous les quotients sont abéliens. On a donc :

$$\frac{K_i}{K_{i+1}} \text{ groupe abélien, } \forall i \ (0 \leq i \leq r-1)$$

$$\text{et } \frac{\frac{G_j}{N}}{\frac{G_{j+1}}{N}} \simeq \frac{G_j}{G_{j+1}} \text{ groupe abélien, } \forall j \ (0 \leq j \leq s-1).$$

On en déduit que

$$G = G_0 \geq G_1 \geq \dots \geq G_{s-1} \geq N \geq K_1 \geq \dots \geq K_r = (e)$$

est une suite de composition de G , dont tous les quotients sont abéliens, donc G est résoluble.

COROLLAIRE (7.30). *Si H et K sont deux sous-groupes normaux et résolubles de G , alors HK est un sous-groupe normal et résoluble de G .*

Preuve :

$$(H \triangleleft G \text{ et } K \triangleleft G) \Rightarrow (HK \triangleleft G \text{ et } H \triangleleft HK),$$

d'après la proposition (4.18). L'application du second théorème d'isomorphisme donne :

$$\frac{HK}{H} \simeq \frac{K}{H \cap K}.$$

D'après le théorème (7.23), $\frac{K}{H \cap K}$ est résoluble, donc H et $\frac{HK}{H}$ sont résolubles; le théorème (7.29) implique alors HK résoluble.

PROPOSITION (7.31). *Soient deux groupes H et K , alors :*

$$H \text{ et } K \text{ résolubles} \Rightarrow H \times K \text{ résoluble.}$$

Preuve : Posons $G = H \times K$; notons e et e' les éléments unités de H et K ; alors $H' = H \times (e')$ et $K' = (e) \times K$ sont deux sous-groupes de G tels que $H' \simeq H$, $K' \simeq K$, et, d'après la proposition (1.85) :

$$G = H' K', \quad H' \triangleleft G \quad \text{et} \quad K' \triangleleft G.$$

On en déduit que G est résoluble, d'après le corollaire (7.30).

COROLLAIRE (7.32). $\{H_i\}_{1 \leq i \leq n}$ étant une famille finie de groupes ($n \geq 2$ dans N), alors :

$$[H_i \text{ résoluble, } \forall i (1 \leq i \leq n)] \Rightarrow \prod_{1 \leq i \leq n} H_i \text{ résoluble.}$$

Vérification laissée au lecteur.

PROPOSITION (7.33). *Soient deux sous-groupes normaux H et K d'un groupe G , alors :*

$$\frac{G}{H} \text{ et } \frac{G}{K} \text{ résolubles} \Rightarrow \frac{G}{H \cap K} \text{ résoluble.}$$

Preuve : Soit $\varphi : G \rightarrow \frac{G}{H} \times \frac{G}{K}$ tel que, pour tout $x \in G$, $\varphi(x) = (\bar{x}, \hat{x})$, où \bar{x} (resp^t \hat{x}) est la classe de x modulo H (resp^t modulo K).

On vérifie que φ est un morphisme de groupes et

$$\text{Ker } \varphi = H \cap K, \quad \text{d'où } \frac{G}{H \cap K} \simeq \text{Im } \varphi.$$

$\frac{G}{H}$ et $\frac{G}{K}$ étant résolubles, $\frac{G}{H} \times \frac{G}{K}$ est résoluble, d'après la proposition (7.31); compte tenu du théorème (7.23), $\frac{G}{H \cap K}$, isomorphisme à un sous-groupe de $\frac{G}{H} \times \frac{G}{K}$, est résoluble.

B / Groupes finis résolubles

THÉORÈME (7.34). *Un groupe fini, $G \neq (e)$, est résoluble si et seulement si les quotients d'une suite de Jordan-Hölder de G sont (cycliques) d'ordre premier.*

Preuve : Soit un groupe fini, $G \neq (e)$ admettant une suite de Jordan-Hölder :

$$G = G_0 > G_1 > \dots > G_n = (e),$$

telle que, pour tout i ($0 \leq i \leq n-1$), $\frac{G_i}{G_{i+1}}$ est d'ordre premier, donc cyclique, donc abélien.

G est résoluble d'après le théorème (7.25).

Réciproquement, supposons $G \neq (e)$, fini et résoluble.

Ces hypothèses impliquent $D(G) \neq G$. Considérons alors l'ensemble \mathcal{D} des sous-groupes propres normaux de G , contenant $D(G)$.

\mathcal{D} est non vide, car $D(G) \in \mathcal{D}$; G étant fini, \mathcal{D} est un ensemble fini, donc il existe dans \mathcal{D} , ordonné par l'inclusion, au moins un élément maximal G_1 .

$$D(G) \leq G_1 \Rightarrow \frac{G}{G_1} \text{ groupe abélien.}$$

De plus, G_1 étant maximal dans l'ensemble \mathcal{D} , le groupe $\frac{G}{G_1}$ est simple. On en conclut que $\frac{G}{G_1}$ est cyclique d'ordre premier (proposition 4.54)). De même, G_1 étant résoluble, en tant que sous-groupe du groupe résoluble G , on construit G_2 , sous-groupe normal de G_1 tel que $\frac{G_1}{G_2}$ soit cyclique d'ordre premier. En répétant le raisonnement, au bout d'un nombre fini d'opérations (car G est fini), on obtient une suite de composition strictement décroissante de sous-groupes de G :

$$G = G_0 > G_1 > G_2 > \dots > G_n = (e),$$

qui est une suite de Jordan-Hölder de G , dont les quotients sont d'ordre premier.

PROPOSITION (7.35). *Quel que soit le nombre premier p , tout p -groupe fini est résoluble.*

Ce résultat se déduit de façon immédiate du théorème (7.34) et de la proposition (7.18).

3 — Groupes nilpotents

A / Suites centrales. Notion de groupe nilpotent

a) *Notations* : Comme à l'habitude, le centre et le groupe dérivé d'un groupe G seront respectivement notés $Z(G)$ et $D(G)$.

On rappelle, d'autre part, que $H \sqsubset G$ exprime que H est un sous-groupe caractéristique de G (chap. IV).

Si X et Y sont deux parties non vides de G , on désigne par $[X, Y]$ le sous-groupe de G engendré par l'ensemble des commutateurs $[x, y]$, où $x \in X$ et $y \in Y$.

$$[x, y] = x^{-1}y^{-1}xy \Rightarrow [x, y]^{-1} = y^{-1}x^{-1}yx = [y, x]$$

par suite :

$$[X, Y] = [Y, X] \quad (16)$$

De plus, quels que soient X, Y, Z , parties non vides de G , on vérifie facilement que :

$$Y \subseteq Z \Rightarrow [X, Y] \subseteq [X, Z] \quad (17)$$

On remarquera que $[G, G] = D(G)$.

b) Notions de suite centrale et de groupe nilpotent.

Définition (7.36) : Pour un groupe G , une suite de composition

$$G = G_0 \geq G_1 \geq \dots \geq G_{n-1} \geq G_n = (e)$$

sera appelée *suite centrale*, si c'est une suite *normale* telle que $\frac{G_i}{G_{i+1}} \leq Z\left(\frac{G}{G_{i+1}}\right)$, quel que soit i ($0 \leq i \leq n-1$).

PROPOSITION (7.37). Une suite de composition d'un groupe G ,

$$\Sigma: \quad G = G_0 \geq G_1 \geq \dots \geq G_{n-1} \geq G_n = (e),$$

est une suite centrale si et seulement si, pour tout i ($0 \leq i \leq n-1$), on a :

$$[G_i, G] \leq G_{i+1} \quad (18)$$

Preuve :

— Supposons que Σ soit une suite centrale; pour tout i ($0 \leq i \leq n-1$), on a :

$$G_{i+1} \triangleleft G \quad \text{et} \quad \frac{G_i}{G_{i+1}} \leq Z\left(\frac{G}{G_{i+1}}\right).$$

Soient $x \in G_i$ et $g \in G$; notons \bar{x} et \bar{g} leurs classes modulo G_{i+1} , alors

$$\bar{x}\bar{g} = \bar{g}\bar{x} \Leftrightarrow [x, g] \in G_{i+1},$$

d'où $[G_i, G] \leq G_{i+1}$.

— Réciproquement, supposons que Σ vérifie la condition (18). Montrons que G_{i+1} est normal dans G . Soient $x \in G_{i+1}$ et $g \in G$, $G_{i+1} \leq G_i$ implique $x \in G_i$; alors, d'après la condition (18), $[x, g] = x^{-1}(g^{-1}xg)$ appartient à G_{i+1} , d'où $g^{-1}xg \in G_{i+1}$.

De plus, $[x, g] \in G_{i+1}$ équivaut à $x\bar{g} = \bar{g}x$ dans $\frac{G}{G_{i+1}}$, par suite :

$$\frac{G_i}{G_{i+1}} \leq Z\left(\frac{G}{G_{i+1}}\right).$$

Définition (7.38) : Un groupe sera dit *nilpotent* s'il possède une suite centrale.

c) Suite centrale descendante.

G étant un groupe, posons :

$$\Gamma_1 = G, \quad \Gamma_2 = [G, G] = D(G), \quad \Gamma_3 = [\Gamma_2, G]$$

et, d'une façon générale :

$$\Gamma_{k+1} = [\Gamma_k, G], \quad \forall k \in \mathbb{N}^* \quad (19)$$

Compte tenu de la relation (17), $\Gamma_2 \leq \Gamma_1$ implique

$$[\Gamma_2, G] \leq [\Gamma_1, G], \quad \text{c'est-à-dire } \Gamma_3 \leq \Gamma_2.$$

Par récurrence sur k , on prouve, sans difficulté, que :

$$\Gamma_{k+1} \leq \Gamma_k, \quad \forall k \in \mathbb{N}^* \quad (20)$$

Ainsi, pour tout groupe G , on définit la chaîne décroissante de sous-groupes :

$$G = \Gamma_1 \geq \Gamma_2 \geq \dots \geq \Gamma_k \geq \Gamma_{k+1} \geq \dots \quad (21)$$

PROPOSITION (7.39). *Quels que soient le groupe G et l'entier $k \geq 1$, Γ_k est un sous-groupe caractéristique, donc normal, de G .*

Preuve : Soit $\alpha \in \text{Aut}(G)$; $\Gamma_1 = G$, donc $\alpha(\Gamma_1) = \Gamma_1$ et $\Gamma_2 = D(G)$, donc Γ_2 est un sous-groupe caractéristique de G (proposition (4.43)).

Raisonnons par récurrence sur k . Supposons $k > 2$ et $\alpha(\Gamma_{k-1}) = \Gamma_{k-1}$, quel que soit $\alpha \in \text{Aut}(G)$.

$\Gamma_k = [\Gamma_{k-1}, G]$; étant donné $x \in \Gamma_{k-1}$, $y \in G$ et $\alpha \in \text{Aut}(G)$,

$$\alpha([x, y]) = \alpha(x^{-1}y^{-1}xy) = [\alpha(x), \alpha(y)];$$

$$x \in \Gamma_{k-1} \Rightarrow \alpha(x) \in \Gamma_{k-1}; \quad y \in G \Rightarrow \alpha(y) \in G,$$

par suite, $[\alpha(x), \alpha(y)] \in \Gamma_k$, d'où $\alpha(\Gamma_k) \subseteq \Gamma_k$.

En considérant α^{-1} dans $\text{Aut}(G)$, on obtient $\alpha^{-1}(\Gamma_k) \subseteq \Gamma_k$, donc $\Gamma_k \subseteq \alpha(\Gamma_k)$, d'où l'on déduit : $\alpha(\Gamma_k) = \Gamma_k$.

Ainsi, pour tout $k \in \mathbf{N}^*$, on a $\Gamma_k \sqsubset G$, donc $\Gamma_k \triangleleft G$ (remarque (4.42) 2°).

Remarque (7.40) : Si, pour un groupe G , il existe un entier $r \geq 1$ tel que $\Gamma_{r+1} = e$, alors la chaîne décroissante (21) s'écrit :

$$G = \Gamma_1 \geq \Gamma_2 \geq \dots \geq \Gamma_r \geq \Gamma_{r+1} = (e) \quad (22)$$

et, d'après la relation (19) et la proposition (7.39), (22) est une *suite centrale*.

Si $G \neq (e)$ et si $r > 1$ est le plus petit entier tel que $\Gamma_{r+1} = (e)$, alors, pour tout k ($2 \leq k \leq r$), on a $\Gamma_{k-1} > \Gamma_k$, car $\Gamma_k = \Gamma_{k+1}$ implique $\Gamma_j = \Gamma_k$, quel que soit $j \geq k$.

Définition (7.41) : On dit qu'un groupe G a une *suite centrale descendante de longueur r* ($r \geq 1$ dans \mathbf{N}), si la chaîne décroissante (21) s'écrit :

$$G = \Gamma_1 > \Gamma_2 > \dots > \Gamma_r > \Gamma_{r+1} = (e) \quad (23)$$

Dans ce cas, le groupe G est *nilpotent*.

d) *Suite centrale ascendante.*

LEMME (7.42). Si H est un sous-groupe caractéristique d'un groupe G et si $\frac{K}{\bar{H}} = Z\left(\frac{G}{\bar{H}}\right)$, alors K est le plus grand sous-groupe de G contenant H , tel que $[K, G] \leq H$ et K est caractéristique dans G .

Preuve : Soit π l'épimorphisme canonique $G \rightarrow \frac{G}{H}$; pour tout $x \in G$, posons $\bar{x} = \pi(x)$.

$$\frac{K}{H} = Z\left(\frac{G}{H}\right) = \left\{ \bar{x} \in \frac{G}{H}; \bar{x}\bar{g} = \bar{g}\bar{x}, \forall \bar{g} \in \frac{G}{H} \right\}.$$

$$\bar{x}\bar{g} = \bar{g}\bar{x} \Leftrightarrow [\bar{x}, \bar{g}] = \bar{e} \text{ dans } \frac{G}{H}$$

et $[\bar{x}, \bar{g}] = \pi([x, g]), \forall x \in \bar{x}, \forall g \in \bar{g};$

par suite,

$$\frac{K}{H} = Z\left(\frac{G}{H}\right) \Rightarrow [K, G] \leq H \quad (24)$$

Supposons K' sous-groupe de G tel que $H \leq K'$ et $[K', G] \leq H$.

Soit $x \in K'$; quel que soit $g \in G$, on a $[x, g] \in H$, d'où $\pi([x, g]) = \bar{e}$ dans $\frac{G}{H}$; c'est-à-dire $\bar{x}\bar{g} = \bar{g}\bar{x}$, quel que soit $\bar{g} \in \frac{G}{H}$,

donc $\frac{K'}{H} \leq Z\left(\frac{G}{H}\right)$, ce qui entraîne $K' \leq K$.

Soit $\alpha \in \text{Aut}(G)$; $[K, G] \leq H$ implique $[\alpha(K), G] \leq \alpha(H)$.

Par hypothèse, on a $H \sqsubset G$, donc $\alpha(H) = H$; on en déduit, d'une part, $[\alpha(K), G] \leq H$, d'autre part, $H \leq K \Rightarrow H \leq \alpha(K)$; K étant, comme on vient de le montrer, le plus grand sous-groupe de G contenant H tel que $[K, G] = H$, on a $\alpha(K) \leq K$. En utilisant l'automorphisme α^{-1} , on obtient $\alpha^{-1}(K) \leq K$, on en déduit $\alpha(K) = K$, donc $K \sqsubset G$.

Notations (7.43) :

G étant un groupe, posons $Z_0 = (e)$, $Z_1 = Z(G)$.

On sait que Z_1 est caractéristique dans G (proposition (4.43)), par suite l'unique sous-groupe Z_2 de G , contenant Z_1 , tel que $\frac{Z_2}{Z_1} = Z\left(\frac{G}{Z_1}\right)$, est caractéristique dans G .

De proche en proche, on définit, pour tout $i \in \mathbb{N}$, le sous-groupe Z_{i+1} tel que

$$\frac{Z_{i+1}}{Z_i} = Z\left(\frac{G}{Z_i}\right) \quad (25)$$

et Z_{i+1} est caractéristique dans G .

On détermine ainsi une chaîne croissante de sous-groupes de G :

$$(e) = Z_0 \leq Z_1 \leq \dots \leq Z_i \leq Z_{i+1} \leq \dots \quad (26)$$

dans laquelle, pour tout $i \in \mathbb{N}$, on a $Z_i \sqsubset G$, donc $Z_i < G$ et Z_{i+1} est le plus grand sous-groupe de G contenant Z_i , tel que

$$[Z_{i+1}, G] \leq Z_i \quad (27)$$

S'il existe un entier $s \geq 0$ tel que $Z_s = G$, la chaîne (26) s'écrit :

$$(e) = Z_0 \leq Z_1 \leq \dots \leq Z_{s-1} \leq Z_s = G \quad (28)$$

et, d'après ce qui précède, (28) est une *suite centrale* de G .

De plus, si $G \neq (e)$ et si s est le plus petit entier positif tel que $Z_s = G$, alors, pour tout i ($0 \leq i \leq s-1$), on a $Z_i < Z_{i+1}$, car $Z_i = Z_{i+1}$ implique $Z_j = Z_i$, quel que soit $j \geq i$.

Définition (7.44) : On dit qu'un groupe G a une *suite centrale ascendante de longueur s* ($s \geq 1$ dans \mathbb{N}), si la chaîne croissante (26) s'écrit :

$$(e) = Z_0 < Z_1 < \dots < Z_{s-1} < Z_s = G; \quad (29)$$

le groupe G est alors *nilpotent*.

Remarque (7.45) : Le groupe $G = (e)$ sera considéré comme ayant une suite centrale descendante (resp^t ascendante) de longueur 0.

e) Classe de nilpotence.

THÉORÈME (7.46). *Un groupe G a une suite centrale descendante de longueur r si et seulement s'il a une suite centrale ascendante de longueur r .*

Preuve : On considère $G \neq (e)$.

1) On suppose que G a une suite centrale ascendante de longueur r et on considère la chaîne croissante (26) des sous-groupes Z_i de G . Démontrons que, pour tout i ($0 \leq i \leq r$), on a

$$\Gamma_{r+1-i} \leq Z_i \quad (30)$$

Pour $i = 0$, $\Gamma_{r+1} = (e) = Z_0$, la relation (30) est vérifiée.

Raisonnons par récurrence sur i ; supposons $\Gamma_{r+1-i} \leq Z_i$ pour $0 \leq i \leq r-1$ et montrons que $\Gamma_{r-i} \leq Z_{i+1}$.

$\Gamma_{r+1-i} = [\Gamma_{r-i}, G]$, donc (30) équivaut à $[\Gamma_{r-i}, G] \leq Z_i$; or, Z_{i+1} est le plus grand sous-groupe de G contenant Z_i tel que $[Z_{i+1}, G] \leq Z_i$ (voir (27)), par suite, on a

$$\Gamma_{r-i} \leq Z_{i+1}.$$

Pour $i = r$, (30) donne $\Gamma_1 = G \leq Z_r$, donc $Z_r = G$.

On en conclut que G a une suite centrale ascendante de longueur $s \leq r$.

2) Supposons maintenant que G ait une suite centrale ascendante de longueur s et considérons la chaîne décroissante (21) des sous-groupes Γ_i de G . Montrons que, pour tout i ($1 \leq i \leq s+1$), on a

$$\Gamma_i \leq Z_{s+1-i} \quad (31)$$

La relation (31) est vraie pour $i = 1$, car $\Gamma_1 = G = Z_s$.

Raisonnons par récurrence sur i ; la relation (31) étant supposée vraie pour i ($1 \leq i \leq s$), montrons que $\Gamma_{i+1} \leq Z_{s-i}$.

$$\Gamma_i \leq Z_{s+1-i} \Rightarrow [\Gamma_i, G] \leq [Z_{s+1-i}, G]$$

$[\Gamma_i, G] = \Gamma_{i+1}$ et (27) implique $[Z_{s+1-i}, G] \leq Z_{s-i}$, d'où $\Gamma_{i+1} \leq Z_{s-i}$.

Pour $i = s+1$, on obtient : $\Gamma_{s+1} \leq Z_0 = (e)$, d'où $\Gamma_{s+1} = (e)$.

Le groupe G a donc une suite centrale descendante de longueur $r \leq s$; mais, en appliquant la première partie de la démonstration, on trouve $s \leq r$, d'où $r = s$.

THÉORÈME (7.47). *Pour un groupe G , les trois conditions suivantes sont équivalentes :*

- 1) G est nilpotent ;
- 2) G a une suite centrale descendante de longueur r ;
- 3) G a une suite centrale ascendante de longueur r .

Preuve : Le théorème (7.46) exprime que 2) \Leftrightarrow 3) et on sait, d'autre part, que 2) \Rightarrow 1) et 3) \Rightarrow 1) (voir les définitions (7.38), (7.41), (7.44)). Il suffit de prouver que, par exemple, 1) \Rightarrow 2).

Soit Σ une suite centrale de G :

$$G = G_0 \geq G_1 \geq \dots \geq G_n = (e).$$

Vérifions que, pour tout i ($0 \leq i \leq n$), on a

$$\Gamma_{i+1} \leq G_i \quad (32)$$

Pour $i = 0$, $\Gamma_1 = G = G_0$, donc (32) est vérifiée.

Raisonnons par récurrence sur i . Supposons $\Gamma_i \leq G_{i-1}$, pour $0 \leq i \leq n-1$; on en déduit :

$$\Gamma_{i+1} = [\Gamma_i, G] \leq [G_{i-1}, G];$$

or, d'après la proposition (7.37), on a $[G_{i-1}, G] \leq G_i$, d'où $\Gamma_{i+1} \leq G_i$.

Pour $i = n$, la relation (32) implique : $\Gamma_{n+1} \leq G_n = (e)$, par suite G a une suite centrale descendante de longueur $r \leq n$.

Définition (7.48) : Si G est un groupe nilpotent, la longueur commune de sa suite centrale descendante et de sa suite centrale ascendante est appelée : *classe de nilpotence de G* .

Exemple (7.49) :

1° Tout groupe abélien $G \neq (e)$ a une suite centrale ascendante : $(e) = Z_0 < Z_1 = G$.

On en déduit que les groupes nilpotents de classe 1 sont les groupes abéliens $G \neq (e)$.

2° Compte tenu de la remarque (7.45), le groupe $G = (e)$ est considéré comme nilpotent de classe 0.

PROPOSITION (7.50). *Quel que soit le nombre premier p , tout p -groupe fini est nilpotent.*

Preuve : Soit G un p -groupe fini d'ordre p^n , $n \in \mathbb{N}^*$. D'après le théorème (5.27), on a $Z_1 = Z(G) \neq (e)$.

— Si $Z_1 = G$, alors G est abélien, donc nilpotent.

— Si $Z_1 \neq G$, alors $\frac{G}{Z_1}$ est un p -groupe fini dont le centre n'est pas réduit à l'élément unité; par suite, il existe un unique sous-groupe Z_2 de G tel que :

$$Z_1 < Z_2 \quad \text{et} \quad \frac{Z_2}{Z_1} = Z\left(\frac{G}{Z_1}\right);$$

- ou bien, $Z_2 = G$ et $(e) = Z_0 < Z_1 < Z_2 = G$ est une suite centrale ascendante pour G , qui est donc nilpotent de classe 2 ;
- ou bien, $Z_2 \neq G$ et $\frac{G}{Z_2}$ est encore un p -groupe fini, donc il existe Z_3 tel que $Z_2 < Z_3$ et $\frac{Z_3}{Z_2} = Z\left(\frac{G}{Z_2}\right)$.

Ainsi, de proche en proche, on construit la chaîne strictement croissante de sous-groupes de G :

$$(e) = Z_0 < Z_1 < Z_2 < Z_3 < \dots$$

Le groupe G étant fini, il existe nécessairement un entier s tel que $Z_s = G$, donc G est nilpotent.

B / Propriétés générales des groupes nilpotents

PROPOSITION (7.51). *Tout groupe nilpotent est résoluble. (La réciproque est fausse.)*

Preuve : Si G est un groupe nilpotent, il a une suite centrale, qui est une suite normale dont tous les quotients sont abéliens, puisque $\frac{G_i}{G_{i+1}} \leq Z\left(\frac{G}{G_{i+1}}\right)$.

G est donc résoluble (théorème (7.25)).

La réciproque est fausse; en effet, le groupe S_3 , par exemple, est résoluble (remarque (7.28)), mais $Z(S_3) = (e)$, donc S_3 n'a pas de suite centrale ascendante.

PROPOSITION (7.52). *Soient G un groupe nilpotent et Σ une suite centrale de G :*

$$\Sigma: \quad G = G_0 \geq G_1 \geq \dots \geq G_n = (e);$$

alors, pour tout i ($0 \leq i \leq n$), on a :

$$\Gamma_{n-i+1} \leq G_{n-i} \leq Z_i \tag{33}$$

Preuve : Dans la démonstration de théorème (7.47), nous avons prouvé que, pour tout i ($0 \leq i \leq n$), on a $\Gamma_{i+1} \leq G_i$ (relation 32); or, $0 \leq i \leq n$ implique $0 \leq n-i \leq n$; d'où

$$\Gamma_{n-i+1} \leq G_{n-i}, \quad \forall i (0 \leq i \leq n).$$

Il reste à montrer que $G_{n-i} \leq Z_i$ pour tout i ($0 \leq i \leq n$).

Pour $i = 0$, $G_n = (e) = Z_0$, donc la propriété considérée est vraie.

Raisonnons par récurrence sur i ; supposons $G_{n-i} \leq Z_i$ pour $0 \leq i \leq n-1$ et montrons que $G_{n-i-1} \leq Z_{i+1}$.

D'après la proposition (7.37), on a $[G_{n-i-1}, G] \leq G_{n-i}$; en utilisant l'hypothèse de récurrence, on obtient :

$$[G_{n-i-1}, G] \leq Z_i \quad (34)$$

Considérons le sous-groupe $G_{n-i-1} Z_i$ de G contenant Z_i et démontrons que :

$$[G_{n-i-1} Z_i, G] \leq Z_i \quad (35)$$

Soient $x \in G_{n-i-1}$, $y \in Z_i$, $z \in G$,

$$[xy, z] = y^{-1}[x, z]y[y, z] \quad (\text{exercice 31, chap. IV}).$$

$[x, z] \in [G_{n-i-1}, G]$, donc $[x, z] \in Z_i$, d'après (34).

$[y, z] \in [Z_i, G]$, or $Z_i \triangleleft G$ implique $[Z_i, G] \leq Z_i$, donc $[y, z] \in Z_i$, on en conclut que $[xy, z] \in Z_i$, ce qui prouve la relation (35).

On sait, d'autre part, que Z_{i+1} est le plus grand sous-groupe de G , contenant Z_i , tel que $[Z_{i+1}, G] \leq Z_i$, par suite, on a $G_{n-i-1} Z_i \leq Z_{i+1}$, d'où

$$G_{n-i-1} \leq Z_{i+1}.$$

THÉORÈME (7.53). *Si G est un groupe nilpotent, alors tout sous-groupe de G ainsi que tout quotient de G est nilpotent.*

Preuve : Soit Σ une suite centrale de G :

$$\Sigma: \quad G = G_0 \geq G_1 \geq \dots \geq G_n = (e).$$

— Soit $H \leq G$; montrons que :

$$H = G_0 \cap H \geq G_1 \cap H \geq \dots \geq G_n \cap H = (e)$$

est une suite centrale de H .

Dans Σ , on a, pour tout i ($0 \leq i \leq n-1$) :

$$[G_i, G] \leq G_{i+1} \quad (\text{proposition (7.37)})$$

$$\text{d'où} \quad [G_i \cap H, H] \leq H \cap [G_i, G] \leq H \cap G_{i+1}$$

et, d'autre part, $G_i \triangleleft G$ implique $G_i \cap H \triangleleft H$.

— Soit $N < G$; pour tout i ($1 \leq i \leq n$), on a
 $N < G_i N$ et $G_i N < G$;

de plus, pour $1 \leq i \leq n$, on vérifie que :

$$\left[\frac{G_i N}{N}, \frac{G}{N} \right] = \frac{[G_i, G]}{N} \leq \frac{G_{i-1} N}{N}$$

donc :

$$\frac{G}{N} = \frac{G_0 N}{N} \geq \frac{G_1 N}{N} \geq \dots \geq \frac{G_n N}{N} = \frac{N}{N}$$

est une suite centrale de $\frac{G}{N}$.

Remarque (7.54) : Il n'y a pas, pour les groupes nilpotents, de théorème analogue au théorème (7.29) relatif aux groupes résolubles. Il peut exister dans un groupe non nilpotent G un sous-groupe $N < G$, tel que N et $\frac{G}{N}$ soient nilpotents; par exemple, dans S_3 , l'unique sous-groupe N d'ordre 3 est d'indice 2, donc normal dans G ; N et $\frac{G}{N}$ sont abéliens, donc nilpotents, cependant S_3 n'est pas nilpotent (*contre-exemple* (7.51)). Mais il est possible de démontrer pour les groupes nilpotents un résultat semblable à celui du corollaire (7.30) [61].

Les propositions (7.55) et (7.56) montrent, par ailleurs, que les propriétés (7.31) à (7.33) se vérifient pour des groupes nilpotents.

PROPOSITION (7.55). *Soient deux groupes H et K , alors*

$$H \text{ et } K \text{ nilpotents} \Rightarrow H \times K \text{ nilpotent.}$$

Plus généralement, si $\{H_i\}_{1 \leq i \leq n}$ est une famille finie de groupes ($n \geq 2$ dans N), on a

$$\{H_i \text{ nilpotent, } \forall i (1 \leq i \leq n)\} \Rightarrow \prod_{1 \leq i \leq n} H_i \text{ nilpotent.}$$

Preuve : Soient, respectivement, Σ et Σ' des suites centrales de H et K :

$$\Sigma: \quad H = H_0 \geq H_1 \geq \dots \geq H_n = (e).$$

$$\Sigma: \quad K = K_0 \geq K_1 \geq \dots \geq K_m = (e').$$

Si $m \neq n$ et si, en particulier, $m < n$, on prolonge Σ' , par exemple en rajoutant $n - m$ sous-groupes $K_{m+j} = (e')$, $1 \leq j \leq n - m$; donc, sans restreindre la généralité, on peut supposer $m = n$. Pour tout i ($1 \leq i \leq n$) :

$$(H_i \triangleleft H \text{ et } K_i \triangleleft K) \Rightarrow H_i \times K_i \triangleleft H \times K$$

(exercice 3, chap. IV)

et $[H_i \times K_i, H \times K] = [H_i, H] \times [K_i, K]$

(exercice 16, chap. VII).

D'après la proposition (7.37), cette dernière relation implique :

$$[H_i \times K_i, H \times K] \leq H_{i+1} \times K_{i+1};$$

on en déduit que

$$H \times K = H_0 \times K_0 \geq H_1 \times H_2 \geq \dots \geq H_n \times K_n = (e, e')$$

est une suite centrale de $H \times K$, qui est donc nilpotent.

Par récurrence, on généralise la propriété au cas du produit direct d'une famille finie quelconque de groupes nilpotents.

PROPOSITION (7.56). *Soient H et K deux sous-groupes normaux d'un groupe G ; alors :*

$$\frac{G}{H} \text{ et } \frac{G}{K} \text{ nilpotents} \Rightarrow \frac{G}{H \cap K} \text{ nilpotent.}$$

Compte tenu de la proposition (7.55) et du théorème (7.53), la démonstration est la même que dans le cas des groupes résolubles (proposition (7.33)).

PROPOSITION (7.57). *Soit G un groupe nilpotent de classe r ; alors, quel que soit $H < G$, il existe une suite de composition de G vers H , de longueur r .*

Preuve : Considérons la suite centrale ascendante de G :

$$(e) = Z_0 < Z_1 < \dots < Z_r = G$$

et démontrons que :

$$G = HZ_r \geq HZ_{r-1} \geq \dots \geq HZ_0 = H$$

est une suite de composition de G vers H (définition (7.3)).

Pour $1 \leq i \leq r$, on a $\frac{Z_i}{Z_{i-1}} = Z\left(\frac{G}{Z_{i-1}}\right)$; or le centre d'un groupe est contenu dans le normalisateur de n'importe quel sous-groupe, donc :

$$\frac{Z_i}{Z_{i-1}} \leq N_{\frac{G}{Z_{i-1}}} \left(\frac{HZ_{i-1}}{Z_{i-1}} \right).$$

On en déduit :

$$\frac{HZ_{i-1}}{Z_{i-1}} \triangleleft \frac{HZ_{i-1}}{Z_{i-1}} \frac{Z_i}{Z_{i-1}}, \quad \text{d'où} \quad \frac{HZ_{i-1}}{Z_{i-1}} \triangleleft \frac{HZ_i}{Z_{i-1}}$$

et par suite $HZ_{i-1} \triangleleft HZ_i$.

Définition (7.58) : Dans un groupe G , un sous-groupe H sera dit *sous-normal*, s'il existe une suite de composition de G vers H .

Remarques (7.59) :

1° Dans un groupe G , tout sous-groupe normal H est sous-normal, car $G \geq H$ est une suite de composition de G vers H ; la réciproque est fautive (remarque (4.11)).

2° La proposition (7.57) exprime que tout sous-groupe d'un groupe nilpotent est sous-normal. On peut se demander si, réciproquement, un groupe dans lequel tout sous-groupe est sous-normal, est nilpotent. Nous verrons que la réponse est positive dans le cas des groupes *finis* (théorème (7.60)), mais elle est négative en général [38].

C / Groupes nilpotents finis

Dans le théorème ci-dessous, qui caractérise les groupes nilpotents finis, $\Phi(G)$ désigne le sous-groupe de Frattini de G (définition (4.56)), $D(G)$ étant le groupe dérivé de G :

THÉORÈME (7.60). G étant un groupe fini, les sept assertions suivantes sont équivalentes :

- 1) G est nilpotent ;
- 2) tout sous-groupe de G est sous-normal ;
- 3) $H < G \Rightarrow H < N_G(H)$;

- 4) tout sous-groupe maximal de G est normal dans G ;
 5) $D(G) \leq \Phi(G)$;
 6) tout sous-groupe de Sylow de G est normal dans G ;
 7) $G \simeq \prod_{1 \leq i \leq k} P_i$, $k \geq 1$ dans N , les ordres des groupes P_i étant des puissances de nombres premiers distincts p_i ($1 \leq i \leq k$).

Preuve :

1) \Rightarrow 2) : proposition (7.57).

2) \Rightarrow 3) : soit $H < G$, l'hypothèse 2) implique qu'il existe une suite de composition de G vers H ; sa longueur au moins égale à 1, puisque H est un sous-groupe propre de G :

$$G = H_0 > H_1 > \dots > H_n = H$$

$$(H \neq H_{n-1} \text{ et } H \triangleleft H_{n-1}) \Rightarrow H < H_{n-1} \leq N_G(H),$$

donc $H < N_G(H)$.

3) \Rightarrow 4) : soit M un sous-groupe maximal de G ; M est un sous-groupe propre de G ; d'après 3) on a donc $M < N_G(M)$, d'où $N_G(M) = G$ et par suite $M \triangleleft G$.

4) \Rightarrow 5) : par hypothèse, tout sous-groupe maximal M de G est normal dans G ; par suite, d'après la proposition (4.54), $\frac{G}{M}$ est cyclique d'ordre premier, donc abélien. On en déduit $D(G) \leq M$, quel que soit le sous-groupe maximal M de G , d'où $D(G) \leq \Phi(G)$.

5) \Rightarrow 4) : $D(G) \leq \Phi(G)$ implique $D(G) \leq M$, quel que soit le sous-groupe maximal M de G , d'où $\frac{M}{D(G)}$ sous-groupe du groupe abélien $\frac{G}{D(G)}$; alors :

$$\frac{M}{D(G)} \triangleleft \frac{G}{D(G)} \Rightarrow M \triangleleft G.$$

4) \Rightarrow 6) : soit P un p -sous-groupe de Sylow de G ; supposons $N_G(P) < G$; d'après la proposition (4.50), il existe un sous-groupe maximal M de G contenant $N_G(P)$:

$$P < N_G(P) \leq M < G.$$

En appliquant le corollaire (6.11), on obtient alors :

$$N_G(M) = M,$$

ce qui est contraire à l'hypothèse $M < G$.

On en conclut que $N_G(P) = G$, c'est-à-dire $P \triangleleft G$.

6) \Rightarrow 7) : l'hypothèse implique que, pour tout nombre premier p divisant $o(G)$, il existe un unique p -sous-groupe de Sylow dans G . D'après le théorème (6.18), on a $G \simeq \prod_{1 \leq i \leq k} P_i$, où les P_i sont les p_i -sous-groupes de Sylow distincts de G .

7) \Rightarrow 1) : on sait que tout p -groupe fini est nilpotent (proposition (7.50)), on en déduit, en appliquant la proposition (7.55), que $G \simeq \prod_{1 \leq i \leq k} P_i$, où les P_i sont des p_i -groupes finis, est nilpotent.

Sous-groupe de Frattini d'un groupe fini :

LEMME (7.61). *Soit $G \neq (e)$, un groupe fini et $N < G$; alors $N \leq \Phi(G)$ si et seulement s'il n'existe aucun sous-groupe propre H de G tel que $HN = G$.*

Preuve : Supposons $N \leq \Phi(G)$ et soit $H < G$. Il existe un sous-groupe maximal M de G contenant H :

$$N \leq \Phi(G) \Rightarrow N \leq M, \quad \text{d'où } HN \leq M < G;$$

il n'existe donc aucun sous-groupe propre H de G tel que $HN = G$.

Supposons maintenant $N \not\leq \Phi(G)$; on a $G \neq (e)$ et, par hypothèse, il existe un sous-groupe maximal M de G tel que $N \not\leq M$; d'où $M < MN \leq G$ et par suite $MN = G$, puisque M est maximal. Ainsi $N \not\leq \Phi(G)$ implique l'existence d'un sous-groupe propre M de G , tel que $MN = G$.

THÉORÈME (7.62) (Frattini). *Pour tout groupe fini G , $\Phi(G)$ est un groupe nilpotent.*

Preuve : On suppose $G \neq (e)$.

D'après la proposition (4.58), on a $\Phi(G) < G$; alors, si P est un p -sous-groupe de Sylow de $\Phi(G)$, le lemme (6.10) de Frattini implique $G = N_G(P) \Phi(G)$.

Compte tenu du lemme (7.61), on en déduit que $N_G(P) = G$; d'où $P \triangleleft G$, donc $P \triangleleft \Phi(G)$; par suite, $\Phi(G)$ est nilpotent (théorème (7.60) 6°).

Exercices Chapitre VII

- 1) Dans un groupe $G \neq (e)$, on dit qu'un sous-groupe K est *normal minimal*, s'il est minimal dans l'ensemble des sous-groupes normaux de G , distincts de (e) ; donc :

$$(K' \triangleleft G \text{ et } K' \leq K) \Rightarrow K' = (e) \text{ ou } K' = K.$$

a) Si K est un sous-groupe normal minimal de G , vérifier que K est abélien, ou $Z(K) = (e)$.

b) Si K et L sont deux sous-groupes normaux minimaux distincts de G , montrer que KL est un sous-groupe de G isomorphe à $K \times L$.

c) Prouver que le groupe $(\mathbb{Z}, +)$ n'a pas de sous-groupe normal minimal.

- 2) Soit G un groupe; soit $H \triangleleft G$, $N \triangleleft G$ tels que $N \subset H$; démontrer que $\frac{H}{N}$ est normal minimal dans $\frac{G}{N}$, si et seulement si N est maximal dans l'ensemble des sous-groupes normaux de G , strictement inclus dans H .

- 3) Un groupe G sera dit *caractéristiquement simple*, si $G \neq (e)$ et si les seuls sous-groupes caractéristiques de G sont (e) et G .

a) Soit K un sous-groupe normal minimal d'un groupe G ; démontrer que K est un groupe caractéristiquement simple. [Utiliser la proposition (4.44).]

b) K étant un corps, on considère le groupe additif $(K, +)$. Vérifier que, pour tout $a \neq 0$ dans K , l'application $\lambda_a : K \rightarrow K$ telle que $\lambda_a(x) = ax$, quel que soit $x \in K$, est un automorphisme du groupe $(K, +)$.

Montrer que $(K, +)$ est caractéristiquement simple.

c) Prouver que le groupe $(\mathbb{Z}, +)$ n'est pas caractéristiquement simple (voir l'exercice 17, chap. III).

d) Démontrer que si un groupe G est caractéristiquement simple, il en est de même du groupe $G \times G$.

4) Etant donné une suite de composition d'un groupe G :

$$\Sigma : G = G_0 > G_1 > \dots > G_n = (e),$$

on dit que Σ est une *suite principale* de G , si Σ est une suite normale de G , telle que, pour tout i ($1 \leq i \leq n$) $\frac{G_{i-1}}{G_i}$ est normal minimal dans $\frac{G}{G_i}$ (voir exercices 1 et 2, ci-dessus).

Soit G le sous-groupe du groupe symétrique S_4 , engendré par $\{(1, 2), (5, 6), (1, 3), (2, 4)\}$.

a) Vérifier que $(3, 4) \in G$.

b) Soit H le sous-groupe de G engendré par $\{(1, 2), (3, 4), (5, 6)\}$. Prouver que :

$$G \supset H \supset \langle (1, 2), (5, 6) \rangle \supset \langle (1, 2) \rangle \supset (e)$$

est une suite de Jordan-Hölder de G .

Vérifier que cette suite n'est pas principale et qu'aucune suite extraite de celle-ci n'est principale.

5) Etant donné la famille des groupes symétriques S_n , $n \in \mathbb{N}^*$, pour $1 \leq m < n$, on identifie S_m au sous-groupe de S_n , formé par l'ensemble des permutations σ de $\{1, 2, \dots, n\}$, telles que $\sigma(i) = i$, pour tout i ($m+1 \leq i \leq n$); on considère alors le groupe :

$$S = \bigcup_{n \in \mathbb{N}^*} S_n.$$

a) Le groupe S est-il résoluble?

Vérifier que S est isomorphe au sous-groupe $S_{(\mathbb{N}^*)}$ du groupe symétrique $S_{\mathbb{N}^*}$, formé par l'ensemble des permutations de \mathbb{N}^* à support fini (exercice 17, chap. IV).

b) Démontrer que $A = \bigcup_{n \in \mathbb{N}^*} A_n$ est l'unique sous-groupe propre normal de S , autre que (e) , et que A est d'indice 2 dans S .

Prouver que S est un groupe de longueur 2 (définition (7.14)).

c) Soit H le sous-groupe de S engendré par l'ensemble des transpositions : $\{(2n-1, 2n); n \in \mathbb{N}^*\}$.

Vérifier que H est un groupe abélien, infini, et que toute suite de composition de H a un raffinement propre. En déduire que H n'a pas de suite de Jordan-Hölder.

d) A tout $\sigma \in A$, on associe $\varphi_\sigma \in \text{End}(H)$, tel que :

$$\varphi_\sigma : (2m-1, 2m) \mapsto (2n-1, 2n), \quad \text{où } n = \sigma(m).$$

Pour tout $u \in H$, on écrira : $\varphi_\sigma(u) = u^\sigma$.

— Vérifier que $\varphi_\sigma \in \text{Aut}(H)$, quel que soit $\sigma \in A$.

— On considère alors le groupe $G = H \rtimes_\varphi A$ (produit semi-direct).

Montrer qu'il existe un sous-groupe H' de G , isomorphe à H , tel que $G \supset H' \supset (e)$ est une suite principale de G .

Prouver que G n'a pas de suite de Jordan-Hölder.

- 6) On dira qu'un groupe G vérifie les « conditions de chaînes » s'il satisfait aux *deux conditions* suivantes :

(C_1) : toute chaîne strictement décroissante de sous-groupes de G :

$$G = G_0 \supset G_1 \supset \dots \supset G_i \supset G_{i+1} \dots$$

où $G_i \triangleleft G_{i-1}$, pour tout i , est finie.

(C_2) : toute chaîne strictement croissante de sous-groupes de G :

$$(e) = H_0 \subset H_1 \subset \dots \subset H_j \subset H_{j+1} \subset \dots$$

où $H_j \triangleleft H_{j+1}$, pour tout j , est finie.

1° G étant un groupe vérifiant les « conditions de chaînes », démontrer les propriétés suivantes :

a) Tout sous-groupe de G et tout quotient de G vérifient les « conditions de chaînes ».

b) Tout sous-groupe normal de G est contenu dans un sous-groupe normal maximal de G et contient un sous-groupe normal minimal de G .

En déduire qu'en particulier, G contient un sous-groupe normal maximal et un sous-groupe normal minimal.

2° Montrer qu'un groupe G vérifie les « conditions de chaînes », si et seulement si G a une suite de Jordan-Hölder.

- 7) Soit G un groupe vérifiant les « conditions de chaînes » (voir exercice précédent). Soit K un sous-groupe normal minimal de G .

Le but des questions qui suivent est de prouver que K est un groupe simple ou est isomorphe au produit direct d'un nombre fini de sous-groupes simples de G , deux à deux conjugués.

On suppose que K n'est pas simple.

a) Justifier l'existence dans le groupe K d'un sous-groupe normal minimal N . Prouver que pour tout $x \in G$, $x N x^{-1}$ est encore un sous-groupe normal minimal de K .

b) N étant un sous-groupe normal minimal de K , montrer qu'il existe $x_1 \in G$ tel que $x_1 N x_1^{-1} \not\subseteq N$.

On pose alors $N_0 = N$ et $N_1 = N(x_1 N x_1^{-1})$.

Vérifier que $N_1 \triangleleft K$.

Si l'on choisit $x_2 \in G$, tel que $x_2 N x_2^{-1} \not\subseteq N_1$, et si l'on pose $N_2 = N_1(x_2 N x_2^{-1})$, prouver que $N_2 \triangleleft K$.

On construit ainsi une chaîne strictement croissante :

$$N_0 < N_1 < N_2 < \dots$$

Justifier l'existence de $n \in \mathbb{N}^*$ tel que $N_n = K$.

En déduire que l'on a

$$K \simeq N \times x_1 N x_1^{-1} \times x_2 N x_2^{-1} \times \dots \times x_n N x_n^{-1}$$

où N est simple, ainsi que les groupes $x_i N x_i^{-1}$ ($1 \leq i \leq n$).

- 8) Soit G un groupe vérifiant les « conditions de chaînes » (voir exercices 6 et 7 ci-dessus).

Démontrer que G a une suite principale dont chaque quotient est simple ou isomorphe au produit direct d'un nombre fini de groupes simples.

- 9) Trouver deux raffinements équivalents pour les deux suites de composition de \mathbf{Z} :

$$\mathbf{Z} > p\mathbf{Z} > (0) \quad \text{et} \quad \mathbf{Z} > q\mathbf{Z} > (0)$$

où p et q sont des nombres premiers distincts.

- 10) Déterminer, à un isomorphisme près, tous les groupes d'ordre 20; montrer qu'ils sont de même longueur et résolubles.

- 11) Démontrer que pour tout entier $n \geq 2$, le groupe diédral D_n est résoluble.

- 12) Pour $n \geq 3$, on considère le groupe diédral D_n engendré par a et b tels que $o(a) = n$, $o(b) = o(ab) = 2$.

On pose $G = \text{Aut}(D_n)$.

a) Vérifier que $\langle a \rangle$ est un sous-groupe caractéristique de D_n .

b) Soit $N = \{ \alpha \in G; \alpha(a) = a \}$. Démontrer que N est un sous-groupe normal de G , abélien et d'ordre n .

c) Soit $H = \{ \alpha \in G; \alpha(b) = b \}$. Prouver que H est un sous-groupe de G , abélien et d'ordre $\varphi(n)$ (voir exercice 17, chap. III).

d) Vérifier que G est produit semi-direct de N par H .

e) Prouver que G est résoluble.

- 13) Soient p et q deux nombres premiers distincts. Démontrer que :
- Tout groupe d'ordre pq est résoluble.
 - Tout groupe d'ordre p^2q est résoluble (voir, chap. VI : proposition (6.15) et exercice 8).
- 14) Vérifier que le groupe linéaire général $GL(2, Z_2)$, où $Z_2 = \frac{Z}{2Z}$, est résoluble (voir exercice 22, chap. I).
- 15) On considère le groupe linéaire général $G = GL(2, Z_3)$, où $Z_3 = \frac{Z}{3Z}$.
- Démontrer que G est fini, d'ordre 48.
 - Soit $S = SL(2, Z_3)$, le groupe linéaire spécial des matrices d'ordre 2 sur Z_3 (voir exemple (1.63)).
Vérifier que S est un sous-groupe de G , d'ordre 24.
 - Quel est l'ordre du centre de G ? (voir exercice 37, chap. IV).
 - Prouver que S est résoluble et en déduire que G est résoluble.
- 16) Soient deux groupes H et K ; soit $H' \leq H$ et $K' \leq K$, démontrer que $[H' \times K', H \times K] = [H', H] \times [K', K]$.
- 17) a) Soit un groupe G et $K \triangleleft G$; π étant l'épimorphisme canonique $G \rightarrow \frac{G}{K}$, on sait que $D\left(\frac{G}{K}\right) = \pi(D(G))$. Prouver que :
- $K \subseteq Z(G)$ et $\frac{G}{K}$ monogène implique G abélien.
- b) On suppose que pour le groupe G , on a $\frac{D(G)}{D_2(G)}$ et $D_2(G)$ monogènes.
- Déterminer $D_3(G)$.
- Si a est un générateur du groupe $D_2(G)$, montrer que l'on a $D(G) \subseteq C_G(a)$ (voir exercice 25, chap. IV).
En déduire que $D_2(G) \subseteq Z(D(G))$. En conclure que $D_2(G) = (e)$.
- c) On suppose que pour le groupe G , il existe $i \geq 2$ tel que $\frac{D_{i-1}(G)}{D(G)}$ et $\frac{D_i(G)}{D_{i+1}(G)}$ sont monogènes.
- En utilisant le groupe $\frac{D_{i-2}(G)}{D_{i+1}(G)}$, démontrer que $\frac{D(G)}{D_{i+1}(G)} = (e)$.
- d) On considère le groupe S_3 ; démontrer (sans calcul sur les éléments) que
- $$D(S_3) = \{e, \sigma_1, \sigma_2\},$$
- où $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

En conclure que pour un groupe G , la condition : « $\frac{G}{D(G)}$ et $D(G)$ monogènes » n'implique pas $D(G) = (e)$.

e) Vérifier que tout groupe G , pour lequel $\frac{G}{D(G)}$ et $D(G)$ sont monogènes, est résoluble.

- 18) Soit G un groupe fini dont tout sous-groupe de Sylow est cyclique, c'est-à-dire que G est *hypercyclique* (voir exercice 19, chap. VI); on suppose de plus G non abélien et tel que $D(G) \neq G$.

a) Montrer que S_3 satisfait à l'ensemble des conditions imposées au groupe G .

b) Vérifier que $D(G)$ et $\frac{G}{D(G)}$ sont hypercycliques; en déduire que $\frac{G}{D(G)}$ et $\frac{D(G)}{D_2(G)}$ sont cycliques; en conclure que $D_3(G) = D_2(G)$ (voir exercice 17, ci-dessus).

c) On pose $n = o(G)$; montrer que l'on a nécessairement $n \geq 6$ et prouver, par récurrence sur n , que G est résoluble. En déduire que $D_3(G) = D_2(G) = (e)$.

En conclure que si G est un groupe fini non abélien, hypercyclique, tel que $D(G) \neq G$, alors $D(G)$ et $\frac{G}{D(G)}$ sont cycliques.

- 19) Soit G un groupe fini d'ordre $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, où $k, \alpha_1, \alpha_2, \dots, \alpha_k$ sont des entiers positifs, les p_i ($1 \leq i \leq k$) étant des nombres premiers distincts. Démontrer que G est résoluble, si et seulement si G est de longueur $n = \sum_{i=1}^k \alpha_i$.

- 20) Soit $\mathcal{I}(2)$ le groupe des isométries du plan affine euclidien P (exercice 26, chap. I).

Soit $\mathcal{D}(2)$ le groupe des déplacements du plan P (exercice 7, chap. II) et $\mathcal{E}(P)$ le groupe des translations de P .

a) Démontrer que l'on a $\mathcal{E}(P) \triangleleft \mathcal{I}(2)$, donc $\mathcal{E}(P) \triangleleft \mathcal{D}(2)$.

b) Prouver que $\frac{\mathcal{D}(2)}{\mathcal{E}(P)} \simeq \mathcal{R}(P, \omega)$, groupe des rotations du plan P , de centre fixe ω (on montrera qu'une classe de $\mathcal{D}(2)$ modulo $\mathcal{E}(P)$, autre que $\mathcal{E}(P)$, est formée par l'ensemble des rotations $r(O, \alpha)$ où O décrit P et α est fixe). Quel est le groupe dérivé de $\mathcal{D}(2)$?

c) Vérifier que $\mathcal{I}(2)$ est un groupe résoluble; est-il nilpotent?

- 21) Soit $(G, +)$ un groupe *abélien*. On dit que G est un groupe abélien *élémentaire* s'il existe un nombre premier p tel que $px = 0$, quel que soit $x \in G$; dans ce cas, on dit, plus précisément, que G est *p -élémentaire*.

a) $(G, +)$ étant un groupe abélien *p -élémentaire*, montrer que G peut être muni, de façon naturelle, d'une structure d'espace vectoriel sur le corps $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$.

Réciproquement, vérifier que tout espace vectoriel V sur \mathbb{Z}_p est tel que $(V, +)$ est un groupe abélien *p -élémentaire*.

b) Démontrer que, pour un groupe *abélien fini* $(G, +) \neq (0)$, les deux conditions suivantes sont équivalentes :

- (1) G est élémentaire.
- (2) G est caractéristiquement simple (voir exercice 3, ci-dessus).

[(1) \Rightarrow (2) : Considérer G comme un espace vectoriel de dimension finie sur \mathbb{Z}_p . Pour G non isomorphe à \mathbb{Z}_p , $H < G$, $H \neq (0)$, vérifier que si $x \in H \setminus \{0\}$ et $y \notin H$, il existe $\alpha \in \text{Aut}(G)$ tel que $\alpha(x) = y$.

(2) \Rightarrow (1) : Si p premier divise $o(G)$, poser $K = \{x \in G; px = 0\}$ et montrer que K est un sous-groupe caractéristique non nul de G .]

- 22) Soit un groupe $G \neq (e)$.

a) Démontrer que deux suites normales de G admettent des raffinements équivalents, qui sont encore des suites normales de G . [Voir la démonstration du théorème de Schreier.]

b) Prouver que si G a une suite principale (exercice 4 ci-dessus), alors toute suite normale strictement décroissante de G a un raffinement qui est une suite principale de G ; en déduire que deux suites principales de G sont équivalentes.

c) Prouver que tout groupe fini $G \neq (e)$ a une suite principale.

d) Démontrer que pour tout groupe *fini* $G \neq (e)$, les deux conditions suivantes sont équivalentes :

- (1) G est résoluble.
- (2) Tous les quotients d'une suite principale de G sont abéliens élémentaires (exercice 21, ci-dessus).

- 23) Soit Q_8 le groupe des quaternions et C_2 un groupe cyclique d'ordre 2. Prouver que $G = Q_8 \times C_2$ est nilpotent.

Déterminer les suites centrales ascendantes et descendantes de G ; on remarquera que ces suites sont distinctes; en déduire la classe de nilpotence de G .

24) a) p étant un nombre premier, vérifier que tout groupe fini d'ordre p^n , $n \geq 1$ dans N , est nilpotent de classe $r \leq n - 1$. [Raisonnement par récurrence sur n .]

b) Soit $n = 2^k$, $k \geq 2$ dans N . On considère le groupe diédral D_n engendré par a et b tels que

$$o(a) = n, \quad o(b) = o(ab) = 2.$$

— Justifier l'affirmation : D_n est nilpotent de classe $r \leq k$.

— Montrer que $Z_1 = Z(D_n)$ est le sous-groupe de D_n engendré par $a^{2^{k-1}}$ (voir exercice 20, chap. IV).

— Déterminer la suite centrale ascendante de D_n ; en déduire que D_n est nilpotent de classe k .

c) Montrer que pour $n \geq 3$ et impair, D_n n'est pas nilpotent; en déduire que D_n est nilpotent si et seulement si $n = 2^k$, $k \geq 1$ dans N .

d) Démontrer que le groupe dicyclique Q_{4n} (exercice 25, chap. V) est nilpotent si et seulement si $n = 2^k$, $k \geq 1$ dans N ; quelle est alors la classe de nilpotence de Q_{4n} ?

25) Vérifier que pour $n \geq 3$, le groupe symétrique S_n n'est pas nilpotent.

26) Soit K un sous-groupe normal minimal d'un groupe $G \neq (e)$.

a) Montrer que $[K, G] = K$, ou $[K, G] = (e)$.

b) On considère la famille des sous-groupes Γ_n de G définis par les relations (19); vérifier que, si $[K, G] = K$, alors, pour tout $n \in N^*$, on a $K \subseteq \Gamma_n$.

En déduire que, si le groupe G est nilpotent, alors $K \subseteq Z(G)$.

27) A l'aide de l'exercice 26, démontrer que pour un groupe fini G , les deux conditions suivantes sont équivalentes :

(1) G est nilpotent.

(2) Toute suite principale de G est centrale.

28) Démontrer que si G est un groupe nilpotent de classe 2, alors $D(G)$ est abélien.

29) G étant un groupe, on dira que G est *super-résoluble* si G a une suite normale Σ dont tous les quotients sont monogènes (finis ou infinis).

Pour un groupe super-résoluble une telle suite Σ sera dite « normale monogène ».

1° Justifier les propriétés suivantes :

- a) G groupe super-résoluble $\Rightarrow G$ groupe résoluble;
- b) quel que soit le nombre premier p , tout p -groupe fini est super-résoluble.

2° Soit G un groupe super-résoluble. Démontrer que :

- a) tout sous-groupe H de G est super-résoluble;
- b) quel que soit $N \triangleleft G$, $\frac{G}{N}$ est super-résoluble.

3° En considérant le groupe symétrique S_4 , montrer que :

- a) la réciproque du 1° a) est fausse;
- b) un groupe non super-résoluble peut contenir un sous-groupe normal N tel que N et $\frac{G}{N}$ sont super-résolubles.

4° a) Démontrer que si H et K sont deux groupes super-résolubles, alors $H \times K$ est super-résoluble.

Généraliser cette propriété au cas du produit direct d'un nombre fini de groupes super-résolubles.

b) Prouver que tout groupe *fini* nilpotent est super-résoluble.

5° G étant un groupe super-résoluble, soit Σ une suite normale monogène de G :

$$\Sigma : G = G_0 > G_1 > \dots > G_n = (e).$$

a) Soit Σ' un raffinement de Σ ; démontrer que tous les quotients de la suite de composition Σ' sont monogènes et que Σ' a le même nombre de quotients infinis que Σ .

[On prouvera que si $\frac{G_i}{G_{i+1}}$ est isomorphe à \mathbf{Z} et si dans Σ' on a

$$G_i = H_0 > H_1 > \dots > H_k = G_{i+1},$$

alors, $\frac{H_{k-1}}{H_k} \simeq \mathbf{Z}$ et $\frac{H_j}{H_{j+1}}$ est cyclique quel que soit j ($0 \leq j \leq k-2$).]

b) Montrer que deux suites normales monogènes d'un groupe super-résoluble G ont le même nombre de quotients infinis.

6° a) G étant un groupe super-résoluble, on considère, comme dans 5°, une suite normale monogène Σ de G . Si $\frac{G_i}{G_{i+1}}$ est un

quotient *cyclique* de Σ , démontrer qu'il existe une suite de composition de G_i vers G_{i+1} :

$$G_i = H_0 > H_1 > \dots > H_k = G_{i+1}$$

dans laquelle chaque quotient $\frac{H_j}{H_{j+1}}$ ($0 \leq j \leq k-1$) est cyclique d'ordre premier.

Vérifier que pour tout j ($0 \leq j \leq k$), $\frac{H_j}{G_{i+1}}$ est caractéristique dans $\frac{G_i}{G_{i+1}}$; en déduire que pour tout j ($0 \leq j \leq k$) on a $H_j \triangleleft G$.

b) Prouver qu'un groupe G est super-résoluble si et seulement s'il a une suite normale monogène dans laquelle tous les quotients finis sont cycliques d'ordre premier.

30) Soit G un groupe super-résoluble (exercice 29, ci-dessus). Le but de cet exercice est de prouver que $D(G)$ est nilpotent.

Soit Σ une suite normale monogène de G :

$$G = G_0 > G_1 > \dots > G_n = (e).$$

Pour tout i ($0 \leq i \leq n$), on pose $A_i = G_i \cap D(G)$.

a) Vérifier que

$$\Sigma_1 : D(G) = A_0 > A_1 > \dots > A_n = (e)$$

est une suite normale monogène de $D(G)$.

b) Pour tout i ($0 \leq i \leq n-1$), on considère l'application

$$\gamma : G \mapsto \text{Aut} \left(\frac{A_i}{A_{i+1}} \right)$$

$$g \mapsto \gamma_g$$

tel que, pour tout $\bar{x} \in \frac{A_i}{A_{i+1}}$:

$$\gamma_g(\bar{x}) = \bar{g} \bar{x} \bar{g}^{-1},$$

où \bar{g} est la classe de g modulo A_{i+1} dans G .

Soit $K = \text{Ker } \gamma$.

— Vérifier que $\frac{G}{K}$ est abélien (voir exercice 17, chap. III) et

que $\frac{K}{A_{i+1}}$ est le centralisateur de $\frac{A_i}{A_{i+1}}$ dans $\frac{G}{A_{i+1}}$.

— En déduire que Σ_1 est une suite centrale et donc que $D(G)$ est nilpotent.

- 31) Soit $n \geq 2$ dans \mathbb{N} . Soit K_n le sous-groupe de $GL(2, \mathbb{C})$ engendré par les matrices

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad Y = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$$

où $\varepsilon \in \mathbb{C}$, $\varepsilon^{2n} = 1$ et $\varepsilon^{2n-1} \neq 1$.

a) Démontrer que le groupe K_n est non abélien, d'ordre 2^{n+1} . Quel est le groupe K_2 ?

b) Prouver que pour tout $n \geq 2$, K_n est un groupe dicyclique (exercice 25, chap. V).

En déduire que K_n est nilpotent de classe n (exercice 24, ci-dessus).

c) Vérifier que $K = \bigcup_{n \geq 2} K_n$ est un sous-groupe de $GL(2, \mathbb{C})$. Déterminer $D(K)$; en déduire que K n'est pas nilpotent.

- 32) Soit $\Phi(G)$ le sous-groupe de Frattini d'un groupe G ; on suppose $\Phi(G) \neq G$.

a) Montrer que :

$$H \triangleleft G \text{ et } H \subseteq \Phi(G) \Rightarrow \Phi\left(\frac{G}{H}\right) = \frac{\Phi(G)}{H}.$$

b) Un élément $x \in G$ sera dit *superflu* dans G , si, S désignant une partie non vide de G , x est tel que :

$$S \cup \{x\} \text{ engendre } G \Rightarrow S \text{ engendre } G.$$

Soit E l'ensemble des éléments superflus de G .

— Démontrer que $E \subseteq \Phi(G)$ [raisonner « par l'absurde »].

— Soit $x \in G$ tel que $x \notin E$ et soit S une partie non vide de G telle que $\langle S \cup \{x\} \rangle = G$ et $\langle S \rangle \neq G$.

On pose $\mathcal{H} = \{H; H < G, \langle S \rangle \subseteq H \text{ et } x \notin H\}$.

Démontrer, en utilisant l'axiome de Zorn (voir énoncé (4.60)), que \mathcal{H} contient un élément maximal M , qui est un sous-groupe maximal de G .

En déduire que $\Phi(G) = E$.

c) Prouver que si G est tel que $\Phi(G)$ est de type fini, alors :

$$(H \leq G \text{ et } H\Phi(G) = G) \Rightarrow H = G.$$

d) Soit G un groupe tel que tout sous-groupe propre de G est de type fini.

Démontrer (« par l'absurde ») les deux propriétés suivantes :

- si H est un sous-groupe *non* normal de G , alors il existe $g \in G$ tel que :

$$\forall x \in \Phi(G), \quad g H g^{-1} \neq x H x^{-1}.$$

- $H \triangleleft G \Rightarrow \Phi(H) \subseteq \Phi(G)$.

- 33) Déterminer le sous-groupe de Frattini de chacun des groupes suivants :

- a) \mathbb{Z} et C_n groupe cyclique d'ordre $n \geq 2$;
- b) S_n , groupe symétrique de degré $n \geq 3$;
- c) D_n , groupe diédral d'ordre $2n$, $n \geq 2$;
- d) C_{p^∞} , p -groupe de Prüfer (exercices 34 et 36, chap. IV);
- e) Q_8 , le groupe des quaternions, et K_n le groupe dicyclique défini dans l'exercice 31, ci-dessus, pour $n \geq 3$.

- 34) p étant un nombre premier, soit G un p -groupe fini ($G \neq (e)$). Démontrer que $\Phi(G) = (e)$ si et seulement si G est un groupe abélien p -élémentaire (voir exercice 21, ci-dessus).

En déduire que pour tout p -groupe fini G , $\frac{G}{\Phi(G)}$ est un groupe abélien p -élémentaire (voir le a) de l'exercice 32, ci-dessus).

- 35) a) Soit G un groupe tel que $\Phi(G)$ est de type fini et $\Phi(G) \neq G$.

Démontrer que si $\frac{G}{\Phi(G)}$ est de type fini, engendré par au moins n éléments, alors G est de type fini, engendré par au moins n éléments (voir le b) de l'exercice 32, ci-dessus).

b) Soit $G = C_{2^\infty} \times_{\varphi} C_2$, le produit semi-direct du groupe quasi-cyclique C_{2^∞} (exercices 34 et 36, chap. IV) par le groupe $C_2 = \{1, -1\}$, φ étant le morphisme : $C_2 \rightarrow \text{Aut}(C_{2^\infty})$ tel que, pour tout $z \in C_{2^\infty}$, $\varphi_1(z) = z$ et $\varphi_{-1}(z) = z^{-1}$.

Déterminer $\Phi(G)$; vérifier que $\frac{G}{\Phi(G)}$ est fini, alors que G n'est pas de type fini (comparer ce résultat avec a)).

Déterminer $Z(G)$; en déduire que G n'est pas nilpotent.

CHAPITRE VIII

Groupes abéliens

Conformément à l'usage, dans tout ce chapitre, la loi de composition d'un groupe abélien sera notée *additivement*, l'élément neutre étant 0.

Cette notation peut se justifier par le fait que la structure de groupe abélien intervient dans d'autres structures algébriques fondamentales telles que celles des anneaux, des espaces vectoriels, des modules, qui sont tous (conventionnellement) des groupes additifs abéliens (voir la définition de ces structures dans [31] ou [54], par exemple).

En particulier, si A est un anneau unitaire et commutatif, un A -module est un groupe additif abélien, muni d'une loi de composition externe :

$$\begin{aligned} A \times M &\rightarrow M \\ (a, x) &\mapsto ax \end{aligned}$$

telle que

$$\left. \begin{aligned} a(x+y) &= ax+ay \\ (a+b)x &= ax+bx \\ (ab)x &= a(bx) \\ 1x &= x \end{aligned} \right\} \forall (a,b) \in A \times A, \forall (x,y) \in M \times M.$$

Compte tenu des propriétés élémentaires des groupes (formules (2') et (3'), chap. I), on vérifie facilement que la *structure de groupe (additif) abélien coïncide avec celle de \mathbf{Z} -module*.

Ce point de vue explique qu'il y ait plusieurs méthodes pour aborder l'étude des groupes abéliens, dont les résultats peuvent être obtenus, en particulier, comme conséquences directes de la Théorie des Modules sur un anneau principal (voir [37], [41]).

Pour conserver une certaine unité à ce livre, nous avons préféré ne pas trop nous écarter de la Théorie des Groupes; cependant, la décomposition des groupes abéliens de type fini utilisera certaines propriétés des matrices à coefficients dans \mathbb{Z} , que nous rappellerons.

1 — Somme directe de groupes abéliens

A / Notion de somme directe de groupes abéliens

Soit $\{G_i\}_{i \in I}$ une famille de groupes abéliens, I étant un ensemble non vide quelconque.

Considérons le groupe produit direct $G = \prod_{i \in I} G_i$, auquel on associe la famille des épimorphismes canoniques $\{p_i\}_{i \in I}$ et celle des monomorphismes canoniques $\{q_i\}_{i \in I}$ (voir chap. I, paragr. 4).

Considérons dans $G = \prod_{i \in I} G_i$, la famille des sous-groupes $\{\text{Im } q_i\}_{i \in I}$ et posons :

$$\Gamma = \sum_{i \in I} \text{Im } q_i.$$

Γ est, par définition, le sous-groupe de G engendré par $\bigcup_{i \in I} \text{Im } q_i$ (voir chap. I).

Compte tenu de la définition des q_i , on a :

$$\text{pour tout } j \in I, \quad \text{Im } q_j \cap \sum_{\substack{i \in I \\ i \neq j}} \text{Im } q_i = (0),$$

donc Γ est somme directe des sous-groupes $\text{Im } q_i$ de G (définition (1.52)) :

$$\Gamma = \bigoplus_{i \in I} \text{Im } q_i \quad (1)$$

D'après la proposition (1.53), tout $x \in \Gamma$ s'écrit de façon unique :

$$x = \sum_{1 \leq j \leq n} q_{ij}(x_{ij}), \quad \text{où } n \in \mathbf{N}^* \text{ et } \{i_1, i_2, \dots, i_n\} \subseteq I.$$

On en déduit que :

$$\Gamma = \{x \in \prod_{i \in I} G_i; p_i(x) = 0, \text{ sauf pour un nombre fini d'indices } i\}.$$

Définition (8.1) : Etant donné une famille $\{G_i\}_{i \in I}$ de groupes abéliens, où I est un ensemble non vide quelconque, le sous-groupe Γ du groupe $\prod_{i \in I} G_i$, formé par l'ensemble des $x \in \prod_{i \in I} G_i$ qui n'ont qu'un nombre fini de composantes non nulles, est appelé *somme directe des groupes abéliens G_i , $i \in I$* ; on écrit alors

$$\Gamma = \bigoplus_{i \in I} G_i \quad (2)$$

Remarques (8.2) :

1° Dans la formule (1), le signe \bigoplus exprime une *somme directe de sous-groupes*, alors que dans la formule (2), le même signe \bigoplus exprime une *somme directe de groupes*. Eventuellement, pour éviter toute ambiguïté, on dit parfois qu'il s'agit, dans le premier cas, d'une somme directe « *interne* » et, dans le second cas, d'une somme directe « *externe* ».

2° On a $\bigoplus_{i \in I} G_i \leq \prod_{i \in I} G_i$ et $\bigoplus_{i \in I} G_i = \prod_{i \in I} G_i$ si et seulement si I est fini.

Notations (8.3) : Soit G un groupe abélien.

— Pour $n \geq 2$ dans \mathbf{N} , on note G^n la somme directe de n groupes égaux à G : on dit de n « *copies de G* ».

— Si I est un ensemble non vide quelconque, on désigne par G^I le produit direct $\prod_{i \in I} G_i$, où $G_i = G$, quel que soit $i \in I$, c'est-à-dire, où tout G_i est une copie de G .

On note alors $G^{(I)}$ le sous-groupe de G^I égal à $\bigoplus_{i \in I} G_i$, où chaque G_i est une copie de G .

Remarque (8.4) : D'après la remarque (8.2) 2°, on a $G^{(I)} \leq G^I$ et

$$G^{(I)} = G^I \Leftrightarrow I \text{ est fini};$$

de plus si $I = \{i_1, \dots, i_n\}$, où $n \in \mathbb{N}^*$, alors $G^I = G^n$, car tout élément de G^I est un élément de G^n et réciproquement. Plus généralement, si I et J sont deux ensembles non vides tels que

$$\text{card}(I) = \text{card}(J), \text{ alors } G^I = G^J \text{ et } G^{(I)} = G^{(J)}.$$

B / Propriété universelle de la somme directe de groupes abéliens

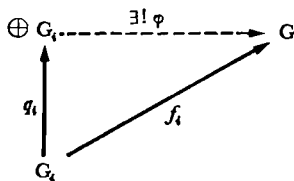
I étant un ensemble non vide, soit $\{G_i\}_{i \in I}$ une famille de groupes abéliens; d'après la définition de $\bigoplus_{i \in I} G_i$, pour tout $i \in I$, le monomorphisme q_i de G_i dans $\prod_{i \in I} G_i$ est tel que $\text{Im } q_i \leq \bigoplus_{i \in I} G_i$; aussi, chaque q_i sera considéré dans ce qui suit comme un monomorphisme de G_i dans $\bigoplus_{i \in I} G_i$.

THÉORÈME (8.5) (propriété universelle). *Soit $\{G_i\}_{i \in I}$ une famille de groupes abéliens, I étant un ensemble non vide quelconque. Soit $\{q_i\}_{i \in I}$ la famille des monomorphismes canoniques associés à la somme directe $\bigoplus_{i \in I} G_i$.*

Etant donné un groupe abélien G , et une famille de morphismes $\{f_i\}_{i \in I}$ tels que, pour tout $i \in I$, $f_i \in \text{Hom}(G_i, G)$, il existe un unique $\varphi \in \text{Hom}(\bigoplus_{i \in I} G_i, G)$ tel que, quel que soit $i \in I$,

$$\varphi \circ q_i = f_i.$$

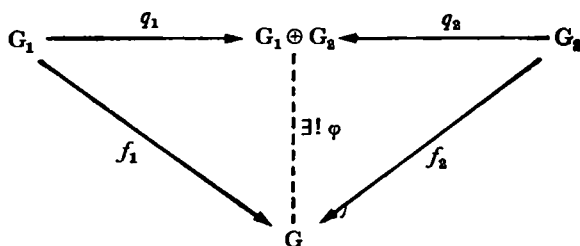
Le théorème (8.5) exprime que, pour tout $i \in I$, le diagramme suivant commute :



Preuve :

a) *Cas où I est fini :* Supposons, pour la démonstration, $I = \{1, 2\}$, celle-ci pourra être étendue sans peine au cas où $I = \{1, 2, \dots, n\}$.

Considérons le diagramme :



où (q_1, q_2) et (f_1, f_2) sont connus.

— *Existence de φ :* Considérons l'application

$$\begin{aligned}
 \varphi : G_1 \oplus G_2 &\rightarrow G \\
 (x_1, x_2) &\mapsto f_1(x_1) + f_2(x_2).
 \end{aligned}$$

Le groupe G étant abélien, on vérifie facilement que

$$\varphi \in \text{Hom}(G_1 \oplus G_2, G).$$

D'autre part, $\varphi \circ q_1(x_1) = \varphi(x_1, 0) = f_1(x_1)$, d'où $\varphi \circ q_1 = f_1$ et on montre de même que $\varphi \circ q_2 = f_2$.

— *Unicité du morphisme φ :* Supposons qu'il existe

$$\varphi' \in \text{Hom}(G_1 \oplus G_2, G)$$

tel que $\varphi' \circ q_1 = f_1$ et $\varphi' \circ q_2 = f_2$. Quel que soit $(x_1, x_2) \in G_1 \oplus G_2$, on a

$$(x_1, x_2) = q_1(x_1) + q_2(x_2),$$

$$\text{d'où } \varphi'(x_1, x_2) = \varphi' \circ q_1(x_1) + \varphi' \circ q_2(x_2),$$

$$\varphi'(x_1, x_2) = f_1(x_1) + f_2(x_2),$$

donc $\varphi'(x_1, x_2) = \varphi(x_1, x_2)$, ce qui implique $\varphi' = \varphi$.

b) Cas où I est infini :

$(x_i)_{i \in I} \in \bigoplus_{i \in I} G_i \Rightarrow x_i = 0$, sauf pour un nombre fini d'indices $i \in I$.

On en déduit que l'on peut, comme précédemment, définir

$$\varphi : \bigoplus G_i \rightarrow G$$

par $(x_i)_{i \in I} \mapsto \sum_{i \in I} f_i(x_i)$,

car $f_i(x_i) = 0$, sauf pour un nombre fini d'indices i , implique que $\sum_{i \in I} f_i(x_i)$ est la somme d'un nombre fini d'éléments de G , donc a un sens dans le groupe G .

Moyennant cette remarque, la méthode de démonstration utilisée dans le cas où I est fini s'adapte sans difficulté au cas où I est infini.

A l'aide du théorème (8.5), on démontre la propriété suivante qui sera souvent utilisée.

PROPOSITION (8.6). *Soit $\{G_i\}_{i \in I}$ une famille de groupes abéliens. Un groupe abélien G est isomorphe au groupe $\bigoplus_{i \in I} G_i$ si et seulement s'il existe une famille $\{H_i\}_{i \in I}$ de sous-groupes de G tels que :*

1) $H_i \simeq G_i, \forall i \in I$

2) $G = \bigoplus_{i \in I} H_i$ (somme directe interne).

Preuve :

— Supposons $G \simeq \bigoplus_{i \in I} G_i$. Soit ψ un isomorphisme de $\bigoplus_{i \in I} G_i$ sur G . Pour tout $i \in I$, q_i étant le monomorphisme canonique de G_i dans $\bigoplus_{i \in I} G_i$, $\psi \circ q_i$ est un monomorphisme de G_i dans G .

Posons $H_i = \psi \circ q_i(G_i)$; on a alors $H_i \simeq G_i$.

D'autre part, tout $x \in G$ s'écrit

$$x = \psi((x_i)_{i \in I}), \quad \text{où } (x_i)_{i \in I} \in \bigoplus_{i \in I} G_i.$$

$(x_i)_{i \in I} = \sum_{i \in I} q_i(x_i)$, où le second membre de cette égalité est la somme d'un nombre fini de termes, puisque les x_i sont nuls, sauf un nombre fini d'entre eux.

On en déduit que $x \in \sum_{i \in I} \psi \circ q_i(x_i)$, d'où $G = \sum_{i \in I} H_i$.

Soit $a \in H_j \cap \sum_{\substack{i \in I \\ i \neq j}} H_i$; on peut écrire :

$$a = \psi \circ q_j(x_j) = \sum_{\substack{i \in I \\ i \neq j}} \psi \circ q_i(x_i), \quad \text{avec } x_j \in G_j \text{ et } x_i \in G_i,$$

$$\text{d'où } \psi\left(\sum_{\substack{i \in I \\ i \neq j}} q_i(x_i) - q_j(x_j)\right) = 0.$$

ψ est injectif, donc $\sum_{\substack{i \in I \\ i \neq j}} q_i(x_i) - q_j(x_j) = 0$, ce qui implique :

$$x_i = 0, \quad \text{quel que soit } i \in I, \quad \text{et par suite } H_j \cap \sum_{\substack{i \in I \\ i \neq j}} H_i = (0).$$

On en conclut que $G = \bigoplus_{i \in I} H_i$.

— Réciproquement, supposons que G contienne une famille de sous-groupes $\{H_i\}_{i \in I}$ tels que $G = \bigoplus_{i \in I} H_i$ et $H_i \simeq G_i$, quel que soit $i \in I$.

Pour tout $i \in I$ désignons par f_i un isomorphisme de G_i sur H_i et considérons le diagramme :

$$\begin{array}{ccc} \bigoplus G_i & \xrightarrow{\exists! \varphi} & G \\ \uparrow q_i & & \nearrow \alpha_i \\ G_i & \xrightarrow{f_i} & H_i \end{array}$$

où α_i est l'injection canonique du sous-groupe H_i dans le groupe G .

D'après le théorème (8.5), il existe un unique

$$\varphi \in \text{Hom}\left(\bigoplus_{i \in I} G_i, G\right)$$

tel que, pour tout $i \in I$:

$$\varphi \circ q_i = \alpha_i \circ f_i.$$

Vérifions que le morphisme φ est bijectif.

Soit $x \in G$; $G = \bigoplus_{i \in I} H_i$ implique

$$x = \sum_{i \in I} h_i, \quad h_i \in H_i, \quad \forall i \in I$$

et $h_i = 0$, sauf pour un nombre fini d'indices i .

Quel que soit $i \in I$, $h_i = \alpha_i(h_i)$ et il existe un unique $x_i \in G_i$ tel que $h_i = f_i(x_i)$, d'où

$$x = \sum_{i \in I} \alpha_i \circ f_i(x_i) = \sum_{i \in I} \varphi \circ q_i(x_i)$$

$$x = \varphi\left(\sum_{i \in I} q_i(x_i)\right) \Rightarrow x \in \text{Im } \varphi,$$

donc φ est surjectif.

D'autre part,

$$\varphi((x_i)_{i \in I}) = 0, \quad \text{avec } (x_i)_{i \in I} \in \bigoplus_{i \in I} G_i,$$

implique :

$$\varphi\left(\sum_{i \in I} q_i(x_i)\right) = \sum_{i \in I} \varphi \circ q_i(x_i) = 0,$$

$$\text{donc } \sum_{i \in I} \alpha_i \circ f_i(x_i) = 0 \quad \text{dans } G = \bigoplus_{i \in I} H_i,$$

c'est-à-dire

$$\sum_{i \in I} f_i(x_i) = 0, \quad \text{avec } f_i(x_i) \in H_i, \quad \text{quel que soit } i \in I$$

on en déduit que $f_i(x_i) = 0$, donc $x_i = 0$, pour tout $i \in I$; par suite, φ est injectif.

On en conclut que φ est un isomorphisme.

COROLLAIRE (8.7). Soient I un ensemble non vide quelconque et deux familles de groupes abéliens indexées par I : $\{G_i\}_{i \in I}$ et $\{G'_i\}_{i \in I}$; alors :

$$(G_i \simeq G'_i, \quad \forall i \in I) \Rightarrow \bigoplus_{i \in I} G_i \simeq \bigoplus_{i \in I} G'_i.$$

Preuve : Posons $\Gamma = \bigoplus_{i \in I} G_i$; $\{q_i\}_{i \in I}$ étant la famille des monomorphismes canoniques associés à la somme directe des groupes G_i ; d'après les relations (1) et (2), $\Gamma = \bigoplus_{i \in I} \text{Im } q_i$ (somme directe interne).

Posons $H_i = \text{Im } q_i$; pour tout $i \in \Gamma$, on a $H_i \simeq G_i$, donc $H_i \simeq G'_i$ et $\Gamma = \bigoplus_{i \in I} H_i$, d'où $\Gamma \simeq \bigoplus_{i \in I} G'_i$, d'après la proposition (8.6).

Définition (8.8) : Soient G un groupe abélien et H un sous-groupe de G . On dit que H est un *facteur direct* de G , s'il existe un sous-groupe K de G tel que

$$G = H \oplus K.$$

K est un *complément* de H dans G et K est aussi un facteur direct de G .

PROPOSITION (8.9). *Etant donné un groupe G et un sous-groupe H , notons q l'injection canonique de H dans G ; alors H est un facteur direct de G , si et seulement s'il existe $p \in \text{Hom}(G, H)$ tel que $p \circ q = \text{id}_H$.*

Preuve :

1° Si $G = H \oplus K$, alors l'injection canonique $q: H \rightarrow G$ et la projection canonique $p: G \rightarrow H$ vérifient la condition $p \circ q = \text{id}_H$ (formule (24), chap. I).

2° Supposons, réciproquement, qu'il existe $p \in \text{Hom}(G, H)$ tel que $p \circ q = \text{id}_H$; on remarque que p est surjectif.

Soit $g \in G$, posons $p(g) = h$; $h = p \circ q(h) = p(h)$ implique $(g - h) \in \text{Ker } p$, d'où $G = H + \text{Ker } p$.

Montrons que cette somme est directe; supposons $x \in H \cap \text{Ker } p$.

$$x \in H \Rightarrow x = p \circ q(x) = p(x),$$

alors $x \in \text{Ker } p \Rightarrow x = 0$,

d'où $H \cap \text{Ker } p = (0)$.

En posant $K = \text{Ker } p$, on obtient $G = H \oplus K$.

2 — Groupes abéliens libres

A / Caractérisations des groupes abéliens libres

Définition (8.10) : On dit qu'un *groupe abélien est libre* s'il est somme directe de groupes monogènes infinis.

Un groupe abélien libre F s'écrit donc sous la forme :

$$F = \bigoplus_{i \in I} \langle x_i \rangle, \quad I \neq \emptyset \quad \text{et} \quad \langle x_i \rangle \simeq \mathbf{Z}, \quad \forall i \in I \quad (3)$$

Compte tenu de la proposition (8.6), on identifie chaque groupe monogène $\langle x_i \rangle$ à un sous-groupe de F et F est alors considéré comme la somme directe (interne) des groupes monogènes infinis $\langle x_i \rangle$, $i \in I$.

Définition (8.11) : Si F est un groupe abélien libre défini par les relations (3), alors $X = \{x_i\}_{i \in I}$ est appelé une *base* de F ; on dit que F est un *groupe abélien libre sur l'ensemble X* et F pourra être noté $F_{(X)}$.

En utilisant les notations (8.3), on vérifie que :

PROPOSITION (8.12). *Quel que soit l'ensemble X , on a*

$$F_{(X)} \simeq \mathbf{Z}^{(X)}.$$

En particulier, si X est fini et $\text{card}(X) = n \geq 1$, on obtient $F_{(X)} \simeq \mathbf{Z}^n$; de plus, par convention, on posera $\mathbf{Z}^0 = (0) = F_{(\emptyset)}$.

Preuve : Supposons X non vide et $X = \{x_i\}_{i \in I}$; alors, par définition, $F_{(X)} = \bigoplus_{i \in I} \langle x_i \rangle$, avec $\langle x_i \rangle \simeq \mathbf{Z}$, quel que soit $i \in I$. En appliquant le corollaire (8.7), on obtient : $F_{(X)} \simeq \mathbf{Z}^{(I)}$.

D'après la remarque (8.4), $\text{card}(X) = \text{card}(I)$ implique $\mathbf{Z}^{(X)} = \mathbf{Z}^{(I)}$, d'où

$$F_{(X)} \simeq \mathbf{Z}^{(X)}.$$

Si X est fini et $\text{card}(X) = n \geq 1$, on a $\mathbf{Z}^{(X)} = \mathbf{Z}^n$ (remarque (8.4)), d'où $F_{(X)} \simeq \mathbf{Z}^n$.

Remarque (8.13) : D'après la proposition précédente, étant donné un ensemble X , il existe, à un isomorphisme près, un seul groupe abélien libre sur X .

PROPOSITION (8.14). *Soit un groupe abélien $F \neq (0)$ et $X = \{x_i\}_{i \in I}$ une famille non vide d'éléments de F ; les conditions suivantes sont équivalentes :*

- 1) F est un groupe abélien libre sur X ;
 2) tout $x \in F$ s'écrit de façon unique sous la forme :

$$x = \sum_{1 \leq j \leq k} n_j x_{i_j},$$

où $k \in \mathbf{N}^*, \{i_1, i_2, \dots, i_k\} \subseteq I$ et $n_j \in \mathbf{Z}, \forall j (1 \leq j \leq k)$;

- 3) X est une partie génératrice de F telle que, quelle que soit la partie finie non vide $\{i_1, i_2, \dots, i_k\}$ de I :

$$0 = \sum_{1 \leq j \leq k} n_j x_{i_j}, \text{ où } n_j \in \mathbf{Z} \text{ pour tout } j (1 \leq j \leq k),$$

implique $n_j = 0$, quel que soit $j (1 \leq j \leq k)$.

Preuve :

— 1) \Leftrightarrow 2) : La condition 1) signifie que X est une base de F , c'est-à-dire : $F = \bigoplus_{i \in I} \langle x_i \rangle$, avec $\langle x_i \rangle \simeq \mathbf{Z}$, quel que soit $i \in I$.

D'après la proposition (1.53), $F = \bigoplus_{i \in I} \langle x_i \rangle$, si et seulement si tout $x \in F$ s'écrit de façon unique :

$$x = \sum_{1 \leq j \leq k} y_{i_j},$$

où $k \in \mathbf{N}^*, \{i_1, i_2, \dots, i_k\} \subseteq I$ et $y_{i_j} \in \langle x_{i_j} \rangle, \forall j (1 \leq j \leq k)$.

Mais, $\langle x_{i_j} \rangle$ isomorphe à \mathbf{Z} quel que soit $j (1 \leq j \leq k)$ équivaut à : pour tout $j (1 \leq j \leq k)$, $y_{i_j} \in \langle x_{i_j} \rangle$ s'écrit de façon unique, $y_{i_j} = n_j x_{i_j}$, où $n_j \in \mathbf{Z}$.

On en déduit l'équivalence des conditions 1) et 2).

— 2) \Leftrightarrow 3) : Vérification laissée au lecteur.

Remarque (8.15) : Dans un groupe abélien libre F une base X est caractérisée dans l'ensemble des parties génératrices de F , par les conditions équivalentes 2) et 3). Un groupe abélien ne possède une base que si c'est un groupe abélien libre.

Définition (8.16) : Dans un groupe abélien G , on dira que les éléments d'une famille $\{u_\lambda\}_{\lambda \in \Lambda}$ sont *linéairement indépendants sur \mathbf{Z}* si, pour toute partie finie, non vide, $\{\lambda_1, \lambda_2, \dots, \lambda_k\}$ de Λ :

$$0 = \sum_{1 \leq i \leq k} n_i u_{\lambda_i}, \text{ où } n_i \in \mathbf{Z} \text{ pour tout } i (1 \leq i \leq k),$$

implique $n_i = 0$, quel que soit $i (1 \leq i \leq k)$.

On dira aussi, dans ce cas, que la famille $\{u_\lambda\}_{\lambda \in \Lambda}$ est *libre sur \mathbf{Z}* .

Remarques (8.17) :

1° D'après la proposition (8.14), dans un groupe abélien libre, une famille *génératrice* est une base si et seulement si c'est une famille libre sur \mathbb{Z} .

2° On vérifiera que dans tout groupe abélien G , une sous-famille non vide d'une famille libre sur \mathbb{Z} est libre sur \mathbb{Z} ; en particulier tout élément d'une famille libre sur \mathbb{Z} est non nul.

B / Rang d'un groupe abélien libre

a) *Cas d'un groupe abélien libre, de type fini.*

THÉORÈME (8.18). *Un groupe abélien libre F est de type fini si et seulement s'il a une base finie ; dans ce cas, toutes les bases de F sont finies et ont le même nombre d'éléments ; si ce nombre est n , on dira que F est un groupe abélien libre de rang n .*

Preuve : On suppose $F \neq (0)$.

1° Si F est un groupe libre ayant une base X finie, alors F est de type fini, puisque X est une partie génératrice finie de F (définition (1.40)).

2° Soit F un groupe abélien libre, de type fini; montrons que F a une base finie.

Soit $X = \{x_i\}_{i \in I}$ une base de F ; d'autre part, soit

$$Y = \{y_1, y_2, \dots, y_s\}$$

une partie génératrice finie de F ($s \in \mathbb{N}^*$).

Quel que soit m ($1 \leq m \leq s$), il existe une *partie finie* J_m de I telle que $y_m \in \sum_{j \in J_m} \langle x_j \rangle$; or tout $x \in F$ s'écrit

$$x = \sum_{1 \leq m \leq s} a_m y_m, \quad \text{où } a_m \in \mathbb{Z},$$

quel que soit m ($1 \leq m \leq s$).

On en déduit que tout $x \in F$ appartient à $\sum_{j \in J} \langle x_j \rangle$, où

$J = \bigcup_{1 \leq m \leq s} J_m$; J est une *partie finie non vide* de I , donc $\{x_j\}_{j \in J}$ est une *base finie* de F , car c'est une famille génératrice de F , qui est libre sur \mathbb{Z} , en tant que sous-famille de $\{x_i\}_{i \in I}$ (remarque (8.17) 2°).

Démontrons que $I = J$.

Supposons qu'il existe $k \in I$ tel que $k \notin J$; $x_k \notin \{x_j; j \in J\}$ et x_k est non nul (remarque (8.17) 2°), donc il existe des entiers non tous nuls, n_j , où $j \in J$, tels que :

$$x_k = \sum_{j \in J} n_j x_j;$$

on en déduit :

$$\langle x_k \rangle \cap \sum_{\substack{i \in I \\ i \neq k}} \langle x_i \rangle \neq (0),$$

d'où une contradiction, puisque, par hypothèse, $F = \bigoplus_{i \in I} \langle x_i \rangle$.

On en conclut que toute base de F est finie.

3° Soit F un groupe abélien libre, de type fini, ayant une base $X = \{x_1, x_2, \dots, x_n\}$, $n \geq 1$ dans \mathbf{N} .

Soit $2F = \{2x; x \in F\}$; $2F$ est un sous-groupe de F .

Tout $x \in F$ s'écrit de façon unique sous la forme :

$$x = \sum_{1 \leq i \leq n} a_i x_i, \quad a_i \in \mathbf{Z}, \quad \forall i (1 \leq i \leq n);$$

par suite, $x \in 2F \Leftrightarrow [a_i \in 2\mathbf{Z}, \forall i (1 \leq i \leq n)]$.

On en déduit que $2F = \bigoplus_{1 \leq i \leq n} 2 \langle x_i \rangle$, d'où

$$\frac{F}{2F} = \frac{\bigoplus_{1 \leq i \leq n} \langle x_i \rangle}{\bigoplus_{1 \leq i \leq n} 2 \langle x_i \rangle} \simeq \bigoplus_{1 \leq i \leq n} \frac{\langle x_i \rangle}{2 \langle x_i \rangle}$$

(voir exercice 3, chap. IV).

Pour tout $i (1 \leq i \leq n)$, on a $\frac{\langle x_i \rangle}{2 \langle x_i \rangle} \simeq \frac{\mathbf{Z}}{2\mathbf{Z}}$, alors :

$$\frac{F}{2F} \simeq \left(\frac{\mathbf{Z}}{2\mathbf{Z}} \right)^n \Rightarrow [F : 2F] = 2^n.$$

$[F : 2F]$ ne dépend que de F , donc toute base de F est nécessairement de cardinal n .

b) Cas général : La notion de rang s'étend aux groupes abéliens libres quelconques, grâce au théorème suivant :

THÉORÈME (8.19). Quels que soient les ensembles X et Y , on a

$$F_{(X)} \simeq F_{(Y)} \Leftrightarrow \text{card}(X) = \text{card}(Y).$$

En particulier, toutes les bases d'un groupe abélien libre F ont le même cardinal, celui-ci sera appelé le rang de F .

Preuve :

1° Supposons $\text{card}(X) = \text{card}(Y)$; on a (proposition (8.12)) :

$$F_{(X)} \simeq Z^{(X)} \quad \text{et} \quad F_{(Y)} \simeq Z^{(Y)}$$

or, d'après la remarque (8.4),

$$\text{card}(X) = \text{card}(Y) \Rightarrow Z^{(X)} = Z^{(Y)}$$

d'où $\text{card}(X) = \text{card}(Y) \Rightarrow F_{(X)} \simeq F_{(Y)}$.

2° Supposons $F_{(X)} \simeq F_{(Y)}$ et $F_{(X)} \neq (0)$, car $F_{(X)} = (0)$ implique $F_{(Y)} = (0)$, donc $X = Y = \emptyset$.

1^{er} cas : X est fini et $\text{card}(X) = n \geq 1$.

Soit φ un isomorphisme de $F_{(Y)}$ sur $F_{(X)}$. Posons $Y = \{y_i\}_{i \in I}$; Y étant une base de $F_{(Y)}$, on vérifie que $\varphi(Y) = \{\varphi(y_i); i \in I\}$ est une base de $F_{(X)}$; or, d'après le théorème (8.18) toutes les bases de $F_{(X)}$ sont finies et de cardinal n , d'où $\text{card}(\varphi(Y)) = n$, on en déduit que $\text{card}(Y) = n = \text{card}(X)$.

2^e cas : X est infini ; démontrons qu'on a alors :

$$\text{card}(F_{(X)}) = \text{card}(X).$$

Désignons par $\mathcal{F}(F)$ l'ensemble des parties finies de X .

$$x \in F_{(X)} \Leftrightarrow \exists A \in \mathcal{F}(X), \quad x \in F_{(A)};$$

par suite,

$$F_{(X)} = \bigcup_{A \in \mathcal{F}(X)} F_{(A)} \quad (4)$$

(Pour $A = \emptyset$, $F_{(\emptyset)} = (0)$.)

Nous allons utiliser, en les rappelant, quelques propriétés des cardinaux, dont on pourra (par exemple) trouver les démonstrations dans la *Théorie des ensembles* de Bourbaki (E III) [8 b].

(P₁) L'ensemble $\mathcal{F}(X)$ des parties finies d'un ensemble infini X est équipotent à X [E III, p. 50]. Autrement dit :

$$\text{card}(\mathcal{F}(X)) = \text{card}(X) \quad (5)$$

(P₂) Le produit d'une famille finie d'ensembles dénombrables est dénombrable [E III, p. 49].

Or, quel que soit $A \neq \emptyset$ dans $\mathcal{F}(X)$, tel que $\text{card}(A) = n \geq 1$, on a d'après la proposition (8.12) :

$$F_{(A)} \simeq \mathbb{Z}^n;$$

\mathbb{Z} est dénombrable, donc \mathbb{Z}^n est dénombrable, d'après (P₂); de plus $F_{(\emptyset)} = (0)$, par suite :

$$\forall A \in \mathcal{F}(X), \quad F_{(A)} \text{ est dénombrable.}$$

(P₃) Si f est une application d'un ensemble E sur un ensemble infini E' , telle que, pour tout $y \in E'$, $f^{-1}(y)$ soit dénombrable, alors E' est équipotent à E [E III, p. 50].

Posons $X = \{x_i\}_{i \in I}$ et considérons $f: F_{(X)} \rightarrow \mathcal{F}(X)$, définie par : $x \mapsto A$ tel que :

— si $x = 0$, $A = f(0) = \emptyset$;

— si $x \neq 0$ et x s'écrit de façon unique :

$$x = \sum_{1 \leq j \leq k} n_j x_{i_j}, \quad \text{où } k \in \mathbb{N}^*, \quad n_j \in \mathbb{Z}^*, \quad \forall j \quad (1 \leq j \leq k),$$

$$\text{alors} \quad A = f(x) = \{x_{i_1}, x_{i_2}, \dots, x_{i_k}\} \quad (6)$$

f est alors une application *surjective* et quel que soit $A \in \mathcal{F}(X)$, on a $f^{-1}(A) \subseteq F_{(A)}$.

Or, on a vu plus haut que $F_{(A)}$ est dénombrable, donc $f^{-1}(A)$ est dénombrable [E III, p. 49].

En appliquant la propriété (P₃), on obtient alors :

$$\text{card}(\mathcal{F}(X)) = \text{card}(F_{(X)}),$$

d'où, en tenant compte de (5) :

$$\text{card}(F_{(X)}) = \text{card}(X) \quad (7)$$

On en conclut que :

$$F_{(X)} \simeq F_{(Y)} \Rightarrow \text{card}(X) = \text{card}(Y).$$

Une conséquence immédiate du théorème (8.19) est la suivante :

Remarque (8.20) : Soit F un groupe abélien libre; alors :

$$(F \text{ est de rang fini } n) \Leftrightarrow F \simeq \mathbb{Z}^n.$$

COROLLAIRE (8.21). *Quel que soit l'ensemble X non vide, il existe un groupe abélien équipotent à X .*

Preuve :

— Si X est infini, d'après la proposition (8.12) et la relation (7) :

$$\text{card}(\mathbf{Z}^{(X)}) = \text{card}(X),$$

donc $\mathbf{Z}^{(X)}$ est un groupe abélien équipotent à X .

— Si X est fini, posons $X = \{x_1, x_2, \dots, x_n\}$, $n \geq 1$ dans \mathbf{N} .

Pour $n = 1$, $X = \{x_1\}$ est équipotent au groupe abélien (0).

Pour $n > 1$; on vérifiera que l'on peut définir sur X une structure de groupe cyclique, en posant :

$$x_2 = 2x_1, \quad x_3 = 3x_1, \dots, x_n = nx_1, \quad x_1 = (n+1)x_1$$

et quels que soient j et k dans $\{1, 2, \dots, n\}$, $x_j + x_k = lx_1 = x_k + x_j$, où $l \equiv j + k \pmod{n}$ et $1 \leq l \leq n$; par suite, X est équipotent au groupe $\frac{\mathbf{Z}}{n\mathbf{Z}}$.

Remarque (8.22) : Signalons que l'axiomatique de la *Théorie des ensembles* de Gödel ⁽¹⁾ - Bernays ⁽²⁾ permet de prouver que si l'on considère tous les ensembles, ils forment une « classe » qui n'est pas un ensemble; l'intérêt du corollaire (8.21) est alors de montrer que tous les groupes abéliens constituent aussi une « classe » qui n'est pas un ensemble et on peut en déduire que, *a fortiori*, la « classe des groupes » n'est pas un ensemble (voir la notion de « classe », par exemple, dans [54]).

C / Propriété universelle d'un groupe abélien libre

THÉORÈME (8.23). *Soit F un groupe abélien et X une partie génératrice de F ; alors F est libre sur X , si et seulement si, quels que soient le groupe abélien G et l'application $\sigma : X \rightarrow G$, il existe un unique morphisme $f \in \text{Hom}(F, G)$ tel que $f \circ j_X = \sigma$, où j_X est l'injection canonique de X dans F .*

⁽¹⁾ Paul Isaak Bernays (1888-1972).

⁽²⁾ Kurt Gödel (1906-1978).

Preuve : Posons $X = \{x_i\}_{i \in I}$; quel que soit $i \in I$, $j_X(x_i) = x_i$.

a) Supposons F libre sur X ; dans le diagramme :

$$\begin{array}{ccc}
 X & \xrightarrow{j_X} & F \\
 \sigma \downarrow & \nearrow \exists! f & \\
 G & &
 \end{array} \quad (8)$$

où le groupe G et l'application σ sont donnés, définissons

$$\begin{aligned}
 & f: F \rightarrow G \\
 \text{par} \quad & \sum_{i \in I} n_i x_i \mapsto \sum_{i \in I} n_i \sigma(x_i).
 \end{aligned}$$

Tout $x \in F$ s'écrivant *de façon unique* sous la forme $x = \sum_{i \in I} n_i x_i$, où les n_i sont « presque tous nuls » (proposition (8.14) et chap. I), f définit bien une application de F dans G .

Quel que soit $x_i \in X$, $f \circ j_X(x_i) = f(x_i) = \sigma(x_i)$, d'où

$$f \circ j_X = \sigma.$$

D'autre part, quels que soient $x = \sum_{i \in I} n_i x_i$ et $y = \sum_{i \in I} m_i x_i$ dans F , on a, compte tenu de la commutativité des groupes F et G :

$$f(x + y) = f\left(\sum_{i \in I} (n_i + m_i) x_i\right) = \sum_{i \in I} (n_i + m_i) \sigma(x_i),$$

$$\text{d'où} \quad f(x + y) = \sum_{i \in I} n_i \sigma(x_i) + \sum_{i \in I} m_i \sigma(x_i),$$

$$f(x + y) = f(x) + f(y); \quad \text{donc } f \in \text{Hom}(F, G).$$

Unicité de f : Supposons qu'il existe $f' \in \text{Hom}(F, G)$ tel que $f' \circ j_X = \sigma$; on vérifie alors, facilement, que pour tout $x \in F$, on a $f'(x) = f(x)$, d'où $f' = f$.

b) Réciproquement, supposons que le groupe abélien F ait une partie génératrice X satisfaisant à la propriété énoncée dans le théorème (8.23).

Posons $X = \{x_i\}_{i \in I}$ et soit $F_{(Y)}$ un groupe libre de base $Y = \{y_i\}_{i \in I}$, donc $\text{card}(Y) = \text{card}(X)$.

Considérons l'application $\sigma : X \rightarrow F_{(Y)}$
 $x_i \mapsto y_i$.

L'hypothèse implique qu'il existe un unique morphisme f de $F_{(Y)}$, tel que $f \circ j_Y = \sigma$.

Pour tout $x = \sum_{1 \leq j \leq k} n_j x_{ij}$ de F , on a alors

$$f(x) = \sum_{1 \leq j \leq k} n_j y_{ij};$$

on en déduit facilement que f est un isomorphisme et que, par suite, F est libre sur X .

Remarque (8.24) : La propriété énoncée dans le théorème (8.23) est la « propriété universelle » du groupe abélien libre sur X , qui est défini à un isomorphisme près (remarque (8.13)).

En application de cette propriété on obtient le résultat important suivant :

THÉORÈME (8.25). *Tout groupe abélien est image homomorphe d'un groupe abélien libre ; en particulier, tout groupe abélien de type fini est image homomorphe d'un groupe abélien libre de rang fini.*

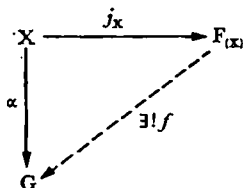
Preuve : Soit G un groupe abélien. Soit X une partie génératrice de G .

(0) étant un groupe abélien libre sur l'ensemble vide, on peut supposer $G \neq (0)$.

Soit $F_{(X)}$ un groupe abélien libre sur X .

Notons j_X l'injection canonique $X \rightarrow F_{(X)}$ et α l'injection canonique $X \rightarrow G$.

D'après le théorème (8.23), il existe un unique $f \in \text{Hom}(F_{(X)}, G)$ tel que $f \circ j_X = \alpha$.



Si $X = \{x_i\}_{i \in j}$, tout $x \in G$ s'écrit

$$x = \sum_{1 \leq j \leq k} n_j x_{ij}, \quad k \in \mathbb{N}^* \quad \text{et} \quad n_j \in \mathbb{Z}, \quad \forall j (1 \leq j \leq k).$$

D'autre part, pour tout j ($1 \leq j \leq k$), on a

$$x_{ij} = \alpha(x_{ij}) = f \circ j_X(x_{ij}),$$

$$\text{donc} \quad x = \sum_{1 \leq j \leq k} n_j f \circ j_X(x_{ij});$$

$f \in \text{Hom}(F_{(X)}, G)$ implique alors, $x = f(\sum_{1 \leq j \leq k} n_j j_X(x_{ij}))$; par suite, f est surjectif, d'où

$$G \simeq \frac{F_{(X)}}{\text{Ker } f}.$$

Si G est un groupe abélien de type fini et si $\{x_1, x_2, \dots, x_n\}$, $n \in \mathbb{N}^*$, est une partie génératrice de G , d'après ce qui précède G est image homomorphe d'un groupe abélien libre de base $\{x_1, x_2, \dots, x_n\}$, donc de rang fini n .

D / Sous-groupes d'un groupe abélien libre

Le résultat fondamental de ce paragraphe est le théorème (8.29); la démonstration, que nous en donnons, s'appuie sur la notion d'ensemble bien ordonné, que nous rappelons préalablement.

Définition (8.26) : Un ensemble non vide X est dit *bien ordonné* si c'est un ensemble ordonné tel que toute partie non vide de X a un plus petit élément.

Remarques (8.27) :

1° Si X est un ensemble bien ordonné, alors X est totalement ordonné, car pour toute partie $\{x, y\}$ de X , on a nécessairement $x \leq y$ ou $y \leq x$. On en déduit que toute partie finie, non vide, d'un ensemble bien ordonné a un plus grand élément.

2° Nous admettrons que « Tout ensemble non vide peut être bien ordonné » [26].

THÉORÈME (8.28). *Tout sous-groupe d'un groupe abélien libre est un groupe abélien libre.*

Preuve : Soit F un groupe abélien libre; on suppose $F \neq (0)$.

Soient $X = \{x_i\}_{i \in I}$ une base de F et H un sous-groupe de F . Si $H = (0)$, alors H est un groupe abélien libre sur l'ensemble vide; on supposera donc dans la suite $H \neq (0)$ et $H \neq F$.

X étant considéré comme un ensemble bien ordonné, soit $\mathcal{F}(X)$ l'ensemble des parties finies de X .

Soit $h \in H \setminus \{0\}$; h s'écrit de façon unique :

$$h = \sum_{1 \leq j \leq k} n_j x_{i_j}, \quad (9)$$

où $k \in \mathbf{N}^*$ et $n_j \in \mathbf{Z}^*$, $\forall j$ ($1 \leq j \leq k$).

Comme dans la démonstration du théorème (8.19) (relation (6)), on considère

$$f(h) = \{x_{i_1}, x_{i_2}, \dots, x_{i_k}\}; \quad f(h) \in \mathcal{F}(X).$$

D'après la remarque (8.27) 1^o, il existe un plus grand élément dans $f(h)$, que l'on désignera par $g(h)$.

On définit ainsi une application : $g : H \setminus \{0\} \rightarrow X$
 $h \mapsto g(h)$.

Pour tout $x_i \in g(H \setminus \{0\})$, choisissons dans $g^{-1}(x_i)$, un élément, que l'on notera h_i , ayant pour coefficient de x_i , dans son expression sous la forme (9), l'entier positif, le plus petit possible.

On remarque que si $g(h) = x_i$ et que le coefficient de h relativement à x_i est négatif, alors $g(-h) = x_i$ et le coefficient de $-h$, relativement à x_i est positif.

Soit S l'ensemble des éléments h_i de H respectivement associés aux éléments $x_i \in g(H \setminus \{0\})$.

Démontrons que S est une base de H .

a) Vérifions que les éléments de S sont linéairement indépendants sur \mathbf{Z} .

Soit $\{h_{i_1}, h_{i_2}, \dots, h_{i_n}\}$, où $n \in \mathbf{N}^*$, une famille finie d'éléments de S si $x_{i_j} = g(h_{i_j})$, $1 \leq j \leq n$, on suppose $x_{i_1} > x_{i_2} > \dots > x_{i_n}$ dans X . Soient a_1, a_2, \dots, a_n dans \mathbf{Z}^* , alors l'élément

$$h = a_1 h_{i_1} + a_2 h_{i_2} + \dots + a_n h_{i_n}$$

est non nul dans H , car dans l'expression de h sous la forme (9), le coefficient de x_{i_1} , par exemple, est non nul.

On en déduit que $h = 0$ implique $a_k = 0$ pour tout k ($1 \leq k \leq n$), donc la somme des sous-groupes $\langle h_i \rangle$ de H est directe.

Posons $K = \bigoplus_{h_i \in S} \langle h_i \rangle$; on a $\langle h_i \rangle \simeq \mathbf{Z}$, puisque d'après ce qui précède chaque $h_i \in S$ est libre sur \mathbf{Z} .

b) Supposons $H \neq K$.

Soit $T = \{x_i \in X; \exists h \in H \setminus K, g(h) = x_i\}$. T est une partie non vide de X , donc il existe, dans T , un plus petit élément, que l'on notera x_{i_0} .

D'après la définition de x_{i_0} , il existe au moins un $h \in H \setminus K$, tel que $g(h) = x_{i_0}$; h s'écrit de façon unique sous la forme :

$$h = \sum_{0 \leq j \leq k} n_j x_{i_j}, \quad \text{où } n_j \in \mathbf{Z}^*, x_{i_j} \in X, \quad \forall j (0 \leq j \leq k).$$

D'autre part, il existe $h_0 \in S$ tel que $g(h_0) = x_{i_0}$; h_0 s'écrit de façon unique sous la forme :

$$h_0 = \sum_{0 \leq l \leq r} m_l x_{i_l},$$

$$\text{où } m_l \in \mathbf{Z}^*, \quad \forall l (0 \leq l \leq r) \quad \text{et} \quad x_{i_0} = x_{i_0}.$$

D'après la définition de h_0 , on a $0 < m_0 \leq n_0$; on peut donc écrire dans \mathbf{Z} : $n_0 = m_0 q + r$, avec $0 \leq r < m_0$; si $r \neq 0$, alors $(h - qh_0) \in H$ et $h - qh_0 = rx_{i_0} + \dots$, avec $0 < r < m_0$, d'où une contradiction. On en conclut que $H = K$, donc H est un groupe abélien libre.

Remarque (8.29) : Si F est un groupe abélien libre, alors :

$$H \leq F \Rightarrow \text{rang}(H) \leq \text{rang}(F).$$

— Si F est de rang infini, d'après la démonstration du théorème (8.19) (relation (7)), on a $\text{rang}(F) = \text{card}(F)$; alors :

- ou bien H est de rang fini, donc $\text{rang}(H) < \text{rang}(F)$;
- ou bien H est de rang infini; dans ce cas, $\text{rang}(H) = \text{card}(H)$ et $H \subseteq F$ implique

$$\text{rang}(H) \leq \text{rang}(F).$$

— Si F est de rang fini : le résultat sera démontré plus loin (théorème (8.54)).

Remarquons qu'il est possible d'avoir

$$H \neq F \quad \text{et} \quad \text{rang}(H) = \text{rang}(F).$$

En effet, si $F = \mathbf{Z}$ et $H = n\mathbf{Z}$, $n \geq 2$, on a

$$n\mathbf{Z} \neq \mathbf{Z} \quad \text{et} \quad \text{rang}(n\mathbf{Z}) = 1 = \text{rang}(\mathbf{Z}).$$

Le théorème (8.28) permet de donner une nouvelle caractérisation des groupes abéliens libres :

THÉORÈME (8.30). *Un groupe abélien F est libre, si et seulement s'il vérifie la propriété (\mathcal{P}) suivante :*

(\mathcal{P}) : *Quels que soient les groupes abéliens A et B , le morphisme $f \in \text{Hom}(F, B)$ et l'épimorphisme $g \in \text{Hom}(A, B)$, il existe*

$$h \in \text{Hom}(F, A) \quad \text{tel que} \quad g \circ h = f.$$

Preuve :

1° Supposons le groupe F abélien libre et considérons le diagramme :

$$\begin{array}{ccc} & F & \\ \exists h \swarrow & \downarrow f & \\ A & \xrightarrow{g} & B \end{array} \quad (g \text{ surjectif}) \quad (10)$$

dans lequel f et g sont des morphismes donnés.

Soit $X = \{x_i\}_{i \in I}$ une base de F .

Quel que soit $i \in I$, $f(x_i) \in B$; g étant surjectif, il existe $a_i \in A$ tel que $f(x_i) = g(a_i)$. En choisissant pour chaque x_i un $a_i \in f^{-1}(x_i)$, on définit une application $\sigma : X \rightarrow A$ et on considère le diagramme :

$$\begin{array}{ccc}
 X & \xrightarrow{j_X} & F \\
 \sigma \downarrow & \nearrow \exists! h & \\
 A & &
 \end{array} \quad (11)$$

D'après la propriété universelle du groupe abélien F libre sur X (théorème (8.23)), il existe un unique $h \in \text{Hom}(F, A)$ tel que $h \circ j_X = \sigma$; alors, quel que soit $i \in I$,

$$h \circ j_X(x_i) = h(x_i) = \sigma(x_i) = a_i,$$

$$\text{d'où } g \circ h(x_i) = f(x_i), \quad \forall i \in I.$$

f, g, h étant des morphismes de groupes, on en déduit que :

$$g \circ h = f.$$

On notera que pour une application σ déterminée, le morphisme h est unique dans le diagramme (11); cependant le *morphisme h n'est pas unique* dans le diagramme (10), car la détermination de σ n'est pas unique, en général.

2° On suppose que F est un groupe abélien vérifiant la propriété (\mathcal{P}). Soit X une partie génératrice de F . Si $F_{(X)}$ est un groupe abélien libre sur X , d'après le théorème (8.25), F est isomorphe à un quotient de $F_{(X)}$; on a donc un diagramme de la forme :

$$\begin{array}{ccc}
 & F & \\
 & \downarrow f & \\
 F_{(X)} & \xrightarrow{\pi} & F_{(X)} / K
 \end{array} \quad (\text{épigroupe canonique})$$

(épigroupe canonique)

où f est un isomorphisme. Compte tenu de la propriété (\mathcal{P}), il existe $\varphi \in \text{Hom}(F, F_{(X)})$ tel que $\pi \circ \varphi = f$.

Montrons que φ est injectif; en effet, $\varphi(x) = 0$, implique

$$\pi \circ \varphi(x) = 0 = f(x);$$

f étant un isomorphisme, on a $x = 0$.

On en déduit que F est isomorphe à $\text{Im } \varphi$, donc à un sous-groupe du groupe abélien libre $F_{(x)}$, par suite, F est abélien libre, d'après le théorème (8.28).

Remarque (8.31) : Si on considère un groupe abélien comme un \mathbf{Z} -module, le théorème (8.30) exprime qu'un groupe abélien est libre, si et seulement si c'est un \mathbf{Z} -module *projectif*, car la propriété (\mathcal{P}) caractérise les modules projectifs ([54], tome 2).

En application du théorème (8.30), nous démontrons le résultat suivant :

PROPOSITION (8.32). *Soit G un groupe abélien. Si H est un sous-groupe de G tel que $\frac{G}{H}$ soit libre, alors H est un facteur direct de G .*

Preuve : Soit π la surjection canonique $G \rightarrow \frac{G}{H}$. On peut alors appliquer le théorème (8.30) au diagramme suivant :

$$\begin{array}{ccc} & & \frac{G}{H} \\ & \nearrow \exists \varphi & \downarrow \text{id}_{\frac{G}{H}} \\ G & \xrightarrow{\pi} & \frac{G}{H} \end{array}$$

il existe donc $\varphi \in \text{Hom}\left(\frac{G}{H}, G\right)$ tel que $\pi \circ \varphi = \text{id}_{\frac{G}{H}}$.

Pour tout $x \in G$, posons $\pi(x) = \bar{x}$; on a

$$\bar{x} = \pi \circ \varphi(\bar{x}),$$

d'où $(x - \varphi(\bar{x})) \in H$, quel que soit $x \in G$.

Considérons alors l'application $p : G \rightarrow H$

$$x \mapsto x - \varphi(\bar{x}).$$

On vérifie que $p \in \text{Hom}(G, H)$, de plus si q est l'injection canonique de H dans G , on a, pour tout $h \in H$,

$$p \circ q(h) = h, \quad \text{car } \bar{h} = 0;$$

donc $p \circ q = \text{id}_H$. D'après la proposition (8.9), H est un facteur direct de G .

Remarque (8.33) : Les hypothèses étant celles de la proposition (8.32), le groupe $\frac{G}{H}$ est isomorphe à un facteur direct de G .

En effet, le résultat de la proposition implique qu'il existe $K \leq G$ tel que $G = H \oplus K$; on a alors K facteur direct de G et $\frac{G}{H} \simeq K$.

3 — Groupes abéliens de torsion

A / Groupes de torsion, sans torsion, mixtes

Définitions (8.34) : Soit un groupe quelconque G (pas nécessairement abélien); on dit que :

G est de torsion si tout élément de G est d'ordre fini;

G est sans torsion si tout élément, autre que l'élément neutre, est d'ordre infini;

G est mixte s'il a, à la fois, des éléments d'ordre infini et des éléments d'ordre fini, autres que l'élément neutre.

Parmi les groupes abéliens, on vérifie, par exemple, que :

\mathbb{Q} est un groupe sans torsion; $\frac{\mathbb{Q}}{\mathbb{Z}}$ est un groupe de torsion;

\mathbb{C}^* (groupe multiplicatif des nombres complexes non nuls) est un groupe mixte.

Remarques (8.35) :

1° Tout groupe fini est de torsion.

2° Tout groupe abélien libre est sans torsion.

3° Dans certains ouvrages un groupe de torsion est appelé groupe *périodique*.

4° Signalons ici le problème posé par Burnside en 1902.

Sachant qu'un groupe fini est de type fini et de torsion, un groupe de type fini et de torsion est-il nécessairement fini? La question a une réponse positive si le groupe est résoluble (exercice 15, chap. VIII); mais la réponse est négative, en général, comme l'ont finalement prouvé, en 1964, les mathématiciens russes E. S. Golod et I. R. Shafarevich, qui montrèrent que pour tout nombre premier p , il existe un groupe infini, dont tout élément a pour ordre une puissance de p et qui est engendré par trois éléments (voir [40], p. 193).

THÉORÈME (8.36). *Dans tout groupe abélien G , l'ensemble $T(G)$ des éléments d'ordre fini est un sous-groupe de G et $\frac{G}{T(G)}$ est sans torsion; $T(G)$ est appelé : sous-groupe de torsion de G .*

Preuve : Si G est sans torsion $T(G) = (0)$; si G est de torsion, $T(G) = G$. Supposons G mixte.

Soient x et y dans $T(G)$ tels que $o(x) = m$, $o(y) = n$, alors $mn(x - y) = 0$, donc $(x - y) \in T(G)$.

Soit $\bar{x} \in \frac{G}{T(G)}$, $\bar{x} \neq \bar{0}$.

Pour tout entier $n > 0$,

$$n\bar{x} = \bar{0} \Leftrightarrow nx \in T(G)$$

$$nx \in T(G) \Rightarrow \exists m \in \mathbf{N}^*, \quad mn x = 0,$$

donc $nx \in T(G) \Rightarrow x \in T(G)$,

d'où une contradiction avec l'hypothèse $\bar{x} \neq \bar{0}$; par suite, $\frac{G}{T(G)}$ est sans torsion.

PROPOSITION (8.37). Soit G et G' deux groupes abéliens, alors :

$$G \simeq G' \Rightarrow T(G) \simeq T(G') \quad \text{et} \quad \frac{G}{T(G)} \simeq \frac{G'}{T(G')}.$$

Preuve : Soit φ un isomorphisme de G sur G' .

Soit $x \in T(G)$; il existe $n \in \mathbb{N}^*$ tel que $nx = 0$, d'où $n\varphi(x) = 0$, on en déduit que $\varphi(T(G)) \subseteq T(G')$.

D'autre part, quel que soit $y \in T(G')$, il existe $x \in G$ tel que $y = \varphi(x)$; si $0 = my = m\varphi(x)$ pour un certain $m > 0$ dans \mathbb{N} , alors $\varphi(mx) = 0$ implique $mx = 0$, donc $x \in T(G)$. On en conclut que $T(G') = \varphi(T(G))$, par suite, $\varphi_{T(G)}$ est un isomorphisme de $T(G)$ sur $T(G')$.

On en déduit que $\frac{G}{T(G)}$ est isomorphe à $\frac{G'}{T(G')}$, en considérant le diagramme :

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & & \downarrow \pi' \\ G & \xrightarrow{\exists! \varphi} & G' \\ T(G) & \xrightarrow{\quad} & T(G') \end{array}$$

auquel on applique le lemme (4.32).

PROPOSITION (8.38). Soit G un groupe abélien et $H \leq G$; alors :

- a) $T(H) = H \cap T(G)$
 b) $\frac{T(G)}{T(H)} \simeq \frac{HT(G)}{H}$ et $\frac{HT(G)}{H} \leq T\left(\frac{G}{H}\right).$

Démonstration laissée au lecteur (exercice 1, chap. VIII).

B / Composantes p -primaires d'un groupe abélien de torsion

Définition (8.39) : p étant un nombre premier, on dit qu'un groupe quelconque G (pas nécessairement abélien) est un p -groupe si tout élément de G a un ordre qui est une puissance de p .

Un p -groupe abélien est aussi appelé : groupe abélien p -primaire.

Remarque (8.40) : Un groupe fini G est un p -groupe si et seulement si l'ordre de G est une puissance de p ; c'est-à-dire que G est un p -groupe fini, au sens de la définition (6.6).

En effet, si quel que soit $x \in G$, $o(x) = p^k$, $k \geq 0$ dans \mathbf{N} , alors, d'après le premier théorème de Sylow, p est le seul diviseur premier de l'ordre de G .

Etant donné un groupe abélien G et un nombre premier p , on vérifie facilement que l'ensemble G_p des éléments de G , dont l'ordre est une puissance de p , est un sous-groupe de G .

Définition (8.41) : G étant un groupe abélien, pour tout nombre premier p , le sous-groupe G_p de G , défini ci-dessus, est appelé : *composante p -primaire de G .*

THÉORÈME (8.42). *Soit G un groupe abélien de torsion.*

\mathcal{P} désignant l'ensemble des nombres premiers, on a :

$$G = \bigoplus_{p \in \mathcal{P}} G_p, \quad \text{où } G_p \text{ est la composante } p\text{-primaire de } G.$$

Preuve : Soit $x \in G$; G étant de torsion, il existe $n \in \mathbf{N}^*$ tel que $o(x) = n$.

Supposons $x \neq 0$, donc $n > 1$; alors $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, où les p_i sont des nombres premiers deux à deux distincts et les α_i sont dans \mathbf{N}^* .

Pour tout i ($1 \leq i \leq k$), posons $n_i = \frac{n}{p_i^{\alpha_i}}$.

Les n_i ($1 \leq i \leq k$) sont alors premiers entre eux dans leur ensemble et p_i ne divise pas n_i .

D'après le théorème de Bezout, il existe des entiers $a_i \in \mathbf{Z}$, $1 \leq i \leq k$, tels que

$$a_1 n_1 + a_2 n_2 + \dots + a_k n_k = 1.$$

On peut donc écrire $x = 1x$, c'est-à-dire

$$x = a_1(n_1 x) + a_2(n_2 x) + \dots + a_k(n_k x).$$

Quel que soit i ($1 \leq i \leq k$), $o(n_i x) = p_i^{\alpha_i}$, donc $n_i x \in G_{p_i}$.
On en déduit que $x \in \sum_{1 \leq i \leq k} G_{p_i}$, donc $x \in \sum_{p \in \mathcal{P}} G_p$, par suite :

$$G = \sum_{p \in \mathcal{P}} G_p.$$

Etant donné $p_0 \in \mathcal{P}$, soit $x \in G_{p_0} \cap \sum_{\substack{p \in \mathcal{P} \\ p \neq p_0}} G_p$.

$x \in G_{p_0}$ implique $o(x) = p_0^{\alpha}$, $\alpha \in \mathbb{N}$.

$x \in \sum_{\substack{p \in \mathcal{P} \\ p \neq p_0}} G_p$ implique qu'il existe une partie finie $\{p_1, p_2, \dots, p_k\}$

de $\mathcal{P} \setminus \{p_0\}$ telle que $x \in \sum_{1 \leq i \leq k} G_{p_i}$, donc

$$x = x_1 + x_2 + \dots + x_k, \quad x_i \in G_{p_i}, \quad \forall i (1 \leq i \leq k).$$

Les ordres des x_i étant deux à deux premiers entre eux, l'ordre de $x = \sum_{1 \leq i \leq k} x_i$ est égal au produit des ordres des x_i (exercice 14, chap. III); d'où

$$o(x) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad \alpha_i \in \mathbb{N}, \quad \forall i (1 \leq i \leq k).$$

$p_0 \notin \{p_1, p_2, \dots, p_k\}$, on en déduit que, nécessairement, $x = 0$, d'où :

$$G = \bigoplus_{p \in \mathcal{P}} G_p.$$

Remarque (8.43) : Si G est un groupe abélien fini tel que $o(G) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, où les p_i sont des nombres premiers deux à deux distincts et les $\alpha_i > 0$ dans \mathbb{N} , alors, pour tout i ($1 \leq i \leq k$), G_{p_i} est le p_i -sous-groupe de Sylow de G .

Le résultat du théorème (8.42), se traduit, dans ce cas, par l'égalité : $G = \bigoplus_{1 \leq i \leq k} G_{p_i}$, que l'on avait démontrée au chapitre VI (corollaire (6.19), remarque (6.20)).

4 — Groupes abéliens de type fini

A / Sous-groupes d'un groupe abélien libre de type fini

a) Changement de bases dans un groupe abélien libre de type fini.

On suppose connues les règles élémentaires du calcul matriciel et du calcul des déterminants, ainsi que leur application à la résolution des systèmes d'équations linéaires (voir [31] ou [50]).

Soit F un groupe abélien libre de type fini tel que $\text{rang}(F) = n \geq 1$ (voir théorème (8.18)).

Soient $X = \{x_i\}_{1 \leq i \leq n}$ et $Y = \{y_j\}_{1 \leq j \leq n}$ deux bases de F .

Quels que soient i ($1 \leq i \leq n$) et j ($1 \leq j \leq n$), on peut écrire de façon unique :

$$x_i = \sum_{1 \leq j \leq n} p_{ij} y_j \quad \text{et} \quad y_j = \sum_{1 \leq k \leq n} q_{jk} x_k,$$

où les p_{ij} et q_{jk} sont dans \mathbf{Z} .

On en déduit :

$$x_i = \sum_{1 \leq j \leq n} \left(\sum_{1 \leq k \leq n} p_{ij} q_{jk} x_k \right), \quad \forall i \ (1 \leq i \leq n) \quad (12)$$

$$y_j = \sum_{1 \leq k \leq n} \left(\sum_{1 \leq l \leq n} q_{jk} p_{kl} y_l \right), \quad \forall j \ (1 \leq j \leq n) \quad (13)$$

X et Y étant deux bases de F , les relations (12) et (13) impliquent, quels que soient i, j, k, l dans $\{1, 2, \dots, n\}$:

$$\sum_{1 \leq j \leq n} p_{ij} q_{jk} = \delta_{ik}, \quad \sum_{1 \leq k \leq n} q_{jk} p_{kl} = \delta_{jl} \quad (14)$$

où δ_{ik}, δ_{jl} sont les symboles de Kronecker ⁽³⁾, c'est-à-dire que :

$$\delta_{ik} = \delta_{jl} = 0, \quad \text{si } i \neq k, j \neq l \quad \text{et} \quad \delta_{ii} = \delta_{jj} = 1.$$

Soient P et Q les matrices carrées d'ordre n sur \mathbf{Z} , définies par $P = (p_{ij}), Q = (q_{jk})$.

I_n désignant la matrice unité d'ordre n sur \mathbf{Z} , les relations (14) impliquent :

$$PQ = QP = I_n \quad (15)$$

⁽³⁾ Leopold Kronecker (1823-1891).

On en déduit que $\det(P) \det(Q) = 1$; mais P et Q étant à coefficients entiers, on a nécessairement

$$\det(P) = \det(Q) = \pm 1 \quad (16)$$

Définition (8.44) : Compte tenu des notations ci-dessus, P (resp^t Q) est la *matrice de passage* de la base Y à la base X (resp^t de la base X à la base Y).

PROPOSITION (8.45). Dans l'anneau $M_n(\mathbf{Z})$ des matrices carrées d'ordre n sur \mathbf{Z} , l'ensemble $U_n(\mathbf{Z})$ des matrices de déterminant égal à ± 1 est un groupe multiplicatif.

Vérification laissée au lecteur.

Remarque (8.46) : Les résultats précédents montrent que toute matrice de passage d'une base à une autre base d'un groupe abélien libre F de rang fini $n \geq 1$ est une matrice appartenant au groupe $U_n(\mathbf{Z})$.

Réciproquement, si $X = \{x_i\}_{1 \leq i \leq n}$ est une base de F , et si $Q = (q_{jk})$ appartient à $U_n(\mathbf{Z})$, alors, $Y = \{y_j\}_{1 \leq j \leq n}$ où, quel que soit j ($1 \leq j \leq n$), $y_j = \sum_{1 \leq k \leq n} q_{jk} x_k$, est une base de F .

En effet, Q est inversible et si

$$P = Q^{-1} = (p_{ij}), \quad P \in U_n(\mathbf{Z})$$

$$\text{et} \quad x_i = \sum_{1 \leq j \leq n} p_{ij} y_j, \quad \forall i \ (1 \leq i \leq n).$$

Y est donc une famille génératrice de F , de plus :

$$\begin{aligned} \left(\sum_{1 \leq j \leq n} n_j y_j = 0, \quad n_j \in \mathbf{Z} \right) \\ \Leftrightarrow \sum_{1 \leq j \leq n} n_j \left(\sum_{1 \leq k \leq n} q_{jk} x_k \right) = 0, \quad n_j \in \mathbf{Z} \end{aligned}$$

$$\begin{aligned} \left(\sum_{1 \leq j \leq n} n_j y_j = 0, \quad n_j \in \mathbf{Z} \right) \\ \Leftrightarrow \sum_{1 \leq k \leq n} \left(\sum_{1 \leq j \leq n} n_j q_{jk} \right) x_k = 0, \quad n_j \in \mathbf{Z} \end{aligned}$$

$X = \{x_i\}_{1 \leq i \leq n}$ étant une base de F , la relation précédente équivaut à

$$\forall k \ (1 \leq k \leq n), \quad \sum_{1 \leq j \leq n} n_j q_{jk} = 0.$$

Ainsi les entiers n_j ($1 \leq j \leq n$) sont solutions d'un système linéaire homogène de n équations et n inconnues, à coefficients dans \mathbb{Z} (donc dans \mathbb{Q}), dont le déterminant est non nul; on en déduit que $n_j = 0$, quel que soit j ($1 \leq j \leq n$); par suite, Y est une base de F .

Exemples (8.47) : Soit $X = \{x_i\}_{1 \leq i \leq n}$ une base d'un groupe abélien libre de type fini F .

— Changement de base du *type* (α) :

Soit σ une permutation des entiers $\{1, 2, \dots, n\}$, on vérifie facilement que $Y = \{y_i\}_{1 \leq i \leq n}$ tel que, pour tout i ($1 \leq i \leq n$), $y_i = x_{\sigma(i)}$, est encore une base de F . Dans ce cas, la matrice Q de passage de la base X à la base Y est telle que, dans chaque ligne et dans chaque colonne, tous les éléments sont nuls sauf un seul qui est égal à 1.

— Changement de base du *type* (β) :

Si $i \neq j$ et $a \in \mathbb{Z}$, posons

$$\text{et} \quad \begin{cases} y_i = x_i + ax_j \\ y_k = x_k, \quad \text{pour tout } k \neq i, \quad 1 \leq k \leq n. \end{cases}$$

Ces relations définissent la matrice

$$Q = \begin{pmatrix} & \begin{matrix} i & & j \end{matrix} \\ \begin{matrix} i \\ \\ \\ \\ \\ \\ \\ 0 \end{matrix} & \begin{pmatrix} 1 & 0 \dots 0 & 0 \dots 0 & 0 \dots 0 \\ 0 & 1 & 0 \dots a & 0 \dots 0 \\ & \diagdown & & \\ & & 1 & \\ & & & \diagdown \\ & & & & 1 \end{pmatrix} \end{pmatrix}$$

$\det(Q) = 1$, donc $\{y_1, y_2, \dots, y_n\}$ est une base de F .

— Changement de base du *type* (γ) :

Si, pour tout i ($1 \leq i \leq n$), on pose $y_i = \varepsilon_i x_i$, où $\varepsilon_i = \pm 1$, alors $\{y_i\}_{1 \leq i \leq n}$ est encore une base de F ; la matrice Q s'écrit dans ce cas :

$$Q = \begin{pmatrix} \varepsilon_1 & 0 & \dots & 0 \\ 0 & \varepsilon_2 & & \\ \vdots & & \ddots & \\ 0 & & & \varepsilon_n \end{pmatrix}$$

$$\det Q = \varepsilon_1 \varepsilon_2 \dots \varepsilon_n = \pm 1.$$

PROPOSITION (8.48). *Quel que soit $P \in U_n(\mathbf{Z})$, les entiers formant une ligne (ou une colonne) de P sont premiers entre eux.*

Preuve : Soit $P \in U_n(\mathbf{Z})$, alors $\det(P) = \pm 1$. Si on développe le déterminant de P suivant la i -ème ligne, on a :

$$p_{i1} P_{i1} + p_{i2} P_{i2} + \dots + p_{in} P_{in} = \pm 1 \quad (17)$$

Les cofacteurs P_{ij} ($1 \leq j \leq n$) étant des entiers, la relation (17) exprime que $p_{i1}, p_{i2}, \dots, p_{in}$ sont premiers entre eux (théorème de Bezout).

En développant le déterminant de P suivant la j -ème colonne, on obtient, pour tout j ($1 \leq j \leq n$),

$$p_{1j}, p_{2j}, \dots, p_{nj} \text{ premiers entre eux.}$$

COROLLAIRE (8.49). *Si $X = \{x_i\}_{1 \leq i \leq n}$ est une base d'un groupe abélien libre de type fini F et si $Y = \{y_j\}_{1 \leq j \leq n}$ est une autre base de F , alors, pour tout j ($1 \leq j \leq n$), on a :*

$$y_j = \sum_{1 \leq k \leq n} q_{jk} x_k,$$

où $q_{j1}, q_{j2}, \dots, q_{jn}$ sont des entiers premiers entre eux.

Notation (8.50) : On notera (a_1, a_2, \dots, a_n) un PGCD de n entiers a_i dans \mathbf{Z} ; on exprimera donc que a_1, a_2, \dots, a_n sont premiers entre eux, en écrivant : $(a_1, a_2, \dots, a_n) = 1$.

b) Rang d'un sous-groupe d'un groupe abélien libre de type fini.

Remarque (8.51) : F étant un groupe abélien libre de rang fini $n \geq 1$, une famille génératrice de F ne contient pas nécessairement une base F ; de plus, si $y \in F$ et $y \neq 0$, il n'existe pas nécessairement une base de F contenant y .

Considérons par exemple $F = \mathbf{Z}$; les seules bases de \mathbf{Z} sont $\{1\}$ et $\{-1\}$, donc $\{2, 3\}$ est une partie génératrice de \mathbf{Z} ne contenant aucune base de \mathbf{Z} ; de plus, quel que soit k non nul, tel que $k \neq \pm 1$, il n'existe aucune base de \mathbf{Z} contenant k .

LEMME (8.52) (R. Rado [59]). *Soit $X = \{x_i\}_{1 \leq i \leq n}$ une base d'un groupe abélien de type fini F . Soit $y \in F$ tel que :*

$$y = \sum_{1 \leq i \leq n} a_i x_i, \quad \text{avec } (a_1, a_2, \dots, a_n) = 1;$$

il existe alors une base de F contenant y .

Preuve : Posons $s = |a_1| + |a_2| + \dots + |a_n|$ et supposons $n \geq 2$.

— Si $s = 1$, il existe nécessairement j ($1 \leq j \leq n$) tel que $a_j = \pm 1$ et $a_k = 0$, quel que soit $k \neq j$, $1 \leq k \leq n$.

En posant $y = \pm x_j$ et $y_k = x_k$, pour tout $k \neq j$, on définit un changement de base du type (γ) (exemples (8.47)), ainsi $\{y_1, \dots, y_{j-1}, y, y_{j+1}, \dots, y_n\}$ est une base de F contenant y .

— Supposons $s > 1$ et raisonnons par récurrence sur s . $s > 1$ implique qu'il existe au moins deux entiers a_i non nuls, puisque $(a_1, a_2, \dots, a_n) = 1$. Sans restreindre la généralité, on peut supposer $a_1 \geq a_2 > 0$.

Posons alors $x'_1 = x_1$, $x'_2 = x_2 + x_1$, $x'_j = x_j$ pour tout j ($3 \leq j \leq n$); on définit ainsi un changement de base du type (β) (exemples (8.47)), donc $\{x'_i\}_{1 \leq i \leq n}$ est une base de F et :

$$y = (a_1 - a_2) x'_1 + a_2 x'_2 + a_3 x'_3 + \dots + a_n x'_n,$$

avec $((a_1 - a_2), a_2, a_3, \dots, a_n) = 1$

mais $|a_1 - a_2| + |a_2| + \dots + |a_n| < s$.

L'hypothèse de récurrence sur s permet de conclure qu'il existe une base de F contenant y .

Remarques (8.53) :

1° Les hypothèses étant celles du lemme de Rado, en effectuant éventuellement un changement de base du type (α) (exemples (8.47)), on peut affirmer qu'il existe une base de F , ayant comme premier élément y .

2° $X = \{x_i\}_{1 \leq i \leq n}$ étant une base d'un groupe abélien libre F , alors, le lemme (8.52) et le corollaire (8.49) impliquent que $y = \sum_{1 \leq i \leq n} a_i x_i$ appartient à une base de F , si et seulement si $(a_1, a_2, \dots, a_n) = 1$.

3° On sait (théorème (8.28)) que tout sous-groupe H d'un groupe abélien libre F est un groupe abélien libre. Le lemme de Rado permet alors de construire une base de H à partir d'une base de F et on prouve ainsi que $\text{rang}(H) \leq \text{rang}(F)$ c'est l'objet du théorème suivant :

THÉORÈME (8.54). Soient F un groupe abélien libre de rang fini $n \geq 1$ et H un sous-groupe de F ; alors H est un groupe abélien libre de rang $m \leq n$. De plus, il est possible de choisir une base $\{u_i\}_{1 \leq i \leq n}$ de F de telle façon que H ait une base de la forme :

$$\{h_1 u_1, h_2 u_2, \dots, h_m u_m\},$$

où les h_i ($1 \leq i \leq n$) sont des entiers strictement positifs tels que :

$$h_i \mid h_{i+1}, \quad \forall i \ (1 \leq i \leq m-1)$$

($h_i \mid h_{i+1}$ signifie « h_i divise h_{i+1} »).

Preuve : On suppose $H \neq (0)$.

a) Soit $X = \{x_i\}_{1 \leq i \leq n}$ une base de F .

A tout x non nul de F tel que $x = \sum_{1 \leq i \leq n} a_i x_i$, on associe le PGCD positif des entiers a_i ($1 \leq i \leq n$); on pose

$$\delta(x) = (a_1, a_2, \dots, a_n), \quad \delta(x) > 0.$$

— Montrons que $\delta(x)$ est indépendant du choix de la base X .

En effet, soit $X' = \{x'_i\}_{1 \leq i \leq n}$ une autre base de F ; pour tout i ($1 \leq i \leq n$), on a $x'_i = \sum_{1 \leq j \leq n} p_{ij} x'_j$, où $P = (p_{ij})$ est telle que $\det(P) = \pm 1$.

On en déduit que $x = \sum_{1 \leq j \leq n} a'_j x'_j$ où $a'_j = \sum_{1 \leq i \leq n} a_i p_{ij}$; par suite $\delta(x) \mid a'_j$, quel que soit j ($1 \leq j \leq n$), d'où

$$(a'_1, a'_2, \dots, a'_n) \geq (a_1, a_2, \dots, a_n).$$

En échangeant le rôle des bases X et X' , on obtient

$$(a'_1, a'_2, \dots, a'_n) = (a_1, a_2, \dots, a_n).$$

b) Soit $E = \{\delta(x); x \in H \setminus \{0\}\}$; E est une partie non vide de N , donc E contient *un plus petit élément*, que nous notons h_1 ; on a $h_1 \geq 1$ et il existe $y_1 \in H \setminus \{0\}$ tel que $\delta(y_1) = h_1$. Dans F , y_1 s'écrit de façon unique :

$$y_1 = \sum_{1 \leq i \leq n} b_i x_i, \quad \text{où } b_i \in \mathbf{Z}, \quad \forall i \ (1 \leq i \leq n).$$

$$\delta(y_1) = h_1 \Rightarrow y_1 = h_1 \left(\sum_{1 \leq i \leq n} c_i x_i \right), \quad \text{avec } (c_1, c_2, \dots, c_n) = 1.$$

Posons $u_1 = \sum_{1 \leq i \leq n} c_i x_i$; d'après le lemme (8.52) et la remarque (8.53) ¹⁰, il existe u'_2, u'_3, \dots, u'_n dans F tels que $\{u_1, u'_2, u'_3, \dots, u'_n\}$ soit une base de F .

Utilisons cette nouvelle base de F et montrons que, quel que soit $y \in H \setminus \{0\}$, tel que $y = d_1 u_1 + d_2 u'_2 + \dots + d_n u'_n$, on a $h_1 \mid d_1$.

En effet, supposons $h_1 \nmid d_1$; h_1 étant le plus petit élément de E , il existe q et r dans \mathbf{Z} tels que :

$$d_1 = qh_1 + r, \quad \text{avec } 0 < r < h_1;$$

alors, $y - qy_1 = ru_1 + d_2 u'_2 + \dots + d_n u'_n$ est un élément de H tel que $\delta(y - qy_1) \leq r < h_1$, d'où une contradiction avec la minimalité de h_1 dans E .

Par suite, $d_1 = qh_1$ et

$$y - qy_1 = d_2 u'_2 + \dots + d_n u'_n \quad (18)$$

c) Compte tenu de ce qui précède, démontrons le théorème (8.54) par récurrence sur n .

— Si $n = 1$. On a $F \simeq \mathbf{Z}$. Tout sous-groupe non nul de \mathbf{Z} est de la forme $k\mathbf{Z}$, $k \geq 1$ dans \mathbf{N} ; par suite, si $F = \langle u_1 \rangle$, tout sous-groupe non nul H de F est de la forme $H = \langle ku_1 \rangle$, $k \geq 1$

dans N (avec les notations de la démonstration b) on trouve, en effet, dans le cas $n = 1$, $H = \langle h_1 u_1 \rangle$.

— Supposons $n > 1$; posons $F_1 = \bigoplus_{2 \leq i \leq n} \langle u'_i \rangle$ et $H_1 = H \cap F_1$; la relation (18) montre que $y - qy_1 \in H_1$, puisque y et y_1 sont dans H .

1^{er} cas : $H_1 = (0)$; alors $y = qy_1 = qh_1 u_1$, donc $H = \langle h_1 u_1 \rangle$ d'où $\text{rang } H = 1 < n$.

2^e cas : $H_1 \neq (0)$; on applique l'hypothèse de récurrence à F_1 et H_1 , puisque $\text{rang } F_1 = n - 1$; ainsi, il existe une base $\{u_2, u_3, \dots, u_n\}$ de F_1 telle que H_1 ait une base de la forme : $\{h_2 u_2, \dots, h_m u_m\}$, avec $2 \leq m \leq n$, les h_i étant des entiers positifs non nuls tels que $h_i \mid h_{i+1}$, quel que soit i ($2 \leq i \leq m - 1$). Démontrons que $\{u_1, u_2, \dots, u_n\}$ est une base de F .

On sait, d'après la partie b) de la démonstration, que $\{u_1, u'_2, \dots, u'_n\}$ est une base de F .

D'autre part, $\{u'_2, \dots, u'_n\}$ et $\{u_2, \dots, u_n\}$ étant deux bases de F_1 , pour tout i ($2 \leq i \leq n$), on a :

$$u_i = \sum_{2 \leq j \leq n} p_{ij} u'_j, \quad \text{où les } p_{ij} \text{ sont dans } \mathbb{Z}.$$

Supposons que :

$$\sum_{1 \leq i \leq n} b_i u_i = 0 \quad \text{avec } b_1, b_2, \dots, b_n \text{ non tous nuls dans } \mathbb{Z}.$$

Les u_i ($2 \leq i \leq n$) étant linéairement indépendants sur \mathbb{Z} , on a nécessairement $b_1 \neq 0$, on en déduit :

$$b_1 u_1 + b_2 \left(\sum_{2 \leq j \leq n} p_{2j} u'_j \right) + \dots + b_n \left(\sum_{2 \leq j \leq n} p_{nj} u'_j \right) = 0.$$

Or $\{u_1, u'_2, \dots, u'_n\}$ étant une base de F , l'égalité précédente implique $b_1 = 0$, d'où une contradiction; ainsi $\{u_1, u_2, \dots, u_n\}$ est une base de F .

Vérifions alors que $H = \bigoplus_{1 \leq i \leq m} \langle h_i u_i \rangle$.

D'après la définition de u_1 , $y_1 = h_1 u_1$ appartient à H ; d'autre part,

$$H_1 = H \cap F_1 = \bigoplus_{2 \leq i \leq m} \langle h_i u_i \rangle.$$

$\{u_i\}_{1 \leq i \leq n}$ étant une base de F , la famille $\{u_i\}_{1 \leq i \leq m}$ est libre sur \mathbf{Z} et il en est de même de la famille $\{h_i u_i\}_{1 \leq i \leq m}$. De plus, d'après (18), tout $y \in H \setminus \{0\}$ s'écrit :

$$y = qh_1 u_1 + w, \quad \text{où } w \in H_1,$$

par suite $H = \bigoplus_{1 \leq i \leq m} \langle h_i u_i \rangle$, donc $\text{rang}(H) = m \leq n$.

Il reste à prouver que $h_1 \mid h_2$. Considérons, dans H , l'élément $y_0 = h_1 u_1 + h_2 u_2$. On a $\delta(y_0) \geq h_1$, car h_1 est le plus petit élément de E ; mais,

$$(h_1, h_2) \geq h_1 \Rightarrow (h_1, h_2) = h_1,$$

donc $h_1 \mid h_2$.

B / Décomposition canonique d'un groupe abélien de type fini

a) Théorème de structure :

PROPOSITION (8.55). *G étant un groupe abélien de type fini, alors :*

- 1° *G est de torsion si, et seulement si, G est fini ;*
- 2° *G est sans torsion si, et seulement si, G est libre.*

Preuve :

1° Un groupe abélien fini est de type fini et de torsion; démontrons la réciproque.

Soit $\{x_1, x_2, \dots, x_r\}$ une famille génératrice de G ($r \geq 1$ dans \mathbf{N}). Tout élément $x \in G$ s'écrit sous la forme :

$$x = \sum_{1 \leq i \leq r} n_i x_i, \quad n_i \in \mathbf{Z}, \quad \forall i (1 \leq i \leq r).$$

G étant par hypothèse sans torsion, chaque élément x_i est d'ordre fini; posons

$$\alpha_i = o(x_i), \quad 1 \leq i \leq r.$$

On en déduit que tout $x \in G$ peut s'écrire sous la forme :

$$x = \sum_{1 \leq i \leq r} n_i x_i, \quad 0 \leq n_i \leq \alpha_i - 1 \text{ dans } \mathbf{Z}, \quad \forall i (1 \leq i \leq r).$$

Par suite, G n'a qu'un nombre fini d'éléments.

2° Un groupe abélien libre est sans torsion (remarque (8.35)); démontrons qu'un groupe abélien de type fini et sans torsion est libre.

Soit G un groupe abélien sans torsion, engendré par une famille finie d'éléments x_1, x_2, \dots, x_r , $r \geq 1$ dans N . On peut donc écrire :

$$G = \sum_{1 \leq i \leq r} \langle x_i \rangle, \quad \text{avec } \langle x_i \rangle \simeq \mathbf{Z}, \quad \forall i (1 \leq i \leq r).$$

Si $r = 1$, on a $G \simeq \mathbf{Z}$, donc G est libre de rang 1.

Pour $r > 1$, raisonnons par récurrence sur r . L'hypothèse de récurrence est donc que tout groupe abélien de type fini, sans torsion, engendré par k éléments, $1 \leq k \leq r - 1$, est libre. Dans G , supposons :

$$0 = \sum_{1 \leq i \leq r} n_i x_i,$$

où les n_i ($1 \leq i \leq r$) sont non tous nuls dans \mathbf{Z} et

$$(n_1, n_2, \dots, n_r) = 1.$$

Cette dernière condition est toujours possible, puisque, si $d = (n_1, n_2, \dots, n_r)$, chaque n_i s'écrit

$$n_i = d n'_i, \quad \text{avec } (n'_1, n'_2, \dots, n'_r) = 1$$

et $0 = d \sum_{1 \leq i \leq r} n'_i x_i$ implique $0 = \sum_{1 \leq i \leq r} n'_i x_i$, car G est sans torsion.

1^{er} cas : Il existe j ($1 \leq j \leq r$) tel que $n_j = \pm 1$; on peut supposer $n_1 = \pm 1$, alors

$$0 = \sum_{1 \leq i \leq r} n_i x_i \Rightarrow x_1 = \pm \left(\sum_{2 \leq i \leq r} n_i x_i \right);$$

par suite, G est engendré par $\{x_2, x_3, \dots, x_r\}$, donc G est libre, d'après l'hypothèse de récurrence.

2^e cas : $n_j \neq \pm 1$, quel que soit j ($1 \leq j \leq r$).

$(n_1, n_2, \dots, n_r) = 1$ implique qu'il existe au moins deux entiers n_i et n_j non nuls et tels que $|n_i| \neq |n_j|$. On peut supposer $|n_1| > |n_2| > 0$.

En utilisant l'algorithme de la division euclidienne dans \mathbf{Z} , on peut trouver $\lambda \in \mathbf{Z}$ tel que

$$0 < |n_1 - \lambda n_2| \leq |n_2|.$$

Posons alors $x'_2 = x_2 + \lambda x_1$.

On vérifie facilement que $\{x_1, x'_2, x_3, \dots, x_r\}$ est encore une famille génératrice de G et que :

$$0 = (n_1 - \lambda n_2) x_1 + n_2 x'_2 + \dots + n_r x_r,$$

avec $((n_1 - \lambda n_2), n_2, \dots, n_r) = 1$, et $|n_1 - \lambda n_2| < |n_1|$;

alors,

- ou bien $|n_1 - \lambda n_2| = 1$: on est ramené au 1^{er} cas et G est libre ;
- ou bien $|n_1 - \lambda n_2| > 1$; dans ce cas on réitère le processus précédent jusqu'à ce que l'un des coefficients soit égal à ± 1 .

THÉORÈME (8.56). *Tout groupe abélien de type fini est somme directe, de façon unique, à un isomorphisme près, d'un groupe abélien libre de type fini et d'un groupe fini.*

Preuve : G étant un groupe abélien de type fini, soit $T(G)$ son sous-groupe de torsion ; alors, d'une part, $\frac{G}{T(G)}$ est sans torsion (théorème (8.36)) ; d'autre part, $\frac{G}{T(G)}$ est image homomorphe d'un groupe abélien de type fini, donc est de type fini ; par suite, d'après la proposition (8.55) :

$\frac{G}{T(G)}$ est un groupe abélien libre de type fini.

On en déduit que $T(G)$ est facteur direct dans G (proposition (8.32)), donc il existe $F \leq G$ tel que :

$$G = T(G) \oplus F \tag{19}$$

F est isomorphe à $\frac{G}{T(G)}$, donc F est libre de type fini et $T(G)$ est isomorphe à $\frac{G}{F}$, par suite $T(G)$ est de type fini et de torsion, donc $T(G)$ est fini (proposition (8.55)).

Supposons $G = H \oplus K$ où H est un groupe abélien fini et K un groupe abélien libre de type fini. D'après la proposition (8.6), on peut supposer que G est somme directe interne de H et K .

On a nécessairement $H \leq T(G)$; soit $x \in T(G)$, x s'écrit de façon unique $x = h + k$, $h \in H$, $k \in K$.

Supposons $o(x) = n > 1$, alors, $nh + nk = 0$, d'où $nh = -nk$. $H \cap K = (0)$ implique $nh = -nk = 0$.

Dans le groupe abélien libre K , $nk = 0$, $n \neq 0$ implique $k = 0$, d'où $x = h$. On en déduit que $H = T(G)$, d'où $K \simeq \frac{G}{T(G)}$, donc $K \simeq F$.

THÉORÈME (8.57). Théorème de structure.

G étant un groupe abélien de type fini, on a

$$G = \langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \dots \oplus \langle x_r \rangle \oplus \langle y_1 \rangle \oplus \langle y_2 \rangle \oplus \dots \oplus \langle y_s \rangle \quad (20)$$

où $r \in \mathbb{N}$ et si $r \neq 0$, $\langle x_i \rangle \simeq \mathbb{Z}$, quel que soit i ($1 \leq i \leq r$), $s \in \mathbb{N}$ et si $s \neq 0$, pour tout j ($1 \leq j \leq s$), $\langle y_j \rangle$ est cyclique d'ordre d_j , tel que $d_{j+1} \mid d_j$, $1 \leq j \leq s-1$.

Preuve : G étant abélien de type fini, il existe un groupe abélien libre de rang fini F et un sous-groupe H de F tel que $G \simeq \frac{F}{H}$ (théorème (8.25)). Compte tenu de la proposition (8.6), il suffit de démontrer la relation (20) pour le groupe $\frac{F}{H}$.

Posons $\text{rang}(F) = n > 0$ et $\text{rang}(H) = m$, $0 \leq m \leq n$.

Si $m = 0$, $\frac{F}{H} = F$; la relation (20) est vérifiée avec $r = n$, $s = 0$.

Si $m = n$, $\frac{F}{H} = (0)$; la relation (20) est vérifiée avec $r = 0$, $s = 1$, $d_1 = 1$.

Lorsque $n = 1$, on est ramené aux cas ci-dessus, on suppose donc, dans ce qui suit : $n > 1$ et $0 < m < n$.

D'après le théorème (8.54), il existe une base $\{u_i\}_{1 \leq i \leq n}$ de F telle que H ait une base de la forme : $\{h_i u_i\}_{1 \leq i \leq m}$ où les h_i sont

des entiers strictement positifs tels que $h_i \mid h_{i+1}$, quel que soit i ($1 \leq i \leq m-1$).

Ecrivons $H = \bigoplus_{1 \leq i \leq n} \langle h_i u_i \rangle$, avec $h_i = 0$ pour $m+1 \leq i \leq n$.

Par ailleurs, pour $1 \leq i \leq m$, certains h_i peuvent être égaux à 1; supposons : $h_i = 1$ pour $0 < i \leq l$, avec $0 \leq l \leq m$; pour $l+1 \leq i \leq m$, on a alors : $1 < h_i \leq h_{i+1} \leq \dots \leq h_m$.

$$\frac{F}{H} = \frac{\bigoplus_{1 \leq i \leq n} \langle u_i \rangle}{\bigoplus_{1 \leq i \leq n} \langle h_i u_i \rangle} \simeq \bigoplus_{1 \leq i \leq n} \frac{\langle u_i \rangle}{\langle h_i u_i \rangle} \quad (\text{exercice 3, chap. IV}).$$

Posons $\frac{\langle u_i \rangle}{\langle h_i u_i \rangle} = \langle \bar{u}_i \rangle$, pour $1 \leq i \leq n$; on a alors : pour $1 \leq i \leq l$, $\langle \bar{u}_i \rangle = \bar{0}$; pour $l+1 \leq i \leq m$, $\langle \bar{u}_i \rangle$ cyclique d'ordre $h_i > 1$ et $h_i \mid h_{i+1}$; pour $m+1 \leq i \leq n$, $\langle \bar{u}_i \rangle \simeq \mathbf{Z}$.

Si l'on pose $n-m=r$, $m-l=s$ et : pour $1 \leq i \leq r$, $\langle x_i \rangle = \langle \bar{u}_{m+i} \rangle$, on a $\langle x_i \rangle \simeq \mathbf{Z}$, $\forall i$ ($1 \leq i \leq r$); pour $1 \leq j \leq s$ (si $s \neq 0$), $\langle y_j \rangle = \langle \bar{u}_{m-j+1} \rangle$, on a $\langle y_j \rangle$ cyclique d'ordre $d_j = h_{m-j+1}$; et $h_{m-j} \mid h_{m-j+1}$ implique

$$d_{j+1} \mid d_j, \quad \forall j \ (1 \leq j \leq s-1).$$

On obtient ainsi la relation (20) pour le groupe $\frac{F}{H}$.

b) *Théorème d'unicité. Invariants et diviseurs élémentaires.*

Nous allons démontrer, dans ce paragraphe, l'unicité de la décomposition d'un groupe abélien de type fini sous la forme (20).

THÉORÈME (8.58). Théorème d'unicité.

Si G est un groupe abélien de type fini, tel que :

$$G = \langle x_i \rangle \oplus \dots \oplus \langle x_r \rangle \oplus \langle y_1 \rangle \oplus \dots \oplus \langle y_s \rangle \quad (20)$$

$$\text{et} \quad G = \langle v_1 \rangle \oplus \dots \oplus \langle v_q \rangle \oplus \langle w_1 \rangle \oplus \dots \oplus \langle w_t \rangle \quad (21)$$

où r, s, q, t sont dans \mathbf{N} et

$$\langle x_i \rangle \simeq \mathbf{Z}, \quad \langle v_k \rangle \simeq \mathbf{Z}, \quad \forall i \ (1 \leq i \leq r), \quad \forall k \ (1 \leq k \leq q);$$

- pour $1 \leq j \leq s$, $\langle y_j \rangle$ est cyclique d'ordre d_j , tel que $d_{j+1} \mid d_j$,
 — pour $1 \leq l \leq t$, $\langle w_l \rangle$ est cyclique d'ordre e_l , tel que $e_{l+1} \mid e_l$;
 alors 1° $r = q$;

2° $s = t$ et $d_j = e_j$, quel que soit j ($1 \leq j \leq s$).

Preuve : Elle se fera en trois étapes :

1° Les hypothèses impliquent que :

$$F_1 = \bigoplus_{1 \leq i \leq r} \langle x_i \rangle \quad \text{et} \quad F_2 = \bigoplus_{1 \leq k \leq q} \langle v_k \rangle$$

sont des groupes libres de rang fini :

$$\text{rang}(F_1) = r \quad \text{et} \quad \text{rang}(F_2) = q;$$

$$T_1 = \bigoplus_{1 \leq j \leq s} \langle y_j \rangle \quad \text{et} \quad T_2 = \bigoplus_{1 \leq l \leq t} \langle w_l \rangle$$

sont des groupes finis et

$$G = F_1 \oplus T_1 = F_2 \oplus T_2.$$

Or, d'après le théorème (8.56), G s'écrit de façon unique, à un isomorphisme près : $G = F \oplus T(G)$, où F est libre de rang fini et $T(G)$ est fini.

On en déduit :

- $F_1 \simeq F$ et $F_2 \simeq F$, donc $F_1 \simeq F_2$, d'où $r = q$;
 — $T_1 \simeq T(G)$ et $T_2 \simeq T(G)$, d'où $T_1 \simeq T_2$, ce résultat implique $d_1 d_2 \dots d_s = e_1 e_2 \dots e_t$, mais il faut prouver que $s = t$ et $d_j = e_j$, pour tout j ($1 \leq j \leq s$).

On remarque que, si (20) et (21) sont des sommes directes internes (ce que l'on peut toujours supposer), alors $T_1 = T(G) = T_2$ (voir la démonstration du théorème (8.56)).

Si $T(G)$ est d'ordre $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ où les p_i sont des nombres premiers distincts et les $\alpha_i > 0$ dans \mathbb{N} , on a

$$T(G) = \bigoplus_{1 \leq i \leq k} P_i \quad \text{où } o(P_i) = p_i^{\alpha_i} \quad (\text{remarque (8.44)}).$$

Démontrons, alors, l'unicité de la relation (21) pour un p -groupe abélien fini, p , étant un nombre premier donné.

2° LEMME (8.59). Soit P un p -groupe abélien fini tel que l'on ait :

$$P = \bigoplus_{1 \leq j \leq s} \langle y_j \rangle = \bigoplus_{1 \leq l \leq t} \langle w_l \rangle \quad (22)$$

où $o(y_j) = p^{\delta_j}$, $1 \leq j \leq s$; $o(w_l) = p^{\epsilon_l}$, $1 \leq l \leq t$

et $\delta_1 \geq \delta_2 \geq \dots \geq \delta_s$, $\epsilon_1 \geq \epsilon_2 \geq \dots \geq \epsilon_t$,

alors $s = t$ et $\delta_j = \epsilon_j$, $\forall j$ ($1 \leq j \leq s$).

Posons $o(P) = p^\alpha$, $\alpha \geq 1$ dans N .

Si $\alpha = 1$, P est cyclique d'ordre premier p ; dans ce cas, on a nécessairement $s = t = 1$ et $\delta_1 = \epsilon_1 = 1$.

Supposons $\alpha > 1$ et raisonnons par récurrence sur α .

Posons $H_p = \{x \in P; o(x) = p\}$; H_p est un sous-groupe de P , déterminons son ordre.

Soit $x \in H_p$, d'après la première égalité (22), on peut écrire :

$$x = \sum_{1 \leq j \leq s} a_j y_j, \quad a_j \in \mathbb{Z}, \quad 0 \leq a_j < p^{\delta_j}, \quad \forall j \ (1 \leq j \leq s).$$

$$px = 0 \Rightarrow pa_j y_j = 0, \quad \forall j \ (1 \leq j \leq s),$$

$$\text{donc } px = 0 \Rightarrow p^{\delta_j} \mid pa_j, \quad \forall j \ (1 \leq j \leq s).$$

On en déduit que, pour tout j ($1 \leq j \leq s$), on a

$$a_j = b_j p^{\delta_j - 1}, \quad \text{avec } 0 \leq b_j < p \text{ dans } N.$$

Pour chaque indice j , il y a p valeurs possibles de b_j , donc de a_j , tels que $px = 0$; par suite, $o(H_p) = p^s$.

En utilisant la seconde décomposition de P , on aurait

$$o(H_p) = p^t,$$

$$\text{d'où } s = t.$$

Il reste à prouver que $\delta_j = \epsilon_j$, pour tout j ($1 \leq j \leq s$).

Posons $K_p = \{x \in P; \exists x' \in P, x = px'\}$;

$$x \in K_p \Leftrightarrow x = \sum_{1 \leq j \leq s} pc_j y_j, \quad c_j \in \mathbb{Z}, \quad \forall j \ (1 \leq j \leq s);$$

on en déduit que K_p est un sous-groupe de P et $K_p = \sum_{1 \leq j \leq s} \langle py_j \rangle$.

Si $y_j \in H_p$, alors $py_j = 0$, donc $o(y_j) = p$, c'est-à-dire $\delta_j = 1$.

Supposons

$$\delta_1 \geq \delta_2 \geq \dots \geq \delta_q > 1$$

et $\delta_{q+1} = \delta_{q+2} = \dots = \delta_s = 1,$

alors $K_p = \bigoplus_{1 \leq j \leq q} \langle py_j \rangle, \quad o(py_j) = p^{\delta_j-1}, \quad \forall j (1 \leq j \leq q).$

En utilisant la seconde décomposition de P , on obtient de même :

$$K_p = \bigoplus_{1 \leq l \leq q'} \langle pw_l \rangle, \quad 0 < q' \leq s, \\ o(pw_l) = p^{q'-1}, \quad \forall l (1 \leq l \leq q').$$

Si $\delta_j = 1$, pour tout j ($1 \leq j \leq s$), alors $K_p = (0)$, $q = 0$, donc $q' = 0$ et $\delta_j = \varepsilon_j = 1$, quel que soit j ($1 \leq j \leq s$).

Si $q \neq 0$, K_p est un sous-groupe propre, non nul de P , donc $o(K_p) = p^{\alpha'}$ avec $0 < \alpha' < \alpha$. L'hypothèse de récurrence appliquée au p -groupe K_p donne :

$$q = q' \quad \text{et} \quad \delta_j = \varepsilon_j \quad \text{pour tout } j (1 \leq j \leq q);$$

d'autre part, pour $q + 1 \leq j \leq s$, on a $\delta_j = \varepsilon_j = 1$, par suite

$$\delta_j = \varepsilon_j, \quad \text{quel que soit } j (1 \leq j \leq s).$$

Définition (8.60) : Pour un p -groupe abélien fini P , tel que

$$P = \bigoplus_{1 \leq j \leq s} \langle y_j \rangle, \quad \text{où } o(y_j) = p^{\delta_j}, \quad 1 \leq j \leq s,$$

les $p^{\delta_1}, p^{\delta_2}, \dots, p^{\delta_s}$, tels que $\delta_1 \geq \delta_2 \geq \dots \geq \delta_s$, sont appelés les *diviseurs élémentaires* de P .

D'après ce qui précède, deux p -groupes abéliens finis sont isomorphes, si et seulement s'ils ont les mêmes diviseurs élémentaires.

Définition (8.61) : Pour p , nombre premier donné, on dira qu'un p -groupe abélien fini est de *type* $(\delta_1, \delta_2, \dots, \delta_s)$ si ses diviseurs élémentaires sont $p^{\delta_1}, p^{\delta_2}, \dots, p^{\delta_s}$.

3° Pour achever la démonstration du théorème (8.58), il suffit de prouver que si T est un groupe abélien fini tel que :

$$T = \bigoplus_{1 \leq j \leq s} \langle y_j \rangle = \bigoplus_{1 \leq l \leq t} \langle w_l \rangle,$$

où, pour $1 \leq j \leq s$, $o(y_j) = d_j$ et $d_{j+1} \mid d_j$,

et pour $1 \leq l \leq t$, $o(w_l) = e_l$ et $e_{l+1} \mid e_l$,

alors $s = t$ et $d_j = e_j$, quel que soit j ($1 \leq j \leq s$).

Ecrivons T comme somme directe de ses p_i -sous-groupes de Sylow; si $o(T) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$:

$$T = \bigoplus_{1 \leq i \leq k} P_i, \quad \text{où } o(P_i) = p_i^{\alpha_i}, \quad \alpha_i \geq 1.$$

Quel que soit j ($1 \leq j \leq s$), $o(y_j)$ divise $o(T)$, donc

$$d_j = p_1^{\delta_{j1}} p_2^{\delta_{j2}} \dots p_k^{\delta_{jk}}, \quad \text{avec } 0 \leq \delta_{ji} \leq \alpha_i$$

$$\alpha_i = \sum_{1 \leq j \leq s} \delta_{ji} \quad \text{et} \quad \delta_{j+1,i} \leq \delta_{ji}, \quad \text{car } d_{j+1} \mid d_j.$$

Pour tout j ($1 \leq j \leq s$), on a alors :

$$\langle y_j \rangle = \bigoplus_{1 \leq i \leq k} \langle y_{ji} \rangle, \quad \text{où } o(y_{ji}) = p_i^{\delta_{ji}},$$

$$\text{d'où } T = \bigoplus_{1 \leq j \leq s} \left(\bigoplus_{1 \leq i \leq k} \langle y_{ji} \rangle \right),$$

$$\text{donc } T = \bigoplus_{1 \leq i \leq k} \left(\bigoplus_{1 \leq j \leq s} \langle y_{ji} \rangle \right)$$

$$\text{et } o\left(\bigoplus_{1 \leq j \leq s} \langle y_{ji} \rangle\right) = p_i^{\delta_{1i} + \delta_{2i} + \dots + \delta_{si}} = p_i^{\alpha_i},$$

par suite,

$$\bigoplus_{1 \leq j \leq s} \langle y_{ji} \rangle = P_i$$

et P_i est un p_i -groupe abélien fini de type $(\delta_{1i}, \delta_{2i}, \dots, \delta_{si})$.

En utilisant la décomposition de T sous la forme

$$T = \bigoplus_{1 \leq l \leq t} \langle w_l \rangle, \quad o(w_l) = e_l, \quad e_{l+1} \mid e_l,$$

on trouve que

$$e_i = p_1^{\varepsilon_{1i}} p_2^{\varepsilon_{2i}} \dots p_k^{\varepsilon_{ki}}, \quad \text{avec } \alpha_i = \sum_{1 \leq l \leq t} \varepsilon_{li}, \quad \varepsilon_{l+1,i} \leq \varepsilon_{li}$$

et
$$T = \bigoplus_{1 \leq i \leq k} \left(\bigoplus_{1 \leq l \leq t} \langle w_{li} \rangle \right) \quad \text{avec } P_i = \bigoplus_{1 \leq l \leq t} \langle w_{li} \rangle,$$

ce qui implique que P_i est un p_i -groupe abélien fini de type $(\varepsilon_{1i}, \varepsilon_{2i}, \dots, \varepsilon_{ti})$.

L'application du lemme (8.59) donne alors :

$$s = t \quad \text{et} \quad \delta_{ji} = \varepsilon_{ji},$$

pour tout j ($1 \leq j \leq s$) et tout i ($1 \leq i \leq k$); on en déduit que $d_j = \varepsilon_j$, quel que soit j ($1 \leq j \leq s$).

Définition (8.62) : Compte tenu de l'unicité de la décomposition d'un groupe abélien de type fini G sous la forme (20) :

$$G = \langle x_1 \rangle \oplus \dots \oplus \langle x_r \rangle \oplus \langle y_1 \rangle \oplus \dots \oplus \langle y_s \rangle,$$

où, pour $1 \leq i \leq r$, $\langle x_i \rangle \simeq \mathbf{Z}$ et pour $1 \leq j \leq s$, $o(y_j) = d_j$ et $d_{j+1} \mid d_j$, celle-ci sera dite *décomposition canonique* de G .

Définition (8.63) : Etant donné un groupe abélien fini :

$$G = \bigoplus_{1 \leq j \leq s} \langle y_j \rangle, \quad \text{où } o(y_j) = d_j \quad \text{et} \quad d_{j+1} \mid d_j,$$

les entiers d_1, d_2, \dots, d_s sont appelés les *invariants* du groupe G .

Si p_1, p_2, \dots, p_k sont les diviseurs premiers distincts de $o(G)$ tels que $o(G) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, et pour tout j ($1 \leq j \leq s$) :

$$d_j = p_1^{\delta_{j1}} p_2^{\delta_{j2}} \dots p_k^{\delta_{jk}}$$

avec $\delta_{j+1,i} \leq \delta_{ji}$ et $\alpha_i = \delta_{1i} + \delta_{2i} + \dots + \delta_{si}$, quel que soit i ($1 \leq i \leq k$) alors, les $p_i^{\delta_{ji}}$, pour $1 \leq i \leq k$ et $1 \leq j \leq s$, sont les *diviseurs élémentaires* du groupe G .

On peut résumer les caractéristiques du groupe abélien fini G par le tableau suivant :

	p_1	p_2	$\dots\dots$	p_k
d_1	δ_{11}	δ_{12}	$\dots\dots$	δ_{1k}
d_2	δ_{21}	δ_{22}	$\dots\dots$	δ_{2k}
\vdots	\vdots	\vdots		
\vdots	\vdots	\vdots		
d_s	δ_{s1}	δ_{s2}	$\dots\dots$	δ_{sk}

(23)

— Pour tout i ($1 \leq i \leq k$), les éléments de la i -ème colonne : $\delta_{1i} \geq \delta_{2i} \geq \dots \geq \delta_{si}$, définissent le type du p_i -sous-groupe de Sylow de G :

$$o(P_i) = p_i^{\delta_{1i} + \delta_{2i} + \dots + \delta_{si}}$$

et
$$o(G) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad \text{où } \alpha_i = \delta_{1i} + \delta_{2i} + \dots + \delta_{si}.$$

— Pour tout j ($1 \leq j \leq s$), les éléments de la j -ème ligne : $\delta_{j1}, \dots, \delta_{jk}$ sont les puissances des nombres premiers p_i dans l'invariant d_j :

$$d_j = p_1^{\delta_{j1}} p_2^{\delta_{j2}} \dots p_k^{\delta_{jk}} \quad \text{et} \quad o(G) = d_1 d_2 \dots d_s.$$

c) Exemples et applications :

1° Trouver les invariants et la décomposition canonique du groupe abélien fini dont les diviseurs élémentaires sont : $2^3, 2, 3^2, 3, 3$.

Le tableau (23) s'écrit dans ce cas :

	2	3
d_1	3	2
d_2	1	1
d_3	0	1

d'où $d_1 = 2^3 \times 3^2 = 72$; $d_2 = 2 \times 3 = 6$; $d_3 = 3$.

En notant C_k un groupe cyclique d'ordre k ($k \in \mathbb{N}^*$) on a

$$G \simeq C_{72} \oplus C_6 \oplus C_3; \quad o(G) = d_1 d_2 d_3 = 648.$$

2° Trouver les diviseurs élémentaires, les invariants et la décomposition canonique de

$$G \simeq C_{30} \oplus C_{18}.$$

On remarque, en effet, que cette décomposition n'est pas canonique, car 18 ne divise pas 30.

$$30 = 2 \times 3 \times 5 \Rightarrow C_{30} = C_2 \oplus C_3 \oplus C_5$$

$$18 = 2 \times 3^2 \Rightarrow C_{18} = C_2 \oplus C_9.$$

Les diviseurs élémentaires sont donc : 2, 2, 3^2 , 3, 5; on en déduit la décomposition de G en somme directe de ses composantes p -primaires, c'est-à-dire de ses p -sous-groupes de Sylow :

$$G \simeq (C_2 \oplus C_2) \oplus (C_9 \oplus C_3) \oplus C_5.$$

Le tableau (23) s'écrit alors :

	2	3	5
d_1	1	2	1
d_2	1	1	0

$$d_1 = 2 \times 3^2 \times 5 = 90, \quad d_2 = 2 \times 3 = 6; \quad o(G) = d_1 d_2 = 540.$$

La décomposition canonique de G est : $G = C_{90} \oplus C_6$.

d) Technique de décomposition d'un groupe abélien de type fini. On suppose connue la notion de rang d'une matrice.

1° *Remarques préliminaires :* Tout groupe abélien de type fini étant, à un isomorphisme près, le quotient d'un groupe abélien libre de rang fini, considérons un tel quotient $\frac{F}{H}$.

Posons $\text{rang}(F) = n \geq 1$ et $\text{rang}(H) = m$, $0 \leq m \leq n$.

Soit $X = \{x_j\}_{1 \leq j \leq n}$ une base de F et $\{z_i\}_{1 \leq i \leq m}$ une base de H . Pour tout i ($1 \leq i \leq m$), on a :

$$z_i = \sum_{1 \leq j \leq n} a_{ij} x_j, \quad a_{ij} \in \mathbb{Z} \quad (24)$$

Soit $A = (a_{ij})$ la matrice à m lignes et n colonnes sur \mathbf{Z} dont la i -ème ligne est formée par les composantes a_{ij} de z_i dans la base $\{x_j\}_{1 \leq j \leq n}$ de F .

Les z_i ($1 \leq i \leq m$) étant linéairement indépendants sur \mathbf{Z} , on en déduit que : $\text{rang}(A) = m$.

D'autre part, d'après le théorème (8.54), il existe une base $\{u_i\}_{1 \leq i \leq n}$ de F telle que H ait une base de la forme

$$\{h_i u_i\}_{1 \leq i \leq m}, \quad \text{avec } h_i > 0 \text{ dans } \mathbf{N}.$$

Le passage de la base $\{x_i\}_{1 \leq i \leq n}$ à la base $\{u_i\}_{1 \leq i \leq n}$ de F transforme donc la matrice A en la matrice $A' \in M_{m \times n}(\mathbf{Z})$, telle que :

$$A' = \begin{pmatrix} h_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & h_2 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & 0 & & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & h_m & 0 & \dots & 0 \end{pmatrix}$$

dont les $n - m$ dernières colonnes sont nulles.

On démontre en algèbre linéaire (voir [51]) que, dans la pratique, la matrice A' peut être obtenue à partir de la matrice A , par des « transformations élémentaires » successives, qui correspondent à des changements de bases de types (α) , (β) , (γ) vus dans les exemples (8.47).

Ces trois types de transformations élémentaires peuvent être symbolisés de la façon suivante :

- Type $T_{i,j}$: échange des vecteurs x_i et x_j , donc dans A : échange des colonnes i et j .
- Type $T_i + aT_j$: remplacement de x_i par $x_i + ax_j$, $a \in \mathbf{Z}$, donc dans A : remplacement de la i -ème colonne par la i -ème colonne additionnée de la j -ème colonne multipliée par a .
- Type $-T_i$: remplacement de x_i par $-x_i$, donc dans A : remplacement de la i -ème colonne par son opposée.

On démontre, en algèbre linéaire, que des transformations de même type peuvent être faites sur les lignes de A .

Elles seront respectivement notées : $L_{i,j}$, $L_i + aL_j$, $-L_i$ et elles correspondent à l'échange ou au remplacement de certaines relations du système (24) par d'autres, ces opérations transformant le système (24) en un système équivalent, le rang de la matrice des coefficients est donc conservé.

La détermination de la matrice A' permet de connaître les entiers h_i ($1 \leq i \leq m$), donc d'obtenir une décomposition de $\frac{F}{H}$ comme somme directe de groupes monogènes, puisqu'en écrivant :

$$H = \bigoplus_{1 \leq i \leq n} \langle h_i u_i \rangle, \quad \text{avec } h_i = 0 \text{ pour } m+1 \leq i \leq n,$$

on a (voir démonstration du théorème (8.54)) :

$$\frac{F}{H} = C_{h_1} \oplus C_{h_2} \oplus \dots \oplus C_{h_m} \oplus C_\infty \oplus \dots \oplus C_\infty \quad (25)$$

où, pour tout i ($1 \leq i \leq m$), C_{h_i} est cyclique d'ordre h_i et $C_\infty \oplus \dots \oplus C_\infty$ est la somme directe de $n - m$ groupes monogènes infinis.

Remarque (8.64) : Dans la matrice de la forme A' obtenue à partir de A par des transformations élémentaires successives, les entiers $h_i > 0$ ne vérifient pas nécessairement des conditions de divisibilité telles que $h_i \mid h_{i+1}$ (voir théorème (8.54)), la décomposition obtenue n'est donc pas toujours canonique.

2° Décomposition d'un groupe abélien de type fini, donné par une famille génératrice : Soient F un groupe abélien libre de rang $n \geq 1$ et H un sous-groupe de F de rang m , dont une base $\{z_i\}_{1 \leq i \leq m}$ est définie en fonction d'une base $\{x_j\}_{1 \leq j \leq n}$ de F , par les relations (24).

Notons \bar{x} la classe modulo H d'un élément x quelconque de F . Le groupe $\frac{F}{H}$ est alors engendré par les n éléments $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n$ qui vérifient les m relations :

$$\begin{cases} \sum_{1 \leq j \leq n} a_{ij} \bar{x}_j = \bar{0}, & 1 \leq i \leq m, \quad a_{ij} \in \mathbb{Z} \\ \text{et } A = (a_{ij}) \text{ de rang } m. \end{cases}$$

Réciproquement, étant donné un groupe abélien de type fini G , engendré par n éléments g_1, g_2, \dots, g_n , vérifiant m relations de la forme :

$$\left\{ \begin{array}{l} \sum_{1 \leq j \leq n} a_{ij} g_j = 0, \quad 1 \leq i \leq m, \quad a_{ij} \in \mathbb{Z} \\ \text{et } A = (a_{ij}) \text{ de rang } m, \end{array} \right.$$

alors, G est isomorphe au quotient $\frac{F}{H}$ d'un groupe abélien libre de rang n , par un sous-groupe H de rang m .

Pour obtenir, à un isomorphisme près, une décomposition d'un tel groupe G , en somme directe de groupes monogènes, il suffit de transformer la matrice A au moyen de transformations élémentaires, afin de trouver une matrice de la forme A' et on applique alors la formule (25). On pourra en déduire les invariants, les diviseurs élémentaires et, si c'est nécessaire, la décomposition canonique de G , comme dans les exemples vus au paragraphe précédent.

Principe général de réduction de la matrice A :

On suppose $0 < m < n$, car, pour $m = 0$, $A = 0$, G est libre de rang n ; pour $m = n$, $\frac{F}{H} = 0$, donc $G = (0)$.

On remarque que, dans la matrice A' que l'on veut obtenir, tous les h_i sont des entiers strictement positifs. La matrice $A \in M_{m \times n}(\mathbb{Z})$, étant de rang m , quel que soit i ($1 \leq i \leq m$), les éléments a_{ij} de la i -ème ligne ne sont pas tous nuls.

Au moyen de transformations élémentaires :

— on peut se ramener à une matrice A_1 dans laquelle on a :

$$a_{11} > 0, \quad a_{11} < |a_{i1}| \quad \text{et} \quad a_{11} < |a_{1j}|, \\ \text{pour tout } i > 1 \text{ et } j > 1;$$

— en opérant successivement sur les colonnes et sur les lignes, on transforme A_1 sous la forme :

$$\begin{pmatrix} a_{11} & 0 & \dots & \dots & \dots & 0 \\ 0 & \vdots & \dots & \dots & \dots & \vdots \\ \vdots & \vdots & & & & \\ \vdots & \vdots & & & & \\ \vdots & \vdots & & & & \\ \vdots & \vdots & & & & \\ \vdots & \vdots & & & & \\ 0 & \vdots & & & & \end{pmatrix} \quad \begin{matrix} \\ \\ \\ \\ B \\ \\ \\ \end{matrix}$$

où $a_{11} > 0$ dans N et B est une matrice à $(m-1)$ lignes et $(n-1)$ colonnes sur \mathbf{Z} ;

— on répète sur B les opérations précédentes et ainsi de suite, jusqu'à ce qu'on obtienne une matrice de la forme A' .

3° Exemples :

— Soit G un groupe abélien de type fini engendré par 3 éléments x, y, z vérifiant les relations :

$$\begin{cases} 5x - 2y \times 12z = 0 \\ 3x + 4z = 0. \end{cases}$$

On a

$$A = \begin{pmatrix} 5 & -2 & 12 \\ 3 & 0 & 4 \end{pmatrix}$$

$$A \rightarrow \begin{pmatrix} 2 & 5 & 0 \\ 0 & 3 & -2 \end{pmatrix}$$

$$\text{par } (-T_2) + (T_{1,2}) + (T_3 - T_1) + (T_3 - 2T_2)$$

$$\begin{pmatrix} 2 & 5 & 0 \\ 0 & 3 & -2 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 2 & 2 \\ 0 & 3 & -2 \end{pmatrix}$$

$$\text{par } L_1 - L_2 \text{ (opération sur les lignes)}$$

$$\begin{pmatrix} 2 & 2 & 2 \\ 0 & 3 & -2 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\text{par } (T_2 - T_1) + (T_3 - T_1) + (T_2 + T_3) + (T_3 + 2T_2)$$

On en déduit que $G \simeq C_2 \oplus C_\infty$.

— Soit G engendré par 4 éléments x, y, z, t vérifiant les conditions

$$\begin{cases} 2x + 4y - 4t = 0 \\ 6x - 12z + 3t = 0 \end{cases}$$

$$A = \begin{pmatrix} 2 & 4 & 0 & -4 \\ 6 & 0 & -12 & 3 \end{pmatrix}$$

$$A \rightarrow \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{pmatrix}$$

par $(T_4 + T_2) + (T_1 - 2T_4) + (T_3 - 2T_1) + (T_3 + 4T_4) + (T_{2,4})$

d'où $G \simeq C_2 \oplus C_3 \oplus C_\infty \oplus C_\infty$.

Exercices Chapitre VIII

- 1) Démontrer la proposition (8.38).
- 2) Soit $\{G_i\}_{i \in I}$ une famille de groupes abéliens, montrer que, pour tout groupe abélien G , les ensembles $\text{Hom}(\bigoplus_{i \in I} G_i, G)$ et $\prod_{i \in I} (\text{Hom}(G_i, G))$ sont équipotents.

- 3) Soit \mathcal{P} l'ensemble des nombres premiers; pour tout $p \in \mathcal{P}$, on note $\left(\frac{\mathbb{Q}}{\mathbb{Z}}\right)_p$ la composante p -primaire du groupe abélien $\left(\frac{\mathbb{Q}}{\mathbb{Z}}, +\right)$.

a) $\left[\frac{a}{s}\right]$ désignant la classe modulo \mathbb{Z} d'un élément $\frac{a}{s}$ quelconque de \mathbb{Q} , comment s'écrivent les éléments de $\left(\frac{\mathbb{Q}}{\mathbb{Z}}\right)_p$?

b) Pour $p \in \mathcal{P}$, on note G_n le sous-groupe de $\frac{\mathbb{Q}}{\mathbb{Z}}$ engendré par $\left[\frac{1}{p^n}\right]$, où $n \in \mathbb{N}$.

Prouver que $\left(\frac{\mathbb{Q}}{\mathbb{Z}}\right)_p = \bigcup_{n \in \mathbb{N}} G_n$.

En déduire que $\left(\frac{\mathbb{Q}}{\mathbb{Z}}\right)_p \simeq C_{p^\infty}$ (groupe p -quasi-cyclique, exercice 34, chap. IV).

En conclure que $\frac{\mathbb{Q}}{\mathbb{Z}} \simeq \bigoplus_{p \in \mathcal{P}} C_{p^\infty}$.

- 4) Soit $\{G_i\}_{i \in I}$ une famille de groupes abéliens. Vérifier que :

$$T(\prod_{i \in I} G_i) \subseteq \bigoplus_{i \in I} T(G_i) \quad \text{et} \quad T(\bigoplus_{i \in I} G_i) = \bigoplus_{i \in I} T(G_i),$$

où, pour un groupe abélien G , $T(G)$ désigne le sous-groupe de torsion de G .

- 5) Etant donné un groupe abélien $(G, +)$ et un entier $n \in \mathbb{N}^*$, on dira qu'un élément $x \in G$ est *divisible par n* , s'il existe $y \in G$, tel que $x = ny$.

On dit que le groupe abélien G est un *groupe divisible* si, quels que soient $n \in \mathbb{N}^*$ et $x \in G$, x est divisible par n ; c'est-à-dire que

$$G = nG = \{nx; x \in G\}, \quad \text{quel que soit } n \in \mathbb{N}^*.$$

(Un groupe abélien multiplicatif est divisible si

$$G = G^n = \{x^n; x \in G\}, \quad \text{quel que soit } n \in \mathbb{N}^*.)$$

a) Parmi les groupes suivants, quels sont ceux qui sont divisibles? \mathbb{Z} , $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}$, \mathbb{Q} , \mathbb{R} , $\frac{\mathbb{Q}}{\mathbb{Z}}$, C_{p^∞} (groupe p -quasi-cyclique), \mathbb{C}^* (groupe multiplicatif des nombres complexes non nuls), \mathbb{R}_+ (groupe multiplicatif des nombres réels positifs).

b) Démontrer que, pour un groupe abélien $(G, +)$, les trois conditions suivantes sont équivalentes :

- (1) : G est divisible;
- (2) : $G = pG$, quel que soit le nombre premier p ;
- (3) : G a une partie génératrice S telle que, pour tout $x \in S$ et tout $n \in \mathbb{N}^*$, il existe $y \in G$, vérifiant $x = ny$.

c) Prouver que, si G est un groupe abélien divisible, alors $\frac{G}{N}$ est divisible, quel que soit $N \triangleleft G$.

d) Soit $\{G_i\}_{i \in I}$ une famille de groupes abéliens; vérifier que :

$$G = \bigoplus_{i \in I} G_i \text{ est divisible} \Leftrightarrow G_i \text{ est divisible,} \\ \text{quel que soit } i \in I.$$

e) Etant donné un groupe abélien $G \neq (0)$, montrer que :

G divisible $\Rightarrow G$ n'est pas de type fini.

- 6) Soit \mathcal{P} l'ensemble des nombres premiers et soit $G = \prod_{p \in \mathcal{P}} \mathbb{Z}_p$, où $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$.

a) $T(G)$ étant le sous-groupe de torsion de G , prouver que

$$T(G) = \bigoplus_{p \in \mathcal{P}} \mathbb{Z}_p$$

(voir exercice 4, ci-dessus).

b) Vérifier que le groupe G n'est pas divisible [on montrera qu'il n'existe aucun élément non nul de G divisible par tout $p \in \mathcal{P}$].

c) Soit $a = (a_p)_{p \in \mathcal{P}}$, où, pour tout $p \in \mathcal{P}$, a_p est non nul dans \mathbb{Z}_p .

Démontrer que, quel que soit $q \in \mathcal{P}$, il existe $x = (x_p)_{p \in \mathcal{P}}$ dans G et $y = (y_p)_{p \in \mathcal{P}}$ dans $T(G)$ tels que :

$$qx = a - y.$$

En déduire que la classe \bar{a} , de a modulo $T(G)$, est divisible par q dans $\frac{G}{T(G)}$, quel que soit $q \in \mathcal{P}$.

En tenant compte du résultat b), prouver que $T(G)$ n'est pas facteur direct dans G .

- 7) Soit G un groupe abélien tel que $\Phi(G) \neq G$ où $\Phi(G)$ est le sous-groupe de Frattini de G . On note \mathcal{P} l'ensemble des nombres premiers et \mathcal{M} l'ensemble des sous-groupes maximaux de G .

a) Montrer que, pour tout $M \in \mathcal{M}$, il existe $p \in \mathcal{P}$ tel que $[G : M] = p$.

b) Pour $p \in \mathcal{P}$, on pose $\mathcal{M}_p = \{M \in \mathcal{M}; [G : M] = p\}$.

Démontrer que $\bigcap_{M \in \mathcal{M}_p} M = pG$, où $pG = \{px; x \in G\}$.

En déduire que $\Phi(G) = \bigcap_{p \in \mathcal{P}} pG$.

En conclure que :

$$G \text{ groupe abélien divisible} \Leftrightarrow \Phi(G) = G.$$

- 8) a) Soit G un groupe abélien *sans torsion* et *divisible* (exercice 5, ci-dessus).

Prouver que G peut être muni, de façon naturelle, d'une structure d'espace vectoriel sur le corps \mathbb{Q} des nombres rationnels.

En déduire que tout groupe abélien divisible et sans torsion est isomorphe à une somme directe de copies de \mathbb{Q} . [On rappelle que tout espace vectoriel a une base [46].]

b) Montrer que tout groupe abélien p -élémentaire est isomorphe à une somme directe de copies de $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (voir exercice 21, chap. VII); en déduire qu'un tel groupe est non divisible.

c) Vérifier que le groupe additif des nombres réels \mathbb{R} est isomorphe à une somme directe de copies de \mathbb{Q} .

- 9) Soit G un groupe abélien; le but de cet exercice est de prouver que G est divisible si et seulement s'il vérifie la condition (C) suivante :

(C) : Quels que soient le groupe abélien A , le sous-groupe B de A et le morphisme $\lambda \in \text{Hom}(B, G)$, il existe $\varphi \in \text{Hom}(A, G)$ qui prolonge λ ; c'est-à-dire que si j est l'injection canonique de B dans A , le diagramme suivant commute :

$$\begin{array}{ccc} B & \xrightarrow{j} & A \\ \lambda \downarrow & \nearrow \exists \varphi & \\ G & & \end{array} \quad \varphi \circ j = \lambda.$$

a) On suppose G divisible. On considère l'ensemble \mathcal{H} des couples (H, θ) , où H est un sous-groupe de A contenant B , tel qu'il existe $\theta \in \text{Hom}(H, G)$ prolongeant λ .

Vérifier que \mathcal{H} est non vide. On munit \mathcal{H} d'une relation d'ordre telle que :

$$(H, \theta) \leq (H', \theta') \Leftrightarrow H \leq H' \text{ et } \theta'_H = \theta.$$

Démontrer (en utilisant l'axiome de Zorn (énoncé (4.60))) qu'il existe un élément maximal (H_0, θ_0) dans \mathcal{H} .

Prouver (par l'absurde) que $H_0 = A$ [si $H_0 \neq A$ et $x \in A \setminus H_0$, tel que $H_0 \cap \langle x \rangle \neq (0)$, on pose $H_1 = H_0 + \langle x \rangle$ et on note n le plus petit entier positif tel que $nx \in H_0$; on considère

$$\begin{aligned} \theta_1 : H_0 + \langle x \rangle &\rightarrow G \\ (h + rx) &\mapsto h + ry \end{aligned}$$

où $h \in H$, $r \in \mathbb{N}$, $0 \leq r < n$ et $y \in G$ est tel que $ny = \theta_0(nx)$].

b) On suppose que G vérifie la condition (C); en appliquant cette condition au cas où $A = \mathbb{Z}$ et $B = n\mathbb{Z}$, démontrer que G est divisible [on remarquera que $\varphi \in \text{Hom}(\mathbb{Z}, G)$ et $\lambda \in \text{Hom}(n\mathbb{Z}, G)$ sont respectivement déterminés par $\varphi(1)$ et $\lambda(n)$].

[Remarque : La condition (C) exprime qu'un groupe abélien divisible est un \mathbb{Z} -module *injectif* ([54], tome 2).]

- 10) Démontrer que tout sous-groupe divisible D d'un groupe abélien G est facteur direct dans G [utiliser l'exercice précédent et la proposition (8.9)].
- 11) Soient G un groupe abélien et \mathcal{D} l'ensemble des sous-groupes divisibles de G . On pose

$$d(G) = \sum_{D \in \mathcal{D}} D.$$

- a) Prouver que $d(G)$ est un sous-groupe divisible de G .
 b) Un groupe abélien G tel que $d(G) = (0)$ est dit *réduit*.
 Démontrer que $G = d(G) \oplus R$, où R est un sous-groupe réduit de G .
 c) Vérifier que, si H et K sont deux groupes abéliens, on a :

$$H \simeq K \Leftrightarrow d(H) \simeq d(K) \quad \text{et} \quad \frac{H}{d(H)} \simeq \frac{K}{d(K)}.$$

- 12) Soient H et K deux groupes abéliens divisibles p -primaires.
 On pose $H^1 = \{x \in H; px = 0\}$ et $K^1 = \{y \in K; py = 0\}$.
 Démontrer que $H \simeq K$ si et seulement si $H^1 \simeq K^1$.
 [Pour prouver que $H^1 \simeq K^1$ implique $H \simeq K$, considérer un isomorphisme $\lambda: H^1 \rightarrow K^1$, comme un morphisme de H^1 dans K , en déduire qu'il existe $\varphi \in \text{Hom}(H, K)$ tel que $\varphi|_{H^1} = \lambda$ (voir exercice 9, ci-dessus) et démontrer que φ est un isomorphisme.]

- 13) Soit H un groupe abélien *divisible et de torsion*.

Soit H_p la composante p -primaire de G .

- a) En utilisant les notations de l'exercice précédent, prouver qu'il existe un ensemble $I \neq \emptyset$ tel que

$$H_p^1 \simeq \mathbb{Z}_p^{(I)}$$

(voir exercice 8 ci-dessus).

- b) Soit $(K, +)$ un groupe abélien tel que :

$$H \simeq C_{p^\infty}^{(I)}, \quad \text{où } C_{p^\infty} \text{ est } p\text{-quasi cyclique.}$$

Démontrer que l'on a $K^1 \simeq H_p^1$; en déduire que H_p est isomorphe à une somme directe de groupes p -quasi-cycliques.

- c) Prouver que tout groupe abélien divisible, de torsion, est isomorphe à une somme directe de copies de groupes p -quasi-cycliques, p décrivant une partie de l'ensemble \mathcal{P} des nombres premiers.

- 14) Démontrer que tout groupe abélien divisible est isomorphe à une somme directe de copies de \mathbb{Q} et de copies de C_{p^∞} , p décrivant une partie de l'ensemble des nombres premiers.

[Utiliser les exercices 8 et 13 ci-dessus.]

- 15) Soit G un groupe de type fini, de torsion et résoluble; démontrer que G est un groupe fini [raisonner par récurrence sur n , où n est le plus petit entier tel que $D_n(G) = \{e\}$].

- 16) Soit G un groupe abélien, tel que $G \simeq \frac{F_{(X)}}{K}$ où $F_{(X)}$ est un groupe abélien libre sur $X = \{x_i\}_{i \in I}$.

a) Vérifier que $F_{(X)}$ est isomorphe à un sous-groupe de $\mathbb{Q}^{(I)}$, où \mathbb{Q} est le groupe des nombres rationnels.

En déduire que *tout groupe abélien G est isomorphe à un sous-groupe d'un groupe divisible.*

b) Prouver qu'un groupe abélien est divisible si et seulement s'il est facteur direct de tout groupe qui le contient.

- 17) Soient deux groupes divisibles G_1 et G_2 ; d'après l'exercice 14 ci-dessus, on peut écrire : $G_1 = T_1 \oplus H_1$, $G_2 = T_2 \oplus H_2$, où H_1 et H_2 sont des espaces vectoriels sur \mathbb{Q} et T_1 , T_2 sont des sommes directes de groupes p -quasi-cycliques (pour différentes valeurs de p).

Si, pour tout nombre premier p , on pose

$$T_1^1(p) = \{x \in T_1; px = 0\} \quad \text{et} \quad T_2^1(p) = \{x \in T_2; px = 0\},$$

démontrer que G_1 est isomorphe à G_2 , si et seulement si $\dim_{\mathbb{Q}}(H_1) = \dim_{\mathbb{Q}}(H_2)$ et, pour tout nombre premier p ,

$$\dim_{\mathbb{Z}_p}(T_1^1(p)) = \dim_{\mathbb{Z}_p}(T_2^1(p))$$

(voir exercice 12 ci-dessus).

- 18) Soit U le groupe circulaire, $U = \{z \in \mathbb{C}^*; |z| = 1\}$ et soit $\Gamma_\infty = \{z \in \mathbb{C}^*; n \in \mathbb{N}, z^n = 1\}$.

\mathcal{P} désignant l'ensemble des nombres premiers, on pose $G = \prod_{p \in \mathcal{P}} C_{p^\infty}$, où C_{p^∞} est p -quasi-cyclique.

a) Comparer les groupes Γ_∞ et $\bigoplus_{p \in \mathcal{P}} C_{p^\infty}$.

Les groupes U , Γ_∞ et G sont-ils divisibles? (Voir exercices 11 et 12, chap. IV et exercice 3 ci-dessus.)

b) Quels sont les sous-groupes de torsion de U et de G ?

Prouver que les groupes U et $\prod_{p \in \mathcal{P}} C_{p^\infty}$ sont isomorphes.

19) Soit G un groupe abélien de type fini.

a) Démontrer que le groupe $\text{Aut}(G)$ est fini si et seulement s'il existe, au plus, un facteur isomorphe à \mathbb{Z} , dans la décomposition canonique de G .

b) Montrer que, dans tous les cas, $\text{Aut}(G)$ est dénombrable.

20) Soit G un groupe abélien fini d'ordre n .

Démontrer que, pour tout diviseur d de n , il existe au moins un sous-groupe H de G qui est d'ordre d (réciproque du théorème de Lagrange pour les groupes abéliens).

21) Soit F un groupe abélien libre de base $\{x_1, x_2, x_3\}$.

Soit H le sous-groupe de F engendré par

$$y_1 = 3x_1 + x_2 + x_3, \quad y_2 = x_1 + 3x_2 + x_3, \quad y_3 = x_1 + x_2 + 3x_3.$$

Déterminer une base $\{u_1, u_2, u_3\}$ de F telle qu'il existe une base de H de la forme $\{h_1 u_1, h_2 u_2, h_3 u_3\}$, où h_1, h_2, h_3 sont des entiers positifs vérifiant $h_i \mid h_{i+1}$ ($1 \leq i \leq 2$).

22) a) Trouver les invariants et la décomposition canonique du groupe abélien fini dont les diviseurs élémentaires sont :

$$2, 2, 3^3, 3, 5^2, 5.$$

b) Trouver les diviseurs élémentaires, les invariants et la décomposition canonique du groupe

$$G = C_{20} \oplus C_6 \oplus C_{15}.$$

23) Trouver les diviseurs élémentaires, les invariants et la décomposition canonique des groupes abéliens suivants :

G_1 , engendré par x et y tels que $10x = 9y = 0$.

G_2 , engendré par x, y, z tels que $15x = 6y = 4z = 0$.

G_3 , engendré par x, y, z tels que

$$\begin{cases} 2x - y - 3z = 0 \\ 3x - 2y - 3z = 0 \end{cases}$$

G_4 , engendré par x, y, z tels que

$$\begin{cases} 2x - y - 3z = 0 \\ 3x - 2y - 3z = 0 \\ 7x + 4y + 10z = 0. \end{cases}$$

CHAPITRE IX

Groupes libres *Générateurs et relations* *Produit libre de groupes*

Dans le chapitre VIII, nous avons défini la notion de groupe abélien libre sur un ensemble X et la propriété universelle d'un tel groupe $F_{(X)}$ (théorème (8.24)) nous a permis de montrer que tout groupe abélien engendré par un ensemble X est isomorphe à un quotient de $F_{(X)}$.

Nous allons maintenant montrer que, plus généralement, on peut construire, à partir d'un ensemble donné X , un groupe, dit *libre sur X* (non abélien, si $\text{card}(X) > 1$), satisfaisant à une propriété universelle qui permet de prouver que tout groupe engendré par X est image homomorphe d'un groupe libre sur X .

1 — Groupe libre

A / Construction d'un groupe libre

Soit X un ensemble non vide; I étant un ensemble de même cardinal que X , posons

$$X = \{x_i\}_{i \in I}.$$

Considérons un ensemble disjoint de X et équipotent à X que nous noterons X^{-1} et dont nous écrirons les éléments sous la forme x_i^{-1} , pour $i \in I$ (« x_i^{-1} » est ici, seulement, une *notation*, qui sera commode par la suite).

Définition (9.1) : On appelle *mot sur* $X \cup X^{-1}$ toute suite finie (ou ensemble fini ordonné) de n éléments de $X \cup X^{-1}$ ($n \in \mathbb{N}$) plusieurs éléments de cet ensemble pouvant être égaux; n s'appelle la *longueur du mot*.

Par convention, il n'existe qu'un seul mot de longueur 0, que l'on notera 1; on l'appelle le *mot vide*, car il correspond à la partie vide de $X \cup X^{-1}$.

Un mot de longueur $n > 0$ s'écrit sous la forme :

$$x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_n}^{\varepsilon_n}, \quad \text{où } \varepsilon_j = \pm 1, \quad \text{pour tout } j \ (1 \leq j \leq n);$$

c'est-à-dire :

$$\begin{aligned} \varepsilon_j &= 1, & \text{si } x_{i_j}^{\varepsilon_j} &\in X \\ \varepsilon_j &= -1, & \text{si } x_{i_j}^{\varepsilon_j} &\in X^{-1}. \end{aligned}$$

On désignera par $(X \cup X^{-1})$ l'ensemble des mots sur $X \cup X^{-1}$.

Exemple (9.2) : Si $X = \{x, y\}$, $x, yy^{-1}, x^{-1}yyxy, x^{-1}xx^{-1}, 1$ sont des mots sur $X \cup X^{-1}$.

Egalité de deux mots : D'une façon générale, dans $(X \cup X^{-1})$, on a :

$$x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_n}^{\varepsilon_n} = x_{j_1}^{\delta_1} x_{j_2}^{\delta_2} \dots x_{j_p}^{\delta_p} \Leftrightarrow \begin{cases} n = p \\ x_{i_k}^{\varepsilon_k} = x_{j_k}^{\delta_k}, \quad \forall k \ (1 \leq k \leq n). \end{cases}$$

Dans l'exemple (9.2), tous les mots considérés sont distincts.

Notion de produit de mots :

— Quel que soit $w \in (X \cup X^{-1})$, on pose

$$1w = w1 = w \tag{1}$$

— Etant donné deux mots de longueurs non nulles dans $(X \cup X^{-1})$:

$$u = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}, \quad v = x_{j_1}^{\delta_1} \dots x_{j_p}^{\delta_p},$$

par définition, le produit uv est le mot :

$$x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n} x_{j_1}^{\delta_1} \dots x_{j_p}^{\delta_p} \tag{2}$$

$$\text{donc } \text{long}(uv) = \text{long}(u) + \text{long}(v) \tag{3}$$

Remarques (9.3) :

1° Un mot de longueur 1 est un élément de $X \cup X^{-1}$; tout mot de longueur $n > 0$ est donc produit de n mots de longueur 1.

2° Le produit de mots défini dans $(X \cup X^{-1})$ par les relations (1) et (2) est associatif et 1 est élément unité; mais $(X \cup X^{-1})$ n'est pas un groupe, relativement à ce produit, car, 1 étant de longueur 0, la relation (3) montre qu'aucun mot de longueur $n > 0$ ne peut avoir d'inverse.

$(X \cup X^{-1})$ muni du produit de mots défini par (1) et (2) est donc un monoïde (voir le chap. I, remarque (1.9)), qu'on appelle *monoïde libre sur $X \cup X^{-1}$* .

L'objet de ce qui suit est de définir dans le monoïde $(X \cup X^{-1})$ une relation d'équivalence \mathcal{R} , compatible avec le produit des mots et telle que le quotient de $(X \cup X^{-1})$ par \mathcal{R} soit un groupe.

Définition (9.4) : Dans $(X \cup X^{-1})$, deux mots u et v seront dits *adjacents* s'il existe deux mots t_1 et t_2 dans $(X \cup X^{-1})$ et un élément $a \in X \cup X^{-1}$ tels que :

$$u = t_1 t_2 \quad \text{et} \quad v = t_1 a a^{-1} t_2,$$

$$\text{ou} \quad u = t_1 a a^{-1} t_2 \quad \text{et} \quad v = t_1 t_2 \quad (4)$$

avec la convention : $(a^{-1})^{-1} = a$, quel que soit $a \in X \cup X^{-1}$.

On écrira $u \mathcal{A} v$ pour exprimer que u est adjacent à v .

Exemple (9.5) : Si $X = \{x, y\}$, alors :

$$x^{-1} x y y^{-1} \mathcal{A} y y^{-1} \quad (\text{on prend } t_1 = 1, t_2 = y y^{-1} \text{ et } a = x^{-1})$$

de même,

$$x^{-1} x y y^{-1} \mathcal{A} x^{-1} x \quad (\text{on prend } t_1 = x^{-1} x, t_2 = 1 \text{ et } a = y)$$

$$\text{et} \quad x^{-1} x x^{-1} \mathcal{A} x^{-1} \quad (\text{on prend } t_1 = 1, t_2 = x^{-1} \text{ et } a = x^{-1}).$$

Remarque (9.6) : Quels que soient u et v dans $(X \cup X^{-1})$,

$$u \mathcal{A} v \Rightarrow v \mathcal{A} u.$$

Considérons alors dans $(X \cup X^{-1})$ la relation binaire \mathcal{R} telle que $u \mathcal{R} v$, s'il existe t_1, t_2, \dots, t_n dans $(X \cup X^{-1})$, $n \geq 1$ dans N , vérifiant les conditions :

$$u = t_1, \quad v = t_n \quad \text{et} \quad t_i \mathcal{A} t_{i+1}, \\ \forall i \ (1 \leq i \leq n-1), \text{ si } n > 1 \quad (5)$$

Le cas $n = 2$ montre que $u \mathcal{A} v \Rightarrow u \mathcal{R} v$.

PROPOSITION (9.7). *La relation binaire \mathcal{R} , définie ci-dessus, est une relation d'équivalence dans le monoïde $(X \cup X^{-1})$, compatible avec le produit des mots et telle que le quotient de $(X \cup X^{-1})$ par \mathcal{R} est un groupe.*

Preuve :

1° Quel que soit $u \in (X \cup X^{-1})$ on a $u \mathcal{R} u$ (cas $n = 1$ dans la définition de \mathcal{R}), donc \mathcal{R} est réflexive.

D'autre part, la relation \mathcal{A} étant symétrique dans $(X \cup X^{-1})$, les conditions (5) impliquent que \mathcal{R} est symétrique.

Supposons $u \mathcal{R} v$ et $v \mathcal{R} w$:

— il existe t_1, t_2, \dots, t_n dans $(X \cup X^{-1})$ tels que

$$u = t_1, \quad v = t_n \quad \text{et} \quad t_i \mathcal{A} t_{i+1}, \\ \text{quel que soit } i \ (1 \leq i \leq n-1)$$

— et il existe $t_n, t_{n+1}, \dots, t_{n+m}$ dans $(X \cup X^{-1})$ tels que

$$v = t_n, \quad w = t_{n+m} \quad \text{et} \quad t_{n+j} \mathcal{A} t_{n+j+1}, \\ \text{quel que soit } j \ (0 \leq j \leq m-1).$$

On en déduit que $u \mathcal{R} w$, donc \mathcal{R} est transitive.

Si $u \mathcal{R} v$ dans $(X \cup X^{-1})$, on dira que u et v sont équivalents.

2° Démontrons que \mathcal{R} est compatible avec le produit des mots, défini dans $(X \cup X^{-1})$ par les relations (1) et (2). D'après la proposition (2.20), il suffit de prouver que \mathcal{R} est compatible à droite et à gauche avec le produit des mots.

Supposons $u \mathcal{R} u'$ et soit $v \in (X \cup X^{-1})$. Soit $t \in (X \cup X^{-1})$ tel que $u \mathcal{A} t$, vérifions que $uv \mathcal{A} tv$.

Supposons $u = z_1 z_2$ et $t = z_1 a a^{-1} z_2$, avec z_1, z_2 dans $(X \cup X^{-1})$ et $a \in X \cup X^{-1}$; alors :

$$uv = z_1 z_2 v \quad \text{et} \quad tv = z_1 a a^{-1} z_2 v,$$

d'où $uv \mathcal{A} tv$.

Or, $u \mathcal{R} u'$ implique qu'il existe $t_1, t_2, \dots, t_n, n \geq 1$ dans N , tels que

$$u = t_1, \quad t_1 \mathcal{A} t_2, \dots, t_{n-1} \mathcal{A} t_n, \quad t_n = u';$$

d'où $uv = t_1 v, \quad t_1 v \mathcal{A} t_2 v, \dots, t_{n-1} v \mathcal{A} t_n v, \quad t_n v = u' v$,

par suite, $uv \mathcal{R} u' v$; \mathcal{R} est donc compatible à droite avec le produit des mots.

De façon analogue, on vérifie que \mathcal{R} est compatible à gauche avec le produit des mots.

3° Désignons par $[X \cup X^{-1}]$ l'ensemble quotient de $(X \cup X^{-1})$ par la relation d'équivalence \mathcal{R} et notons $[u]$ la classe modulo \mathcal{R} d'un mot $u \in (X \cup X^{-1})$. \mathcal{R} étant compatible avec la loi de composition du monoïde $(X \cup X^{-1})$, d'après la proposition (2.21) et la remarque (2.22) 2°, on peut définir, dans $[X \cup X^{-1}]$, un produit tel que, quels que soient $[u]$ et $[v]$:

$$[u] [v] = [uv] \tag{6}$$

et, relativement à cette loi de composition, $[X \cup X^{-1}]$ est un monoïde, dont $[1]$ est l'élément unité; montrons alors que tout élément $[u]$ est inversible dans $[X \cup X^{-1}]$.

Considérons le cas où $u = x$ avec $x \in X \cup X^{-1}$ et vérifions que :

$$xx^{-1} \mathcal{R} 1.$$

On a en effet les conditions (5), en prenant $u = xx^{-1} = t_1$ et $v = 1 = t_2$, puisque $u = 1 xx^{-1} 1$ implique $xx^{-1} \mathcal{A} 1$.

On vérifierait de même que $x^{-1} x \mathcal{R} 1$; par suite, dans le monoïde $[X \cup X^{-1}]$, quel que soit $x \in X \cup X^{-1}$, $[x]$ est inversible et :

$$[x]^{-1} = [x^{-1}] \tag{7}$$

L'application $\theta : (X \cup X^{-1}) \rightarrow [X \cup X^{-1}]$ vérifie, d'après (6) :

$$u \mapsto [u]$$

$\theta(uv) = \theta(u) \theta(v)$, quels que soient u, v dans $(X \cup X^{-1})$.

Par suite, compte tenu de (7), pour tout $u \in (X \cup X^{-1})$ tel que :

$$u = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_n}^{\varepsilon_n}, \quad \text{où } x_{i_j} \in X \cup X^{-1} \text{ et } \varepsilon_j = \pm 1,$$

$[u]$ est inversible dans $[X \cup X^{-1}]$ et $[u]^{-1} = [x_{i_n}^{-\varepsilon_n} x_{i_{n-1}}^{-\varepsilon_{n-1}} \dots x_{i_1}^{-\varepsilon_1}]$.

On en conclut que $[X \cup X^{-1}]$ est un groupe, relativement à la loi de composition définie par (6).

Définition (9.8) : On dira qu'un groupe est *libre sur un ensemble* X , s'il est engendré par X et isomorphe au groupe $[X \cup X^{-1}]$ défini ci-dessus.

En particulier, tout groupe réduit à un seul élément est libre sur l'ensemble vide.

Définition (9.9) : On dit qu'un mot $u \in (X \cup X^{-1})$ est *réduit*, si $u = 1$, ou si $u = a_1 a_2 \dots a_n$, avec $a_i \in X \cup X^{-1}$ pour $1 \leq i \leq n$ et

$$a_{i+1} \neq a_i^{-1}, \quad \text{quel que soit } i \quad (1 \leq i \leq n-1).$$

Exemples (9.10) :

1° Tout mot de longueur 1 est réduit.

2° Si $X = \{x, y\}$, $xxxyx^{-1}$, $x^{-1}yxyy$ sont des mots réduits; par contre, $xyx^{-1}x$, $yxyy^{-1}x^{-1}$ sont non réduits.

THÉORÈME (9.11). *Chaque classe d'équivalence de $(X \cup X^{-1})$ modulo \mathcal{R} contient un mot réduit et un seul.*

Preuve :

1° On peut montrer sans difficulté que, étant donné un mot non réduit $u \neq 1$, il existe $t \in (X \cup X^{-1})$ tel que

$$u \mathcal{A} t \quad \text{et} \quad \text{long}(t) < \text{long}(u).$$

La longueur d'un mot étant un entier positif ou nul, on prouve alors, en raisonnant de proche en proche, qu'il existe nécessairement un mot réduit r équivalent à u ; on en déduit que toute classe d'équivalence modulo \mathcal{R} , dans $(X \cup X^{-1})$, contient un mot réduit. En vue de prouver que chaque classe $[u]$ ne contient qu'un seul mot réduit, nous allons définir une méthode particulière pour obtenir un mot réduit, équivalent à un mot donné u .

Soit $u \in (X \cup X^{-1})$ tel que

$$u = a_1 a_2 \dots a_n, \quad a_i \in X \cup X^{-1}, \quad \forall i (1 \leq i \leq n),$$

l'élément a_n de $X \cup X^{-1}$ sera appelé le « dernier terme » de u .

Associons au mot u la suite de mots u_0, u_1, \dots, u_n définie comme suit :

$$\begin{aligned} u_0 &= 1; & u_1 &= a_1; \\ u_2 &= a_1 a_2 & \text{si } a_1 \neq a_2^{-1}; & & u_2 &= 1, & \text{si } a_1 = a_2^{-1}. \end{aligned}$$

D'une façon générale, u_i étant déterminé, on pose :

$$u_{i+1} = u_i a_{i+1},$$

si le dernier terme de u_i est différent de a_{i+1}^{-1} .

Si le dernier terme de u_i est a_{i+1}^{-1} , on a $u_i = t a_{i+1}^{-1}$ où t est un mot bien déterminé (car $t a_{i+1}^{-1} = t' a_{i+1}^{-1}$ implique $t = t'$, compte tenu de la définition des mots), on pose alors, dans ce cas : $u_{i+1} = t$.

La suite u_0, u_1, \dots, u_n est parfaitement définie à partir de u par le procédé ci-dessus (si $u = 1$, la suite est réduite à $u_0 = 1$).

La définition des u_i implique que chaque u_i est réduit, en particulier u_n est réduit.

D'autre part, on vérifie facilement que, pour tout i ($0 \leq i \leq n$), u_i est équivalent à $a_1 a_2 \dots a_i$; en particulier, u_n est équivalent à u .

La construction de la suite u_0, \dots, u_n montre que, si u est réduit, alors $u_n = u$.

u_n sera appelé : la « forme réduite » de u et sera noté $r(u)$.

2° Démontrons maintenant que, si u et v sont deux mots adjacents, alors leurs formes réduites sont identiques.

Si $u \not\sim v$ dans $(X \cup X^{-1})$, on peut supposer, sans restreindre la généralité :

$$\left. \begin{aligned} u &= a_1 a_2 \dots a_k a_{k+1} \dots a_n \\ v &= a_1 a_2 \dots a_k x x^{-1} a_{k+1} \dots a_n \end{aligned} \right\} \quad (8)$$

avec $a_i \in X \cup X^{-1}$ pour tout i ($1 \leq i \leq n$) et $x \in X \cup X^{-1}$.

Soient u_0, u_1, \dots, u_n et v_0, v_1, \dots, v_{n+2} les suites de mots respectivement associées à u et v , par la méthode exposée plus haut.

Compte tenu des relations (8) et de la détermination des u_i et des v_j , on a

$$u_0 = v_0, \quad u_1 = v_1 \dots, u_k = v_k.$$

Montrons que $u_k = v_{k+2}$.

1^{er} cas : Le dernier terme de u_k est différent de x^{-1} , alors

$$v_k = u_k, \quad v_{k+1} = v_k x \quad \text{et} \quad v_{k+2} = v_k = u_k.$$

2^e cas : Le dernier terme de u_k est x^{-1} ; écrivons $u_k = tx^{-1}$. u_k étant réduit, le dernier terme de t est différent de x , donc $v_k = u_k$, $v_{k+1} = t$ et $v_{k+2} = tx^{-1} = u_k$.

Les relations (8) impliquent alors :

$$u_{k+i} = v_{k+2+i}, \quad \text{pour tout } i \ (0 \leq i \leq n-k);$$

en particulier $u_n = v_{n+2}$, c'est-à-dire $r(u) = r(v)$.

3^o Montrons que deux mots réduits et équivalents, u et v , sont égaux.

u et v étant équivalents, il existe des mots t_1, t_2, \dots, t_n tels que :

$$u = t_1, \quad v = t_n \quad \text{et} \quad t_i \mathcal{A} t_{i+1}, \quad (9)$$

quel que soit $i \ (1 \leq i \leq n-1)$.

En considérant la forme réduite de chaque t_i et en appliquant le résultat précédent, on obtient : $u = r(t_1) = r(t_2) = \dots = r(t_n) = v$.

Ce qui achève la démonstration du théorème (9.11).

Remarque (9.12) : Désignons par F_X l'ensemble des mots réduits de $(X \cup X^{-1})$. D'après le théorème (9.11), F_X est un ensemble de représentants des classes d'équivalences distinctes $[u] \in [X \cup X^{-1}]$.

La bijection qui à chaque classe $[u]$ associe l'unique mot réduit qu'elle contient, $r(u)$, permet de définir dans F_X une loi de composition induite par (6) :

$$\begin{aligned} F_X \times F_X &\rightarrow F_X \\ (u, v) &\mapsto r(uv) \end{aligned} \quad (10)$$

telle que F_X est un groupe engendré par X et isomorphe au groupe $[X \cup X^{-1}]$; donc F_X est un groupe libre sur X (définition (9.8)).

De plus, compte tenu de la notion de mot réduit et de la définition de l'égalité de deux mots dans $(X \cup X^{-1})$, tout élément $u \in F_X$ s'écrit de façon unique sous la forme :

$$\left. \begin{aligned} u &= x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}, \text{ tel que : } n \in \mathbb{N} \text{ et pour } \\ n &= 0, u = 1; \text{ pour } n > 0, x_j^{\epsilon_j} \in X \cup X^{-1}, \\ &\text{avec } x_{j+1}^{\epsilon_{j+1}} \neq x_j^{-\epsilon_j}, \forall j (1 \leq j \leq n-1) \end{aligned} \right\} \quad (11)$$

On traduit cette propriété, en disant que le groupe F_X est librement engendré par X , ou que $X = \{x_i\}_{i \in I}$ est une famille génératrice libre de F_X .

Définition (9.13) : On dira qu'un groupe est libre s'il possède une famille génératrice libre, c'est-à-dire vérifiant les conditions (11) ci-dessus; si cette famille génératrice libre est finie, le groupe sera dit *libre de type fini*.

Remarques (9.14) :

1° Tout groupe isomorphe à un groupe libre est libre; en effet, si θ est un isomorphisme du groupe libre F_X sur un groupe F , alors F est librement engendré par $\theta(X)$. En particulier, le groupe $[X \cup X^{-1}]$ est librement engendré par $\{[x_i]; x_i \in X\}$.

2° Si $X = \{x\}$, alors F_X est le groupe monogène infini engendré par x ; par suite, tout groupe libre sur un ensemble de cardinal 1 est isomorphe à \mathbb{Z} .

3° Un groupe libre sur un ensemble X est *non abélien*, si $\text{card}(X) > 1$.

En effet, quels que soient x et y dans $X \cup X^{-1}$, tels que $x \neq y$, $x^{-1}y^{-1}xy$ est un mot réduit différent de 1, d'où $xy \neq yx$ dans le groupe libre F_X .

4° Tout groupe libre sur un ensemble X , non vide, est *sans torsion*.

Considérons $u \neq 1$ dans F_X et vérifions qu'il est d'ordre infini. u est un mot réduit dans $(X \cup X^{-1})$; supposons

$$u = a_1 a_2 \dots a_n, \text{ où } a_i \in X \cup X^{-1} \text{ pour tout } i (1 \leq i \leq n).$$

$u = r(u)$ implique qu'il existe nécessairement un plus petit entier j ($0 \leq j < n$) tel que $a_{j+1} \neq a_n^{-1} a_j$, c'est-à-dire que u s'écrit sous la forme

$$u = a_1 a_2 \dots a_j b_1 b_2 \dots b_r a_j^{-1} a_{j-1}^{-1} \dots a_1^{-1} \quad (12)$$

avec $0 \leq j \leq n-1$, $1 \leq r \leq n$, $2j+r=n$, $a_1 a_2 \dots a_j$ et $b_1 b_2 \dots b_r$ étant des mots réduits et $b_1 \neq b_r^{-1}$.

On en déduit que, pour tout $k \in \mathbb{N}^*$,

$$u^k = a_1 a_2 \dots a_j (b_1 b_2 \dots b_r)^k a_j^{-1} a_{j-1}^{-1} \dots a_1^{-1};$$

alors u^k est un mot réduit et $\text{long}(u^k) = 2j + kr$ implique $u^k \neq 1$.

B / Propriété universelle d'un groupe libre

THÉORÈME (9.15). (Propriété universelle.) Soit un groupe $F \neq (e)$; soient X une partie génératrice de F et α l'injection canonique de X dans F ; alors F est libre sur X si et seulement si, quels que soient le groupe G et l'application $\sigma : X \rightarrow G$, il existe un unique morphisme $\varphi \in \text{Hom}(F, G)$ tel que

$$\varphi \circ \alpha = \sigma.$$

Preuve :

1° Supposons $F = F_X$; α_X désignant l'injection canonique de X dans F_X , démontrons que le couple (F_X, α_X) vérifie la propriété énoncée.

Dans le diagramme :

$$\begin{array}{ccc} X & \xrightarrow{\alpha_X} & F_X \\ \sigma \downarrow & \searrow \exists! \varphi & \\ G & & \end{array} \quad (13)$$

où G et σ sont donnés, définissons $\varphi : F_X \rightarrow G$ en posant, pour tout $u \in F_X$, écrit sous la forme (11) :

$$\varphi(u) = (\sigma(x_{i_1}))^{e_1} (\sigma(x_{i_2}))^{e_2} \dots (\sigma(x_{i_n}))^{e_n}$$

et $\varphi(1) = e$,

où e est l'élément neutre de G .

On définit ainsi un *morphisme* $\varphi \in \text{Hom}(F_X, G)$ tel que $\varphi(x) = \sigma(x)$, quel que soit $x \in X$, donc $\varphi \circ \alpha_X = \sigma$.

De plus, si $\varphi' \in \text{Hom}(F_X, G)$ et $\varphi' \circ \alpha_X = \sigma$, alors pour tout $u \in F_X$, on a $\varphi'(u) = \varphi(u)$, d'où l'unicité de φ .

2° Réciproquement, considérons un groupe F engendré par une partie non vide X , telle que, si α est l'injection canonique de X dans F , le couple (F, α) vérifie les conditions énoncées dans le théorème.

Compte tenu de l'hypothèse et du résultat précédent, il existe $\varphi \in \text{Hom}(F, F_X)$ et $\psi \in \text{Hom}(F_X, F)$ tels que les diagrammes suivants commutent :

$$\begin{array}{ccc}
 X & \xrightarrow{\alpha} & F \\
 \alpha_X \downarrow & \swarrow \exists! \varphi & \\
 F_X & &
 \end{array}
 \quad
 \begin{array}{ccc}
 X & \xrightarrow{\alpha_X} & F_X \\
 \alpha \downarrow & \swarrow \exists! \psi & \\
 F & &
 \end{array}$$

$\varphi \circ \alpha = \alpha_X$ et $\psi \circ \alpha_X = \alpha$

On en déduit que $\psi \circ \varphi \circ \alpha = \alpha$ et $\varphi \circ \psi \circ \alpha_X = \alpha_X$, d'où

$$\psi \circ \varphi_X = \text{id}_X \quad \text{et} \quad \varphi \circ \psi_X = \text{id}_X$$

φ et ψ sont des morphismes de groupes, F et F_X sont engendrés par X , par suite

$$\psi \circ \varphi = \text{id}_F \quad \text{et} \quad \varphi \circ \psi = \text{id}_{F_X},$$

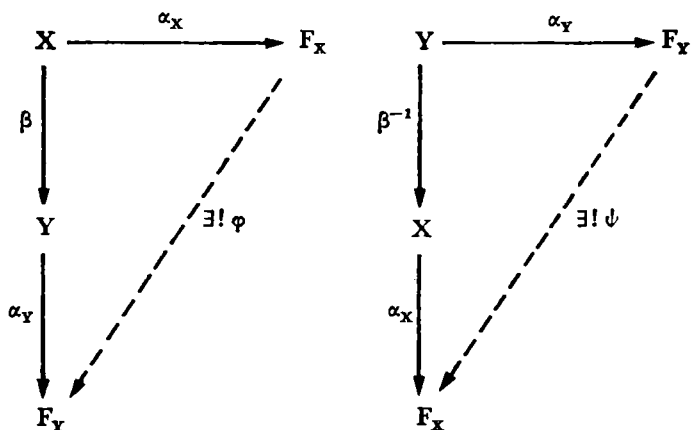
d'où $F \simeq F_X$ et $\psi(X) = X$ implique F libre sur X .

COROLLAIRE (9.16). *Soient deux ensembles X et Y alors :*

$$X \text{ équipotent à } Y \Rightarrow F_X \simeq F_Y.$$

Preuve : La propriété étant vraie pour $X = Y = \emptyset$, on suppose X et Y non vides. Soit β une bijection de X sur Y .

Considérons les diagrammes :



D'après le théorème (9.15), il existe un unique $\varphi \in \text{Hom}(F_X, F_Y)$ et un unique $\psi \in \text{Hom}(F_Y, F_X)$ tels que :

$$\varphi \circ \alpha_X = \alpha_Y \circ \beta \quad \text{et} \quad \psi \circ \alpha_Y = \alpha_X \circ \beta^{-1};$$

par suite,

$$\psi \circ \varphi \circ \alpha_X = \alpha_X \quad \text{et} \quad \varphi \circ \psi \circ \alpha_Y = \alpha_Y.$$

On en déduit que $\psi \circ \varphi = \text{id}_{F_X}$ et $\varphi \circ \psi = \text{id}_{F_Y}$, d'où $F_X \simeq F_Y$.

Remarque (9.17) : Nous verrons plus loin (théorème (9.23)) que, réciproquement, $F_X \simeq F_Y$ implique X et Y équipotents.

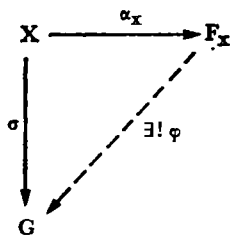
THÉORÈME (9.18). *Tout groupe est image homomorphe d'un groupe libre. En particulier, tout groupe de type fini est image homomorphe d'un groupe libre de type fini.*

Preuve : Soit G un groupe quelconque.

— Si $G = e$, alors G est libre sur l'ensemble vide.

— Supposons $G \neq e$; soit X une partie génératrice de G , notons σ l'injection canonique : $X \rightarrow G$.

Considérons le groupe libre F_X et α_X l'injection canonique de X dans F_X . D'après le théorème (9.15), il existe $\varphi \in \text{Hom}(F_X, G)$ tel que $\varphi \circ \alpha_X = \sigma$.



$\varphi \circ \alpha_X = \sigma$ implique φ surjectif, d'où $G \simeq \frac{F_X}{\text{Ker } \varphi}$, donc G est image homomorphe du groupe libre F_X .

Si G est de type fini, on choisit X fini, donc, dans ce cas, F_X est libre de type fini.

2 — Générateurs et relations

A / Présentation

Remarque (9.19) : Etant donné un groupe G et une famille génératrice $\{x_i\}_{i \in I}$ de G , en général, les générateurs x_i , $i \in I$, sont liés par certaines relations.

Exemples : Si $G = \langle x \rangle$ est cyclique d'ordre n , le générateur x de G vérifie la relation $x^n = e$.

— Si $G = \langle a, b \rangle$ est le groupe diédral D_n , $n \geq 2$, alors G est engendré par a et b tels que :

$$a^n = e, \quad b^2 = e, \quad (ab)^2 = e \quad (\text{voir chap. III}).$$

D'une façon générale, si G est engendré par $X = \{x_i\}_{i \in I}$, toute relation liant les générateurs x_i , $i \in I$, peut s'écrire sous la forme $r = e$, où r peut être considéré comme un élément du groupe libre F_X .

D'autre part, si S est une partie de F_X , notons (S) le sous-groupe normal de F_X engendré par S , c'est-à-dire l'intersection de tous les sous-groupes normaux de F_X contenant S .

Si $S = \emptyset$, $(S) = (1)$.

Définition (9.20) : Soit G un groupe engendré par un ensemble $X = \{x_i\}_{i \in I}$ vérifiant un ensemble de relations $\{r_\lambda = e; \lambda \in \Lambda\}$. (R) étant le sous-groupe normal du groupe libre F_X , engendré par $R = \{r_\lambda\}_{\lambda \in \Lambda}$, on dit que $(X | R)$ est une *présentation* de G , si G est isomorphe au groupe $\frac{F_X}{(R)}$.

Lorsque R est fini, on dit que G est de *présentation finie*.

Exemples (9.21) : On peut vérifier que :

- 1° pour $n \in \mathbb{N}^*$, $(x | x^n)$ est une présentation du groupe cyclique d'ordre n engendré par x ;
- 2° $(\{a, b\} | a^n, b^2, abab)$, avec $a \neq b$ et $n \geq 2$ dans \mathbb{N} , est une présentation du groupe diédral D_n ;
- 3° $(\{a, b\} | a^4, a^2 b^{-2}, ab^{-1} ab)$, avec $a \neq b$, est une présentation du groupe des quaternions Q_8 ;
- 4° quel que soit l'ensemble X , $F_X = \frac{F_X}{(1)}$, donc $(X | \emptyset)$ est une présentation de F_X , c'est-à-dire que F_X est un groupe engendré par $X = \{x_i\}_{i \in I}$, tel que les x_i ne vérifient aucune relation.

PROPOSITION (9.22). Soit X un ensemble non vide. Si G est un groupe de présentation $(X | [x, y]; (x, y) \in X \times X)$, alors G est isomorphe à $\frac{F_X}{D(F_X)}$ et G est un groupe abélien libre sur X .

Preuve : Posons $R = \{[x, y]; (x, y) \in X \times X\}$.

(R) étant le sous-groupe normal du groupe libre F_X , engendré par R , on a

$$(R) \subseteq D(F_X),$$

puisque le groupe dérivé de F_X est engendré par l'ensemble des commutateurs de F_X .

Or, d'après la définition (9.20), on a $G \simeq \frac{F_X}{(R)}$ et la présentation de G implique que G est abélien, d'où (théorème (4.39)) : $D(F_X) \subseteq (R)$.

On en déduit que $(R) = D(F_X)$, donc :

$$G \simeq \frac{F_X}{D(F_X)}.$$

Soit $F_{(X)}$ le groupe *abélien libre* de base X (définition (8.11));
démontrons que les groupes $F_{(X)}$ et $\frac{F_X}{D(F_X)}$ sont isomorphes.

Considérons le diagramme suivant :

$$\begin{array}{ccccc}
 X & \xrightarrow{\alpha_X} & F_{(X)} & \xrightarrow{\pi} & \frac{F_X}{D(F_X)} \\
 \downarrow j_X & & \nearrow \exists! \varphi & & \nearrow \exists! \lambda \\
 & & F_X & &
 \end{array} \quad (14)$$

dans lequel α_X et j_X sont les injections canoniques et π est l'épimorphisme canonique.

La propriété universelle du groupe libre F_X (théorème (9.15)) implique qu'il existe $\varphi \in \text{Hom}(F_X, F_{(X)})$ tel que

$$\varphi \circ \alpha_X = j_X \quad (15)$$

Le groupe $F_{(X)}$ étant abélien, on a $D(F_X) \subseteq \text{Ker } \varphi$.

Par suite, d'après la propriété universelle du groupe quotient (théorème (4.25)), il existe $\lambda \in \text{Hom}\left(\frac{F_X}{D(F_X)}, F_{(X)}\right)$ tel que :

$$\lambda \circ \pi = \varphi \quad (16)$$

Appliquons maintenant la propriété universelle du groupe abélien libre $F_{(X)}$ (théorème (8.23)), dans le cas suivant :

$$\begin{array}{ccc}
 X & \xrightarrow{j_X} & F_{(X)} \\
 \downarrow \pi \circ \alpha_X & & \nearrow \exists! \mu \\
 \frac{F_X}{D(F_X)} & &
 \end{array}$$

Il existe $\mu \in \text{Hom}\left(F_{(X)}, \frac{F_X}{D(F_X)}\right)$ tel que

$$\mu \circ j_X = \pi \circ \alpha_X \quad (17)$$

Les relations (15), (16), (17) impliquent :

$$j_X = \varphi \circ \alpha_X = \lambda \circ \pi \circ \alpha_X = \lambda \circ \mu \circ j_X \quad (18)$$

$$\text{et} \quad \mu \circ \varphi \circ \alpha_X = \mu \circ j_X = \pi \circ \alpha_X \quad (19)$$

α_X et j_X étant les injections canoniques

$$(18) \Rightarrow \varphi/X = \text{id}_X = \lambda \circ \mu/X.$$

λ et μ sont des morphismes de groupes et $F_{(X)}$ est engendré par X , par suite

$$\lambda \circ \mu \text{ est l'identité dans } F_{(X)}, \quad (20)$$

$$(16) \text{ et } (19) \Rightarrow \mu \circ \lambda_{/\pi(X)} = \text{id}_{/\pi(X)};$$

$\frac{F_X}{D(F_X)}$ étant engendré par $\pi(X)$, on en déduit que :

$$\mu \circ \lambda \text{ est l'identité dans } \frac{F_X}{D(F_X)} \quad (21)$$

D'après (20) et (21), λ est un isomorphisme et $\mu = \lambda^{-1}$.

On en conclut que le groupe G défini, à un isomorphisme près, par la présentation $(X \mid [x, y]; (x, y) \in X \times X)$ est abélien libre sur X .

B / Rang d'un groupe libre

THÉORÈME (9.23). X et Y étant deux ensembles non vides, si F_X et F_Y sont des groupes librement engendrés par X et Y , respectivement, alors :

$$F_X \simeq F_Y \Leftrightarrow X \text{ équipotent à } Y.$$

Preuve : On sait, d'après le corollaire (9.16), que :

$$X \text{ équipotent à } Y \Rightarrow F_X \simeq F_Y,$$

démontrons, maintenant, la réciproque :

$$F_X \simeq F_Y \Rightarrow \frac{F_X}{D(F_X)} \simeq \frac{F_Y}{D(F_Y)} \quad (22)$$

Compte tenu de la proposition (9.21), le second membre de la relation (22) exprime que les groupes *abéliens libres* $F_{(X)}$ et $F_{(Y)}$ sont isomorphes; or (théorème (8.19)),

$$F_{(X)} \simeq F_{(Y)} \Leftrightarrow X \text{ équipotent à } Y$$

d'où $F_X \simeq F_Y \Rightarrow X \text{ équipotent à } Y$.

COROLLAIRE (9.24). *Si F est un groupe libre et si X et Y sont deux parties génératrices libres de F , alors*

$$\text{card}(X) = \text{card}(Y).$$

Ce résultat justifie la définition suivante :

Définition (9.25) : Si F est un groupe libre, alors le cardinal d'une partie génératrice libre de F est appelé le *rang de F* .

En particulier, un groupe libre est de *rang fini n* , s'il possède une partie génératrice libre finie de cardinal n .

Remarque (9.26) : Compte tenu du théorème (9.23), si F et F' sont deux groupes libres, alors :

$$F \simeq F' \Leftrightarrow \text{rang}(F) = \text{rang}(F').$$

3 — Sous-groupes d'un groupe libre

L'objet principal de ce paragraphe est de démontrer le théorème fondamental suivant :

THÉORÈME (9.27) (Nielsen ⁽¹⁾-Schreier). *Tout sous-groupe d'un groupe libre est un groupe libre.*

Cette propriété importante n'est pas simple à prouver. La méthode que nous avons adoptée est due à A. J. Weir ([73]; [62]); elle utilise la notion de transversale de Schreier et quelques résultats préliminaires.

(¹) Niels Nielsen (1890-1959).

A / Préliminaires

LEMME (9.28). Soient X un ensemble et Y une partie de X . Si F_X est le groupe librement engendré par X et si K est le sous-groupe normal de F_X engendré par Y , alors $\frac{F_X}{K}$ est un groupe libre, isomorphe au groupe F_E , où $E = X \setminus Y$.

Preuve : Pour $Y = \emptyset$, $\frac{F_X}{K} = F_X$ et pour $Y = X$, $\frac{F_X}{K} \simeq (1)$; on suppose donc, dans la suite, $Y \neq \emptyset$ et $Y \neq X$.

Soit le groupe F_E libre sur $E = X \setminus Y$. Appliquons la propriété universelle du groupe F_E (théorème (9.15)) au diagramme suivant :

$$\begin{array}{ccc}
 E & \xrightarrow{\alpha_E} & F_E \\
 \downarrow \beta & \nearrow \exists! \varphi & \\
 X & & \\
 \downarrow \alpha_X & \nearrow \exists! \psi & \\
 F_X & & \\
 \downarrow \pi & \nearrow & \\
 \frac{F_X}{K} & &
 \end{array} \tag{23}$$

α_E , β et α_X sont les injections canoniques et π est la surjection canonique; il existe alors φ et ψ tels que :

$$\varphi \in \text{Hom}(F_E, F_X), \quad \psi \in \text{Hom}\left(F_E, \frac{F_X}{K}\right)$$

et $\varphi \circ \alpha_E = \alpha_X \circ \beta, \quad \psi \circ \alpha_E = \pi \circ \alpha_X \circ \beta.$

On en déduit que

$$\pi \circ \varphi = \psi$$

et que ψ est surjectif.

Vérifions que ψ est injectif. Soit $w \neq 1$, dans $\text{Ker } \psi$; w s'écrit de façon unique

$$w = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n}, \quad \text{où } n \in \mathbb{N}^*, \quad a_j^{\varepsilon_j} \in E \cup E^{-1}, \quad \varepsilon_j = \pm 1,$$

quel que soit j ($1 \leq j \leq n$).

$$\psi(w) = \bar{1} \Leftrightarrow \pi \circ \varphi(w) = \bar{1}.$$

Pour tout $a \in E$, $\pi \circ \varphi(a) = \pi \circ \varphi \circ \alpha_E(a) = \pi(a)$; par suite,

$$\psi(w) = \bar{1} \Leftrightarrow \pi(a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n}) = \bar{1},$$

donc $\psi(w) = \bar{1} \Leftrightarrow w \in K$.

K étant le sous-groupe normal de F_X engendré par Y , quel que soit $y^* \in Y \cup Y^{-1}$, on a $Ky^* = K$, d'où

$$a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n} = x_1^{\varepsilon'_1} x_2^{\varepsilon'_2} \dots x_p^{\varepsilon'_p} y^*, \quad \text{où } x_1^{\varepsilon'_1} x_2^{\varepsilon'_2} \dots x_p^{\varepsilon'_p} \in K.$$

L'égalité de deux mots dans F_X implique, en particulier, $p = n - 1$ et $a_n^{\varepsilon_n} = y^*$, ce qui est impossible, car $E \cup E^{-1}$ et $Y \cup Y^{-1}$ sont disjoints; on en conclut que $\text{Ker } \psi = (1)$.

ψ est donc un isomorphisme, par suite, $\frac{F_X}{K}$ est un groupe libre, isomorphe à F_E .

Remarque (9.29) : Le lemme (9.28) exprime que, étant donné un ensemble X et une partie Y de X , un groupe de présentation $(X \mid Y)$ est un groupe libre.

Le principe de la démonstration du théorème (9.27) consiste alors à mettre en évidence, pour un sous-groupe H d'un groupe libre, une présentation de H de la forme précédente.

B / Transversales d'un sous-groupe dans un groupe

Définition (9.30) : Etant donné un groupe G et un sous-groupe H de G , on appelle *transversale à droite de H dans G* tout ensemble T de représentants des classes à droite, distinctes, de H dans G .

On définit de même une *transversale à gauche* de H dans G .

Remarques (9.31) : De la définition (9.30), on déduit immédiatement que, si T est une transversale à droite de H dans G , alors tout $g \in G$ s'écrit de façon unique $g = ht$, où $h \in H$ et $t \in T$.

On peut donc associer à la transversale T deux applications *surjectives* :

$$\eta : G \rightarrow H \quad \text{et} \quad \tau : G \rightarrow T$$

telles que, pour tout $g \in G$,

$$g = \eta(g) \tau(g) \quad (24)$$

Les applications η et τ vérifient les propriétés suivantes : quels que soient $h \in H$ et $g \in G$:

$$\eta(hg) = h\eta(g) \quad (25)$$

$$\tau(hg) = \tau(g) \quad (26)$$

LEMME (9.32). Soit un groupe $G \neq (e)$. Soient X une partie génératrice de G et H un sous-groupe de G . Si T est une transversale à droite de H dans G contenant l'élément unité de G , alors H est engendré par l'ensemble

$$Z = \{z_{t,x} = \eta(tx); t \in T, x \in X\}.$$

Preuve : La relation (24) implique $\eta(tx) = tx(\tau(tx))^{-1}$.

Pour $x \in X$ et $t \in T$, posons $z_{t,x^{-1}} = \eta(tx^{-1})$ et vérifions que

$$z_{t,x^{-1}} = (z_{\tau(tx^{-1}),x})^{-1}. \quad (27)$$

$$z_{\tau(tx^{-1}),x} = \tau(tx^{-1}) x(\tau(\tau(tx^{-1}) x))^{-1}$$

or
$$tx^{-1} = \eta(tx^{-1}) \tau(tx^{-1}) \Rightarrow t = \eta(tx^{-1}) \tau(tx^{-1}) x;$$

$t \in T$, $\eta(tx^{-1}) \in H$, donc, en appliquant (26), on obtient :

$$t = \tau(\tau(tx^{-1}) x) \quad (28)$$

d'où $(z_{\tau(tx^{-1}), x})^{-1} = tx^{-1} (\tau(tx^{-1}))^{-1} = z_{t, x^{-1}}$.

Soit $h \in H \setminus \{e\}$; l'application η étant surjective, on peut écrire

$$h = \eta(a_1 a_2 \dots a_n), \quad \text{où } a_i \in X \cup X^{-1}, n \geq 1 \text{ dans } \mathbf{N}.$$

Pour $n = 1$, $h = \eta(a_1) = z_{e, a_1}$.

Pour $n > 1$, on raisonne par récurrence sur n . On suppose que $g = a_1 a_2 \dots a_{n-1}$ est tel que $\eta(g)$ appartient au sous-groupe de H engendré par Z .

$$a_1 a_2 \dots a_n = \eta(g) \tau(g) a_n.$$

D'après la relation (25) :

$$h = \eta(a_1 a_2 \dots a_n) = \eta(g) \eta(\tau(g) a_n)$$

$$h = \eta(a_1 a_2 \dots a_n) = \eta(g) z_{\tau(g), a_n}, \quad a_n \in X \cup X^{-1}$$

donc H est engendré par Z .

On considère, dans toute la suite, un groupe F_X , librement engendré par un ensemble non vide X et un sous-groupe H de F_X . Si T est une transversale à droite de H dans F_X , contenant 1, alors H est engendré par l'ensemble Z défini dans le lemme (9.32).

Soit Y un ensemble équipotent à Z dont les éléments seront notés $y_{t,x}$, $t \in T$, $x \in X$. Soient F_Y un groupe librement engendré par Y et α_Y l'injection canonique de Y dans F_Y .

σ étant l'application de Y dans H telle que $\sigma(y_{t,x}) = z_{t,x}$, il existe, d'après le théorème (9.15), un unique morphisme $\varphi \in \text{Hom}(F_Y, H)$ tel que $\varphi \circ \alpha_Y = \sigma$.

$$\begin{array}{ccc}
 Y & \xrightarrow{\alpha_Y} & F_Y \\
 \sigma \downarrow & \searrow \exists! \varphi & \\
 H & &
 \end{array} \quad (29)$$

H est engendré par les $z_{t,x}$, donc φ est surjectif.

LEMME (9.33). *Dans le contexte défini par les hypothèses et les notations ci-dessus, il existe un morphisme $\psi \in \text{Hom}(H, F_Y)$, tel que*

$$\varphi \circ \psi = \text{id}_H$$

et l'endomorphisme $\lambda = \psi \circ \varphi$ de F_X vérifie la condition :

$$\lambda^2 = \lambda.$$

Preuve : Associons à tout $t \in T$ l'application

$$\psi_t : F_X \rightarrow F_Y$$

telle que :

$$\begin{aligned} \psi_t(1) &= 1 \\ \psi_t(x) &= y_{t,x}, \quad \forall x \in X \end{aligned} \tag{30}$$

et, quels que soient u et v dans F_X ,

$$\psi_t(uv) = \psi_t(u) \psi_{\tau(tu)}(v) \tag{31}$$

La condition (31) implique que, pour tout $x \in X$,

$$\psi_t(x^{-1}x) = 1 = \psi_t(x^{-1}) \psi_{\tau(tx^{-1})}(x)$$

$$\text{d'où} \quad \psi_t(x^{-1}) = (y_{\tau(tx^{-1}), x})^{-1} \tag{32}$$

Ainsi, pour tout $t \in T$, l'application ψ_t est définie, sur l'ensemble des mots de longueur 1, par les relations (30) et (32).

Si $u \in F_X$ est un mot réduit de longueur $n > 1$, on définit $\psi_t(u)$ par récurrence sur n .

On écrit $u = vx^\varepsilon$, où $x^\varepsilon \in X \cup X^{-1}$, $\varepsilon = \pm 1$, donc $\text{long}(v) = n - 1$.

Si l'on suppose $\psi_t(v)$ déterminé, alors, d'après la condition (31), on a

$$\psi_t(u) = \psi_t(v) \psi_{\tau(tv)}(x^\varepsilon) \tag{33}$$

Par hypothèse $1 \in T$; désignons alors par ψ la restriction de ψ_1 à H .

En appliquant la condition (31) au cas où $t = 1$, on obtient, quels que soient u et v dans H :

$$\psi(uv) = \psi(u) \psi(v),$$

donc, $\psi \in \text{Hom}(H, F_Y)$.

Montrons d'autre part que, quels que soient $t \in T$ et $u \in F_X$,

$$\varphi \circ \psi_t(u) = \eta(tu) \quad (34)$$

Pour $x \in X$,

$$\varphi \circ \psi_t(x) = \varphi(y_{t,x}) = \varphi \circ \alpha_Y(y_{t,x}),$$

$$\text{d'où } \varphi \circ \psi_t(x) = z_{t,x} = \eta(tx).$$

Pour $x^{-1} \in X^{-1}$,

$$\varphi \circ \psi_t(x^{-1}) = \varphi(y_{\tau(tx^{-1}),x})^{-1} = (z_{\tau(tx^{-1}),x})^{-1},$$

$$\text{d'où } \varphi \circ \psi_t(x^{-1}) = z_{t,x^{-1}} = \eta(tx^{-1}).$$

De plus,

$$\varphi \circ \psi_t(1) = \varphi(1) = 1.$$

Pour $u \in F_X$, tel que $\text{long}(u) = n > 1$, on procède par récurrence sur n , en posant, comme plus haut, $u = vx^e$ et en utilisant la formule (33).

Pour tout $u \in H$, on a $\eta(u) = u$, d'où :

$$\varphi \circ \psi = \text{id}_H.$$

$\lambda = \psi \circ \varphi$ est un endomorphisme de F_Y et, quel que soit $w \in F_Y$,

$$\lambda \circ \lambda(w) = \psi \circ (\varphi \circ \psi) \circ \varphi(w) = \lambda(w),$$

$$\text{donc } \lambda^2 = \lambda.$$

Remarque (9.34) : La condition $\lambda^2 = \lambda$ implique que $\text{Ker } \lambda$ est le sous-groupe normal de F_Y engendré par l'ensemble : $\{w\lambda(w^{-1}) ; w \in F_Y\}$ (voir exercice 24, chap. V).

Or, $\lambda = \psi \circ \varphi$, donc $\text{Ker } \varphi \subseteq \text{Ker } \lambda$; de plus, pour $w \in F_Y$,

$$\varphi(w\lambda(w^{-1})) = \varphi(w) \varphi \circ \psi \circ \varphi(w^{-1});$$

$$\text{alors } \varphi \circ \psi = \text{id}_H \Rightarrow \varphi(w\lambda(w^{-1})) = 1.$$

On en déduit : $\text{Ker } \lambda \subseteq \text{Ker } \varphi$ et, par suite,

$$\text{Ker } \varphi = \text{Ker } \lambda \quad (35)$$

LEMME (9.35). *Compte tenu des hypothèses et notations précédentes, pour toute transversale à droite T de H dans F_X , contenant 1,*

$$\{y_{t,x}; t \in T, x \in X \mid \psi_1(t); t \in T\}$$

est une présentation de H.

Preuve : N étant le sous-groupe normal de F_Y engendré par l'ensemble : $\{\psi_1(t); t \in T\}$, il faut démontrer que H est isomorphe à $\frac{F_Y}{N}$.

Or, dans le diagramme (29), φ est un épimorphisme, on a donc $H \simeq \frac{F_Y}{\text{Ker } \varphi}$; d'autre part, d'après la relation (34), $\varphi \circ \psi_1(t) = \eta(t) = 1$, d'où :

$$N \subseteq \text{Ker } \varphi \quad (36)$$

Il suffit donc de prouver que : $\text{Ker } \varphi \subseteq N$.

1° Notons M le sous-groupe normal de F_Y engendré par l'ensemble $\{y_{t,x} \lambda(y_{t,x}^{-1}); y_{t,x} \in Y\}$ et vérifions que $\text{Ker } \varphi = M$.

D'après la remarque (9.34), $\text{Ker } \varphi$ est le sous-groupe normal de F_Y engendré par $\{w \lambda(w^{-1}); w \in F_Y\}$, on a donc $M \subseteq \text{Ker } \varphi$. Montrons alors que, pour tout $w \in F_Y$, $w \lambda(w^{-1}) \in M$.

D'après la définition de M, la propriété est vraie pour $w = y_{t,x}$, où $y_{t,x} \in Y$.

Pour $w = y_{t,x}^{-1}$, $w \lambda(w^{-1}) = y_{t,x}^{-1} \lambda(y_{t,x})$

$$y_{t,x}^{-1} \lambda(y_{t,x}) = y_{t,x}^{-1} \lambda(y_{t,x}) y_{t,x}^{-1} y_{t,x} = y_{t,x}^{-1} (y_{t,x} \lambda(y_{t,x}^{-1}))^{-1} y_{t,x}$$

M est normal dans F_Y , donc $y_{t,x}^{-1} \lambda(y_{t,x}) \in M$.

Pour $w \in F_Y$ tel que $\text{long}(w) = n > 1$, on écrit $w = v y_{t,x}^\varepsilon$, où $y_{t,x} \in Y$, $\varepsilon = \pm 1$, donc $\text{long}(v) = n - 1$ et on vérifie, par récurrence sur n , que $w \lambda(w^{-1}) \in M$.

On obtient ainsi $\text{Ker } \varphi = M$; on remarque que cette égalité signifie que : $\{Y \mid y_{t,x} \lambda(y_{t,x}^{-1}); y_{t,x} \in Y\}$ est une présentation de H.

2° Compte tenu du résultat précédent et de l'inclusion (36), démontrons que, pour tout $y_{t,x} \in Y$, $y_{t,x} \lambda(y_{t,x}^{-1}) \in N$.

$$\lambda(y_{t,x}) = \psi \circ \varphi(y_{t,x}) = \psi(z_{t,x}),$$

$$\lambda(y_{t,x}) = \psi_1(tx(\tau(tx))^{-1}).$$

En posant $u = \tau(tx)$, on a, en appliquant la formule (31) :

$$\lambda(y_{t,x}) = \psi_1(tx) \psi_u(u^{-1}) = \psi_1(t) y_{t,x} (\psi_1(u))^{-1},$$

par suite,

$$y_{t,x} \lambda(y_{t,x}^{-1}) = (y_{t,x} \psi_1(u) y_{t,x}^{-1}) (\psi_1(t))^{-1},$$

$\psi_1(t)$ et $\psi_1(u)$ sont dans N et N est normal dans F_X , donc $y_{t,x} \lambda(y_{t,x}^{-1}) \in N$, d'où $M \subseteq N$. On en conclut que $N = M = \text{Ker } \varphi$, ce qui entraîne : $H \simeq \frac{F_X}{N}$.

LEMME (9.36). *Il existe une transversale à droite T de H dans F_X , contenant 1 et telle que*

$$t = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \in T \Rightarrow x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k} \in T, \quad \forall k \ (1 \leq k \leq n) \quad (37)$$

Une telle transversale est appelée : *transversale de Schreier à droite*, de H dans F_X .

Preuve : Etant donné une classe à droite Hu , de H dans F_X , on appellera *longueur de Hu* le minimum de la longueur d'un mot appartenant à Hu .

Démontrons, par récurrence sur $n = \text{long}(Hu)$, qu'en choisissant dans chaque classe Hu un représentant t de longueur minimum, on définit une transversale de Schreier de H dans F_X .

— Dans H , on prend $t = 1$, qui est de longueur 0.

— Dans toute classe de longueur 1, on choisit un représentant t de la forme $x^\varepsilon \in X \cup X^{-1}$, $\varepsilon = \pm 1$.

— Supposons que dans toute classe de longueur n on ait choisi un représentant t vérifiant la condition (37).

Soit Hg une classe de longueur $n + 1$; il existe $u \in Hg$ tel que $\text{long}(u) = n + 1$.

Ecrivons $u = vx^\varepsilon$, où $x^\varepsilon \in X \cup X^{-1}$, $\varepsilon = \pm 1$, donc $\text{long}(v) = n$; alors $\text{long}(Hv) = n$ et si t est le représentant choisi dans Hv , satisfaisant à la condition (37), alors tx^ε est un représentant de Hg , vérifiant cette même condition.

C / Preuve du théorème de Nielsen-Schreier (9.27)

H étant un sous-groupe d'un groupe libre F_X , soit T une *transversale de Schreier* à droite de H dans F_X . En utilisant les mêmes notations que précédemment, posons

$$Y' = Y \cap \text{Ker } \varphi = \{y_{t,x} \in Y; \varphi(y_{t,x}) = 1\}$$

et démontrons que $\{Y | Y'\}$ est une présentation de H.

Soit K le sous-groupe normal de F_Y engendré par Y' .

$$Y' \subseteq \text{Ker } \varphi \Rightarrow K \subseteq \text{Ker } \varphi.$$

D'autre part, d'après le lemme (9.35), $\text{Ker } \varphi$ est le sous-groupe normal de F_Y engendré par l'ensemble $\{\psi_1(t); t \in T\}$; montrons alors que $\psi_1(t) \in K$, quel que soit $t \in T$.

Si $\text{long}(t) = 0$, $t = 1$, $\psi_1(t) = 1$ et $1 \in K$.

Pour $\text{long}(t) = n$, $n > 0$, raisonnons par récurrence sur n . Posons $t = sx^\varepsilon$, où $x^\varepsilon \in X \cup X^{-1}$, $\varepsilon = \pm 1$, donc

$$\text{long}(s) = n - 1.$$

T étant une transversale de Schreier, s appartient à T.

$$\psi_1(t) = \psi_1(sx^\varepsilon) = \psi_1(s) \psi_s(x^\varepsilon).$$

L'hypothèse de récurrence implique $\psi_1(s) \in K$. D'autre part :

— si $\varepsilon = 1$, $t = sx$, $\psi_s(x) = y_{s,x}$ et d'après la relation (34) :

$$\varphi(y_{s,x}) = \varphi \circ \psi_s(x) = \eta(sx),$$

donc $\varphi(y_{s,x}) = \eta(t) = 1$, car $t \in T$; d'où $y_{s,x} \in Y'$, par suite $\psi_s(x) \in K$;

— si $\varepsilon = -1$, $t = sx^{-1}$, $\psi_s(x^{-1}) = (y_{\tau(sx^{-1}),s})^{-1} = (y_{t,x})^{-1}$;

$$\varphi(y_{t,x}) = \varphi \circ \psi_t(x) = \eta(tx)$$

$t = sx^{-1}$ implique $s \in T$, car T est une transversale de Schreier, alors, $\varphi(y_{t,x}) = \eta(s) = 1$, donc $y_{t,x} \in Y'$, par suite,

$$\psi_s(x^{-1}) = (y_{t,x})^{-1} \in K.$$

Ainsi, pour tout $t \in T$, $\psi_1(t) \in K$; on en déduit que $\text{Ker } \varphi = K$, donc $\{Y \mid Y'\}$ est une présentation de H ; Y' étant une partie de Y , le lemme (9.28) permet d'affirmer que H est un groupe libre (remarque (9.29)).

Plus précisément, H est un groupe libre, isomorphe au groupe F_E où $E = Y \setminus Y'$.

$$y_{t,x} \in Y \setminus Y' \Leftrightarrow \varphi(y_{t,x}) \neq 1,$$

or, $\varphi(y_{t,x}) = \eta(tx)$, par suite le résultat du lemme (9.32) conduit à l'énoncé suivant :

PROPOSITION (9.37). *Si H est un sous-groupe d'un groupe libre F_X , si T est une transversale de Schreier à droite de H dans F_X , alors H est librement engendré par l'ensemble des éléments :*

$$z_{t,x} = \eta(tx), \quad \text{tels que } t \in T, x \in X \text{ et } tx \notin T.$$

D / Rang d'un sous-groupe d'un groupe libre

Remarque (9.38) : La proposition (9.37) montre que, si F est un groupe libre de rang fini et si H est un sous-groupe de F , d'indice fini, alors H est un groupe libre de rang fini (détermination du rang de H : exercice 1, chap. IX).

Cependant, comme le prouve le théorème (9.39) ci-dessous, un groupe libre de rang fini peut contenir un sous-groupe de rang infini.

Plus généralement, on peut démontrer (théorème de Schreier [63]) que, si F est un groupe libre et si $H \neq (1)$ est d'indice infini dans F , alors H est de rang infini.

THÉORÈME (9.39). *Si F est un groupe libre de rang 2, alors $D(F)$ est de rang infini dénombrable.*

Preuve : Soit $\{x, y\}$ une partie génératrice libre de F .

Posons $F' = D(F)$; d'après la proposition (9.22), $\frac{F}{F'}$ est un groupe abélien libre de rang 2 et si \bar{x}, \bar{y} désigne les classes de x et y modulo F' dans F , alors $\{\bar{x}, \bar{y}\}$ est une base de $\frac{F}{F'}$.

Quel que soit $\bar{u} \in \frac{F}{F'}$, \bar{u} s'écrit de façon unique :

$$\bar{u} = \bar{x}^m \bar{y}^n, \quad \text{où } m \text{ et } n \text{ sont dans } \mathbf{Z}.$$

On en déduit que $T = \{t_{m,n} = x^m y^n; m \text{ et } n \text{ dans } \mathbf{Z}\}$ est une transversale de Schreier de F' dans F .

Pour tout $t_{m,n}$ tel que $n \neq 0$, on a

$$\eta(t_{m,n} x) = t_{m,n} x (\tau(t_{m,n} x))^{-1}.$$

$t_{m,n} x = x^m y^n x$ et dans $\frac{F}{F'}$, $\bar{x}^m \bar{y}^n \bar{x} = \bar{x}^{m+1} \bar{y}^n$, d'où

$$\tau(t_{m,n} x) = x^{m+1} y^n,$$

par suite :

$$\eta(t_{m,n} x) = x^m y^n x y^{-n} x^{-m-1},$$

donc $\eta(t_{m,n} x) \neq 1$. On remarquera que $\eta(t_{m,n} x) = [t_{m,n}^{-1}, x^{-1}]$.

D'autre part, quels que soient m et n dans \mathbf{Z} , $t_{m,n} y \in T$ et, quel que soit $m \in \mathbf{Z}$, $t_{m,0} x \in T$.

D'après la proposition (9.37), le sous-groupe F' de F est alors librement engendré par l'ensemble des $t_{m,n} x$ tels que $n \neq 0$, donc F' est de rang infini dénombrable.

4 — Produit libre de groupes

Soient I un ensemble non vide et $\{G_i\}_{i \in I}$ une famille de groupes nous connaissons le produit direct des groupes G_i (chap. I), nous allons maintenant associer à la famille $\{G_i\}_{i \in I}$ un autre groupe Γ , engendré par $\bigcup_{i \in I} G_i$ qui sera appelé : produit libre des groupes G_i , $i \in I$ (en théorie des catégories, ce groupe est appelé *coproduit* direct des groupes G_i , $i \in I$).

La construction de Γ se fait par une méthode analogue à celle qui a permis de définir un groupe libre sur un ensemble donné.

A / Construction d'un produit libre de groupes

Soit $\{G_i\}_{i \in I}$ une famille non vide de groupes.

Définition (9.40) : On appelle *mot* sur $\bigcup_{i \in I} G_i$ toute suite finie :

$$a_{i_1} a_{i_2} \dots a_{i_n}, \quad \text{où } n \in \mathbf{N}^*, a_{i_j} \in G_{i_j}$$

quel que soit j ($1 \leq j \leq n$).

Le mot correspondant à la partie vide de $\bigcup_{i \in I} G_i$ sera appelé le *mot vide* et noté 1. On désignera par $(\bigcup_{i \in I} G_i)$ l'ensemble des mots sur $\bigcup_{i \in I} G_i$.

Dans $(\bigcup_{i \in I} G_i)$ deux mots $a_{i_1} a_{i_2} \dots a_{i_n}$ et $b_{j_1} b_{j_2} \dots b_{j_p}$ sont égaux si et seulement si $n = p$ et $a_{i_k} = b_{j_k}$, quel que soit k ($1 \leq k \leq n$).

D'autre part, pour tout $i \in I$, on notera e_i l'élément unité du groupe G_i .

Définitions (9.41) :

1° On dira que les mots

$$a_{i_1} \dots a_{i_{j-1}} a_{i_j} a_{i_{j+1}} \dots a_{i_n}$$

et

$$a_{i_1} \dots a_{i_{j-1}} a_{i_{j+1}} \dots a_{i_n}$$

sont *élémentairement équivalents*, si $a_{i_j} = e_{i_j}$.

De même

$$a_{i_1} \dots a_{i_{j-1}} a_{i_j} a_{i_{j+1}} a_{i_{j+2}} \dots a_{i_n}$$

et

$$a_{i_1} \dots a_{i_{j-1}} a_{i_j}^* a_{i_{j+2}} \dots a_{i_n}$$

sont *élémentairement équivalents*, si a_{i_j} et $a_{i_{j+1}}$ sont dans le même groupe G_{i_j} et que $a_{i_j} a_{i_{j+1}} = a_{i_j}^*$.

2° Deux mots u et v de $(\bigcup_{i \in I} G_i)$ seront dits *équivalents* s'il existe un nombre fini de mots, z_1, z_2, \dots, z_n , tels que :

$$u = z_1, \quad v = z_n$$

et, pour tout i ($1 \leq i \leq n-1$), z_i et z_{i+1} sont *élémentairement équivalents*.

On peut vérifier sans difficulté que la relation « u équivalent à v » est une *relation d'équivalence* dans $(\bigcup_{i \in I} G_i)$; on la notera \mathcal{R} .

On désignera par $[u]$ la *classe d'équivalence* modulo \mathcal{R} d'un mot u et par $[\bigcup_{i \in I} G_i]$ l'*ensemble quotient* de $(\bigcup_{i \in I} G_i)$ par \mathcal{R} .

Produit de mots : Quel que soit $w \in (\bigcup_{i \in I} G_i)$, on pose

$$w1 = 1w = w$$

et pour $u = a_{i_1} a_{i_2} \dots a_{i_n}$ et $v = b_{j_1} b_{j_2} \dots b_{j_p}$ dans $(\bigcup_{i \in I} G_i)$, on pose

$$uv = a_{i_1} \dots a_{i_n} b_{j_1} \dots b_{j_p}.$$

Muni de ce produit, $(\bigcup_{i \in I} G_i)$ est un monoïde.

PROPOSITION (9.42). *La relation d'équivalence \mathcal{R} définie dans $(\bigcup_{i \in I} G_i)$ est compatible avec le produit des mots et l'ensemble quotient $[\bigcup_{i \in I} G_i]$ muni de la loi quotient telle que, quelles que soient les classes d'équivalence $[u]$ et $[v]$:*

$$[u][v] = [uv].$$

est un groupe dont l'élément unité est $[1]$.

Démonstration laissée au lecteur.

Définition (9.43) : On appellera *produit libre* (ou *coproduit direct*) des groupes G_i , $i \in I$, tout groupe engendré par $\bigcup_{i \in I} G_i$ et isomorphe au groupe $[\bigcup_{i \in I} G_i]$ défini dans la proposition (9.42).

Définition (9.44) : Un mot $u \in (\bigcup_{i \in I} G_i)$ est dit *réduit* si $u = 1$, ou si $u = a_{i_1} a_{i_2} \dots a_{i_n}$ est tel qu'aucun des a_i n'est élément unité d'un groupe G_i et tel que, quel que soit j ($1 \leq j \leq n-1$), a_j et a_{j+1} n'appartiennent pas à un même groupe G_i .

Par un procédé analogue à celui utilisé dans la démonstration du théorème (9.11), on définit une méthode de réduction d'un

mot $u = a_{i_1} a_{i_2} \dots a_{i_n}$, en lui associant une suite de mots : u_0, u_1, \dots, u_n , telle que chaque u_i est réduit et, en particulier, u_n est réduit et équivalent à u .

Précisons la construction de la suite u_0, u_1, \dots, u_n .

Si $u = a_{i_1} a_{i_2} \dots a_{i_n}$ est un mot dans $(\bigcup_{i \in I} G_i)$, on pose : $u_0 = 1$; $u_1 = a_{i_1}$, si $a_{i_1} \neq e_{i_1}$ et $u_1 = 1$, si $a_{i_1} = e_{i_1}$.

Si l'on suppose u_k déterminé, pour $1 \leq k \leq n-1$, et si $u_k = b_1 b_2 \dots b_s$, alors :

$$u_{k+1} = u_k, \quad \text{si } a_{i_{k+1}} = e_{i_{k+1}};$$

$$u_{k+1} = u_k a_{i_{k+1}} \quad \text{si } b_s \notin G_{i_{k+1}};$$

si $b_s \in G_{i_{k+1}}$, alors :

$$u_{k+1} = b_1 b_2 \dots b_{s-1}, \quad \text{si } b_s a_{i_{k+1}} = e_{i_{k+1}}$$

$$u_{k+1} = b_1 b_2 \dots b_{s-1} a_{i_{k+1}}^*, \quad \text{si } b_s a_{i_{k+1}} = a_{i_{k+1}}^* \quad \text{dans } G_{i_{k+1}}.$$

Ainsi, pour tout k ($1 \leq k \leq n$), u_k est un mot réduit équivalent à $a_{i_1} a_{i_2} \dots a_{i_k}$; u_n sera appelé la *forme réduite de u* et noté $r(u)$.

Comme dans le cas du groupe libre, on prouve que chaque classe d'équivalence $[u] \in [\bigcup_{i \in I} G_i]$ ne contient qu'un seul mot réduit $r(u)$. (Nous n'explicitons pas la démonstration.)

En particulier, quel que soit $i \in I$, 1 est l'unique mot réduit de $[e_i]$.

Notons $\coprod_{i \in I} G_i$ l'ensemble des mots réduits de $(\bigcup_{i \in I} G_i)$.

Au moyen de la bijection qui associe à chaque classe $[u] \in [\bigcup_{i \in I} G_i]$ l'unique mot réduit qu'elle contient, on définit dans $\coprod_{i \in I} G_i$ une loi de composition telle que, quels que soient les mots réduits u et v :

$$uv = r(uv);$$

relativement à cette loi, $\coprod_{i \in I} G_i$ est un groupe engendré par $\bigcup_{i \in I} G_i$ et isomorphe au groupe $[\bigcup_{i \in I} G_i]$, donc $\coprod_{i \in I} G_i$ est produit libre des groupes G_i , $i \in I$.

Remarque (9.45) : Tout $u \in \prod_{i \in I} G_i$ s'écrit de façon unique :

$$u = a_{i_1} a_{i_2} \dots a_{i_n},$$

où $n \in \mathbb{N}$, $a_{i_j} \in G_{i_j}$ quel que soit j ($1 \leq j \leq n$), avec $u = 1$ si et seulement si $n = 0$; si $u \neq 1$, pour tout j , on a $a_{i_j} \neq e_{i_j}$ et $a_{i_{j+1}} \notin G_{i_j}$.

On en déduit immédiatement qu'un produit libre de groupes $(\prod_{i \in I} G_i)$ est un groupe *non abélien*.

B / Propriété universelle du produit libre de groupes

$\{G_i\}_{i \in I}$ étant une famille non vide de groupes, pour tout $i \in I$, considérons l'application :

$$q_i : G_i \rightarrow \prod_{i \in I} G_i$$

définie par $a_i \mapsto r(a_i)$ (forme réduite de a_i).

Compte tenu de la méthode de réduction d'un mot, développée plus haut, on vérifie que q_i est un monomorphisme de groupes, appelé *monomorphisme canonique* de G_i dans $\prod_{i \in I} G_i$.

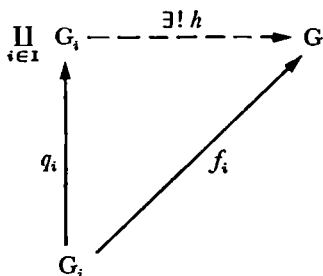
Remarque (9.46) : Quel que soit I , $\prod_{i \in I} G_i$ contient au moins un sous-groupe isomorphe à G_i .

En effet, pour tout $i \in I$, on a $G_i \simeq \text{Im } q_i$.

THÉORÈME (9.47). (Propriété universelle.) Soit $\{G_i\}_{i \in I}$ une famille, non vide, de groupes. Soient Γ un groupe engendré par $\bigcup_{i \in I} G_i$ et $\{\alpha_i\}_{i \in I}$ la famille des injections canoniques de G_i dans Γ ; alors Γ est produit libre des groupes G_i , si et seulement si, quels que soient le groupe G et la famille de morphismes $\{f_i\}_{i \in I}$, telle que, pour tout $i \in I$, $f_i \in \text{Hom}(G_i, G)$, il existe un unique $h \in \text{Hom}(\Gamma, G)$ vérifiant : $h \circ \alpha_i = f_i$, quel que soit $i \in I$.

Preuve :

1° Supposons $\Gamma = \coprod_{i \in I} G_i$ et $\alpha_i = q_i$, quel que soit $i \in I$.
Pour chaque $i \in I$, considérons le diagramme :



dans lequel G et f_i sont donnés.

Pour tout mot réduit $u \in \coprod_{i \in I} G_i$, tel que $u = a_{i_1} a_{i_2} \dots a_{i_n}$, posons :

$$h(a_{i_1} a_{i_2} \dots a_{i_n}) = f_{i_1}(a_{i_1}) f_{i_2}(a_{i_2}) \dots f_{i_n}(a_{i_n}), \quad \text{si } n > 0$$

et $h(1) = e$, si $n = 0$ (e étant l'élément unité de G).

On en déduit que, pour tout $i \in I$, on a $h \circ q_i = f_i$.

Vérifions que h est un morphisme de groupes.

Soient u et v dans $\coprod_{i \in I} G_i$, tels que :

$$u = a_{i_1} a_{i_2} \dots a_{i_n} \quad \text{et} \quad v = b_{j_1} b_{j_2} \dots b_{j_p}, \quad n \neq 0, p \neq 0.$$

Pour $p = 1$, $uv = a_{i_1} a_{i_2} \dots a_{i_n} b_{j_1}$, si $b_{j_1} \notin G_{i_n}$.

Lorsque $b_{j_1} \in G_{i_n}$, $uv = a_{i_1} a_{i_2} \dots a_{i_{n-1}}$, si $a_{i_n} b_{j_1} = e_{i_n}$,
 $uv = a_{i_1} a_{i_2} \dots a_{i_n}^*$, si $a_{i_n} b_{j_1} = a_{i_n}^* \neq e_{i_n}$, dans G_{i_n} .

Dans tous les cas on vérifiera que $h(uv) = h(u) h(v)$.

Pour $p > 1$, on procède par récurrence sur p . On suppose :

$$h(ub_{j_1} b_{j_2} \dots b_{j_{p-1}}) = h(u) h(b_{j_1} b_{j_2} \dots b_{j_{p-1}});$$

en raisonnant comme dans le cas où $p = 1$, on prouve alors que $h(uv) = h(u) h(v)$.

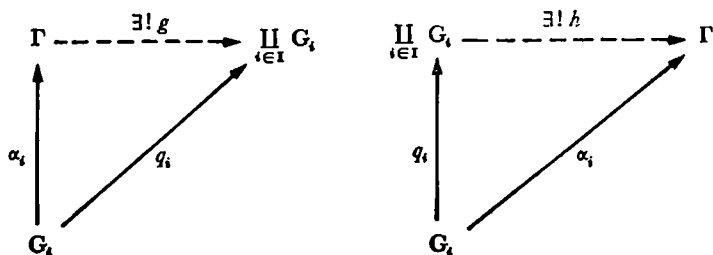
Enfin, si h' est un morphisme de $\coprod_{i \in I} G_i$ dans G , tel que, pour tout $i \in I$, $h' \circ q_i = f_i$, alors, quel que soit $u = a_{i_1} a_{i_2} \dots a_{i_n}$ dans $\coprod_{i \in I} G_i$,

$$\begin{aligned} h'(u) &= h'(q_{i_1}(a_{i_1}) q_{i_2}(a_{i_2}) \dots q_{i_n}(a_{i_n})) \\ &= f_{i_1}(a_{i_1}) f_{i_2}(a_{i_2}) \dots f_{i_n}(a_{i_n}), \end{aligned}$$

d'où $h' = h$.

2° Soit Γ un groupe engendré par $\bigcup_{i \in I} G_i$; pour tout $i \in I$, α_i étant l'injection canonique de G_i dans Γ , on suppose que le couple $(\Gamma, \{\alpha_i\}_{i \in I})$ vérifie les conditions énoncées dans le théorème (9.47).

On considère, pour tout $i \in I$, les deux diagrammes suivants :



Les hypothèses et la partie 1° de la démonstration impliquent qu'il existe $g \in \text{Hom}(\Gamma, \prod_{i \in I} G_i)$ et $h \in \text{Hom}(\prod_{i \in I} G_i, \Gamma)$ tels que, pour tout $i \in I$:

$$g \circ \alpha_i = q_i, \quad h \circ q_i = \alpha_i.$$

On en déduit que $h \circ g \circ \alpha_i = \alpha_i$ et $g \circ h \circ q_i = q_i$.

g et h étant des morphismes de groupes, Γ et $\prod_{i \in I} G_i$ étant engendrés par $\bigcup_{i \in I} G_i$, on a :

$$h \circ g = \text{id}_\Gamma \quad \text{et} \quad g \circ h = \text{id}_{\prod_{i \in I} G_i};$$

par suite, Γ est isomorphe à $\prod_{i \in I} G_i$, on en conclut que Γ est produit libre des groupes G_i , $i \in I$.

COROLLAIRE (9.48). Si $\{G_i\}_{i \in I}$ et $\{G'_i\}_{i \in I}$ sont deux familles de groupes, alors $(G_i \simeq G'_i, \forall i \in I) \Rightarrow \prod_{i \in I} G_i \simeq \prod_{i \in I} G'_i$.

Démonstration laissée au lecteur.

PROPOSITION (9.49). Tout groupe F_X , librement engendré par un ensemble non vide $X = \{x_i\}_{i \in I}$, est produit libre des groupes monogènes infinis $\langle x_i \rangle$, $i \in I$.

Preuve : Quel que soit $i \in I$, notons α_i l'injection canonique de $\langle x_i \rangle$ dans F_X et considérons le diagramme ci-dessous :

$$\begin{array}{ccc} \prod_{i \in I} \langle x_i \rangle & \xrightarrow{\exists! h} & F_X \\ \uparrow q_i & \nearrow \alpha_i & \\ \langle x_i \rangle & & \end{array}$$

D'après le théorème (9.47), il existe un unique

$$h \in \text{Hom}\left(\prod_{i \in I} \langle x_i \rangle, F_X\right)$$

tel que $h \circ q_i = \alpha_i$, pour tout $i \in I$.

F_X étant engendré par X , h est surjectif; vérifions que h est injectif. Soit $u \in \prod_{i \in I} \langle x_i \rangle$, tel que $h(u) = 1$.

u est un mot réduit dans $(\bigcup \langle x_i \rangle)$ qui s'écrit de façon unique :

$$u = x_{i_1}^{m_1} x_{i_2}^{m_2} \dots x_{i_p}^{m_p}, \quad \text{où } p \in \mathbb{N}, x_{i_j}^{m_j} \in \langle x_{i_j} \rangle,$$

quel que soit j ($1 \leq j \leq p$)

$$h(u) = h(q_{i_1}(x_{i_1}^{m_1}) \dots q_{i_p}(x_{i_p}^{m_p})) = x_{i_1}^{m_1} \dots x_{i_p}^{m_p}$$

$x_{i_1}^{m_1} \dots x_{i_p}^{m_p}$ est un mot réduit, élément de F_X , alors

$$x_{i_1}^{m_1} \dots x_{i_p}^{m_p} = 1 \quad \text{dans } F_X \Leftrightarrow p = 0,$$

donc $h(u) = 1$ implique $u = 1$ dans $\prod_{i \in I} \langle x_i \rangle$, par suite on a

$$F_X \simeq \prod_{i \in I} \langle x_i \rangle, \quad \text{avec } \langle x_i \rangle \simeq \mathbb{Z}, \text{ quel que soit } i \in I.$$

D'autre part, F_X peut être considéré comme engendré par $\bigcup_{i \in I} \langle x_i \rangle$, donc F_X est produit libre des groupes monogènes infinis $\langle x_i \rangle$, $i \in I$.

Remarque (9.50) : Comme le justifie la proposition (9.49) (et comme le font certains auteurs [45]) on aurait pu définir un groupe libre comme un produit libre de groupes monogènes infinis. Une telle définition est à rapprocher de celle d'un groupe abélien libre, qui est somme directe de groupes monogènes infinis.

Ce parallélisme vient du fait que le produit libre de groupes et la somme directe de groupes abéliens représentent le même concept de coproduit direct, l'un dans la catégorie des groupes, l'autre dans la catégorie des groupes abéliens (même propriété universelle) [54].

Exercices Chapitre IX

- 1) Soit F un groupe libre de rang fini $n > 1$. Soit H un sous-groupe de F , d'indice fini k .

On désigne par X une famille génératrice libre de F et par T une transversale de Schreier à droite de H dans F ; comme dans le lemme (9.32), on pose

$$Z = \{ z_{t,x} = \eta(tx); t \in T, x \in X \}.$$

- a) Vérifier que, si $t \in T$ et $x \in X$, alors :

$$z_{t,x} = 1 \Leftrightarrow (\exists s \in T, t = sx^{-1}).$$

- b) Montrer que tout $t \in T \setminus \{1\}$ s'écrit de façon unique :

$$t = sx^\varepsilon, \quad \text{où } x \in X, \quad \varepsilon = \pm 1, \quad s \in T$$

et que

$$\varepsilon = -1 \Rightarrow z_{t,x} = 1$$

$$\varepsilon = 1 \Rightarrow z_{s,x} = 1.$$

En déduire que le nombre des éléments de Z égaux à 1 est $k - 1$.

En conclure que $\text{rang}(H) = k(n - 1) + 1$.

[Utiliser la proposition (9.37).]

- 2) Soit G un groupe fini, non cyclique. On suppose $G \simeq \frac{F}{H}$ où F est un groupe libre de rang fini, prouver que :

$$\text{rang}(H) > \text{rang}(F).$$

- 3) Soit $\{G_i\}_{i \in I}$ une famille de groupes ($\text{card}(I) > 1$).

On pose $\Gamma = \coprod_{i \in I} G_i$ et pour tout $i \in I$, q_i désignant l'injection canonique de G_i dans Γ , on identifie chaque G_i à $\text{Im } q_i$.

a) Vérifier que, quels que soient $i \neq j$ dans I , on a $G_i \cap G_j = (1)$.

b) $Z(\Gamma)$ désignant le centre de Γ , prouver que $Z(\Gamma) = (1)$.

c) $Z(F)$ étant le centre d'un groupe libre F , montrer que $\text{rang}(F) > 1 \Rightarrow Z(F) = (1)$.

- 4) G_1, G_2, G_3 étant des groupes, montrer que l'on a :

$$G_1 \sqcup G_2 \simeq G_2 \sqcup G_1$$

$$\text{et } (G_1 \sqcup G_2) \sqcup G_3 \simeq G_1 \sqcup (G_2 \sqcup G_3).$$

- 5) Etant donné une famille non vide de groupes : $\{G_i\}_{i \in I}$, on note q_i les injections canoniques : $G_i \rightarrow \coprod_{i \in I} G_i$.

a) Montrer que, pour tout groupe G , l'application :

$$\begin{aligned} \text{Hom}\left(\coprod_{i \in I} G_i, G\right) &\rightarrow \prod_{i \in I} \text{Hom}(G_i, G) \\ h &\mapsto (h \circ q_i)_{i \in I} \end{aligned}$$

est une bijection.

b) On pose $\Gamma = \coprod_{i \in I} G_i$ et, pour tout $i \in I$, on note H_i le sous-groupe normal de Γ engendré par $\bigcup_{j \neq i} G_j$.

Démontrer que l'on a $\frac{\Gamma}{H_i} \simeq G_i$.

- 6) Soit $\{G_i\}_{i \in I}$ une famille non vide de groupes.

Pour tout $i \in I$, soit $(X_i \mid R_i)$ une présentation du groupe G_i . On note F_{X_i} un groupe libre sur X_i et (R_i) le sous-groupe normal de F_{X_i} engendré par R_i .

a) Vérifier que l'on a $\coprod_{i \in I} \frac{F_{X_i}}{(R_i)} \simeq \coprod_{i \in I} G_i$.

b) On pose $X = \bigcup_{i \in I} X_i$, $R = \bigcup_{i \in I} R_i$ et on note F_X un groupe libre sur X .

Etant donné les injections canoniques :

$$\alpha_{X_i} : X_i \rightarrow F_{X_i}, \quad \alpha_X : X \rightarrow F_X \quad \text{et} \quad \lambda_i : X_i \rightarrow X,$$

montrer que, pour tout $i \in I$, il existe un monomorphisme $\varphi_i \in \text{Hom}(F_{X_i}, F_X)$ tel que $\varphi_i \circ \alpha_{X_i} = \alpha_X \circ \lambda_i$.

En déduire qu'il existe $\bar{\varphi}_i \in \text{Hom} \left(\frac{F_{X_i}}{(R_i)}, \frac{F_X}{(R)} \right)$ tel que

$$\bar{\varphi}_i \circ \pi_i = \pi \circ \varphi_i,$$

où π_i et π sont les épimorphismes canoniques : $F_{X_i} \rightarrow \frac{F_{X_i}}{(R_i)}$ et $F_X \rightarrow \frac{F_X}{(R)}$.

c) Démontrer que $(X | R)$ est une présentation du groupe $\prod_{i \in I} G_i$.

7) Soit X un ensemble équipotent à \mathbb{N} ; on pose $X = \{x_n\}_{n \in \mathbb{N}}$.

a) Le groupe additif des nombres rationnels, $(\mathbb{Q}, +)$, étant engendré par $\left\{ \frac{1}{n!}, n \in \mathbb{N} \right\}$ (exercice 8, chap. III), démontrer que $(X | x_{n+1}^{n+1} x_n^{-1}; n \in \mathbb{N})$ est une présentation de $(\mathbb{Q}, +)$.

b) p étant un nombre premier, soit \mathbb{Q}_p le sous-groupe de $(\mathbb{Q}, +)$ engendré par $\left\{ \frac{1}{p^n}; n \in \mathbb{N} \right\}$ (exercice 10, chap. I).

Montrer que $(X | x_{n+1}^p x_n^{-1}; n \in \mathbb{N})$ est une présentation de \mathbb{Q}_p .

c) Soit $\left(\frac{\mathbb{Q}}{\mathbb{Z}} \right)_p$ la composante p -primaire du groupe additif $\frac{\mathbb{Q}}{\mathbb{Z}}$.
 $\left[\left(\frac{\mathbb{Q}}{\mathbb{Z}} \right)_p \text{ est isomorphe à } C_{p^\infty} : \text{voir exercice 3, chap. VIII.} \right]$

Prouver que $\left(\frac{\mathbb{Q}}{\mathbb{Z}} \right)_p$ a pour présentation :

$$(X | x_0, x_{n+1}^p x_n^{-1}; n \in \mathbb{N}).$$

8) a) Montrer que le groupe diédral infini D_∞ (exercice 31, chap. III et exercice 35, chap. IV) a pour présentation :

$$(\{a, b\} | b^2, (ab)^2).$$

b) En déterminant une autre présentation de D_∞ , prouver, à l'aide de l'exercice 6 ci-dessus, que l'on a $D_\infty \simeq C_2 \sqcup C_2$, où C_2 désigne un groupe cyclique d'ordre 2.

9) Soit $S_2(\mathbb{Z})$ le groupe multiplicatif des matrices de $M_2(\mathbb{Z})$, dont le déterminant est 1.

a) Soient $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

Vérifier que A et B sont d'ordre fini dans $S_2(\mathbb{Z})$, mais que AB et BA sont d'ordre infini.

b) Montrer que toute matrice $X \in S_2(\mathbb{Z})$ dont un élément est nul dans la première, ou dans la seconde colonne, appartient au sous-groupe $\langle A, B \rangle$ de $S_2(\mathbb{Z})$, engendré par A et B .

c) Le but de cette question est de prouver que le groupe $S_2(\mathbb{Z})$ est engendré par A et B .

On suppose $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $S_2(\mathbb{Z})$ telle que $X \notin \langle A, B \rangle$.

On suppose de plus que, parmi les matrices de $S_2(\mathbb{Z})$ n'appartenant pas à $\langle A, B \rangle$, X est telle que $|a| + |c|$ est minimal.

Si $|a| \geq |c|$, montrer qu'il existe $r \in \mathbb{Z}$, tel que $|a + rc| < |a|$ et si $|a| < |c|$, vérifier qu'il existe $s \in \mathbb{Z}$, tel que $|sa + c| < |c|$.

En calculant, respectivement, dans chacun des deux cas précédents :

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} X \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} X.$$

Montrer que l'on obtient une contradiction avec la minimalité de $|a| + |c|$; en conclure que $S_2(\mathbb{Z}) = \langle A, B \rangle$.

d) Montrer que le centre du groupe $S_2(\mathbb{Z})$ est $\{I, -I\}$ où I est la matrice unité de $S_2(\mathbb{Z})$.

e) Soit $P_2(\mathbb{Z}) = \frac{S_2(\mathbb{Z})}{\{I, -I\}}$. Démontrer que $(\{\alpha, \beta\} \mid \alpha^2, \beta^2)$ est une représentation du groupe $P_2(\mathbb{Z})$.

En déduire que l'on a $P_2(\mathbb{Z}) \simeq C_2 \sqcup C_3$, où C_2 et C_3 désignent, respectivement, des groupes cycliques d'ordre 2 et 3 (voir l'exercice 6 ci-dessus).

10) Soit $G = \coprod_{i \in I} G_i$, $\text{card } I > 1$. On pose $D(G) = G'$ et, pour tout $i \in I$, $D(G_i) = G'_i$.

a) Démontrer que l'on a $\frac{G}{G'} \simeq \bigoplus_{i \in I} \frac{G_i}{G'_i}$.

b) Retrouver la proposition (9.22), à l'aide du résultat précédent et de la proposition (9.49).

11) a) Soient G un groupe et $K \triangleleft G$. Démontrer que, si $\frac{G}{K}$ est un groupe libre, alors G contient un sous-groupe H isomorphe à $\frac{G}{K}$, tel que G est produit semi-direct de K par H (définition (5.45)).

b) Soit F un groupe. On suppose que, quels que soient le groupe G et le sous-groupe $K \triangleleft G$ tels que $\frac{G}{K} \simeq F$, G est produit semi-direct de K par un sous-groupe $H \simeq F$.

Démontrer que F est libre.

- 12) *a)* Démontrer que pour tout groupe libre F , tel que $\text{rang}(F) > 1$, $D(F)$ est un groupe libre de rang infini.

[On pourra utiliser le théorème (9.39) et l'exercice précédent.]

b) Prouver que tout groupe libre F tel que $\text{rang}(F) > 1$ est non résoluble.

RÉFÉRENCES BIBLIOGRAPHIQUES

- [1] Arnaudies J.-M., *Les cinq polyèdres réguliers de \mathbf{R}^3 et leurs groupes*, Centre de Documentation universitaire et SEDES réunis, 1969.
- [2] Artin E., *Algèbre géométrique*, Bordas 1978.
- [3] Aschbacher M., The classification of the finite simple groups, *The Mathematical Intelligencer*, Springer-Verlag, vol. 3, n° 2, 1981, p. 59-65.
- [4] Auslander M., Buchsbaum D., *Groups, Rings, Modules*, Harper & Row, 1974.
- [5] Baumslag G., Chandler, B., *Group Theory*, Schaum's outline series, McGraw-Hill, 1968.
- [6] Berger M., *Géométrie : 1 | Action de groupes, espaces affines et projectifs*, CEDIC/Fernand Nathan, 1977.
- [7] Biggs N., *Finite Groups of Automorphisms*, Cambridge University Press, 1971.
- [8a] Bourbaki N., *Algèbre*, chap. 1 à 3, Hermann, 1970.
- [8b] Bourbaki N., *Théorie des ensembles*, Hermann, 1970.
- [9] Budden F.-J., *La fascination des groupes*, OEDL, 1976.
- [10] Burnside W., *Theory of groups of finite order*, 2^e éd., Cambridge, 1911 (Dover, 1955).
- [11] Charles B., *Algèbre générale*, PUF, 1983.
- [12] Chevalley C., Sur certains groupes simples, *Tôhoku Math.* (2), 7, 1955, p. 14-66.
- [13] Chih-Han Sah, *Abstract algebra*, Academic Press, 1967.
- [14] Choquet G., *L'enseignement de la géométrie*, Hermann, 1964.
- [15] Cohn P. M., *Algebra*, vol. 1, John Wiley & Sons, 1974.
- [16] Comtet L., *Analyse combinatoire* (t. I et II), PUF, 1970.
- [17] Conway J. H., Monsters and Moonshine, *The Mathematical Intelligencer*, Springer-Verlag, vol. 2, n° 4, 1980, p. 165-171.
- [18] Coxeter H. S. M., *Regular complex polytopes*, Cambridge University Press, 1974.
- [19] Deheuvels R., *Formes quadratiques et groupes classiques*, PUF, 1981.
- [20] Denes J., Keedwell A. B., *Latin squares*, Academic Press, 1974.
- [21] Dickson L. E., *Linear groups with an exposition of the Galois field theory*, Teubner, 1901 (Dover, 1958).
- [22] Dieudonné J., *Sur les groupes classiques*, Hermann, 1973.
- [23] Dieudonné J., *Algèbre linéaire et géométrie élémentaire*, Hermann, 2^e éd., 1978.

- [24] Dixon J. D., *Problems in Group Theory*, Blaisdell, Publ. Comp., 1967.
- [25] Dixon J. D., *The structure of linear groups*, Van Nostrand Reinhold Comp., 1971.
- [26] Dubreil P., *Algèbre*, t. I : *Equivalences, Opérations, Groupes, Anneaux, Corps*, Gauthier-Villars, 1954.
- [27] Dubreil P., Dubreil-Jacotin M.-L., *Leçons d'algèbre moderne*, Dunod, 1961.
- [28] Exbrayat J.-M., Mazet P., *Algèbre 1*, Hatier, 1971.
- [29] Feit W. and Thomson J. G., Solvability of groups of odd order, *Pacific J. Math.*, 13, 1963, p. 775-1029.
- [30] Fuchs L., *Infinite Abelian groups*, Academic Press, 1970.
- [31] Godement R., *Cours d'algèbre*, Hermann, 1966.
- [32] Gorenstein D., *Finite Groups*, Harper & Row, 1968.
- [33] Gorenstein D., The classification of the finite simple groups, *Bull. AMS*, 1979, p. 43-199.
- [34] Hall F. M., *Abstract Algebra*, vol. 2, Cambridge University Press, 1969.
- [35] Hall M. Jr., *The Theory of Groups*, Mac Millan Comp. (7^e éd.), 1970.
- [36] Hardy G. H. and Wright E. M., *An Introduction to the Theory of Numbers*, Oxford, 1962.
- [37] Hartley B., Hawkes T. O., *Rings, Modules and Linear Algebra*, Chapman & Hall, 1970.
- [38] Heineken H., Mohamed I. J., A group with trivial centre satisfying the normalizer condition, *J. Algebra*, 10, 1968, p. 368-376.
- [39] Herstein I. N., *Topics in Algebra*, Xerox College Publishing, 1964.
- [40] Herstein I. N., *Non commutative rings*, John Wiley & Sons, 1968.
- [41] Jacobson N., *Basic Algebra I*, W. H. Freeman & Comp., 1974.
- [42] Jordan C., *Traité des substitutions et des équations algébriques*, Gauthier-Villars, 1870 (Blanchard, 1957).
- [43] Kochendorffer R., *Introduction to algebra*, Wolters-Noordhoff, 1972.
- [44] Krasner M., *Théorie de Galois*, à paraître aux PUF.
- [45] Kurosh K. A., *The theory of groups*, vol. I et II, Chelsea, 1960.
- [46] Lang S., *Algebra*, Addison-Wesley, 1967.
- [47] Ledermann W., *Introduction to Group Theory*, Longman, 1973.
- [48] Lelong-Ferrand K., Arnaudies J.-M., *Cours de mathématiques*, t. 1 : *Algèbre, MP - Spéciales AA'*, Dunod, 1971.
- [49] Lesieur L., Meyer Y., Joulain C., Lefebvre J., *Algèbre générale*, Armand Colin, coll. « U », 1975.
- [50] Lesieur L., Meyer Y., Joulain C., Lefebvre J., *Algèbre linéaire, Géométrie*, Armand Colin, coll. « U », 1977.
- [51] Lesieur L., Temam R., Lefebvre J., *Compléments d'algèbre linéaire*, Armand Colin, coll. « U », 1978.
- [52] Lyapin E. S., Aizenshtat A. Ya., Lesokhin M. M., *Exercices in group theory*, Plenum Press, 1972.
- [53] Mac Donald I. D., *The theory of group*, Oxford University Press, 1968.
- [54] Mac Lane S., Birkhoff G., *Algèbre*, t. 1 et 2, Gauthier-Villars, 1970 et 1978.
- [55] Malliavin M.-P., *Les groupes finis et leurs représentations complexes*, Masson, 1981.
- [56] Mutafian C., *Le défi algébrique*, t. I et II, Vuibert, 1975.
- [57] Querré J., *Cours d'algèbre*, Masson, 1976.
- [58] Queysanne M., *Algèbre, MP et Spéciales AA'*, Armand Colin, 1964.
- [59] Rado R., A proof of the basis theorem for finitely generated Abelian groups, *J. London Math. Soc.*, 26 (1951), 74-75, 160.

- [60] Ramis E., Deschamps C., Odoux J., *Cours de Mathématiques spéciales*, 1 : *Algèbre*, Masson, 1974.
- [61] Rose J. S., *A course on group theory*, Cambridge University Press, 1978.
- [62] Rotman J. J., *The theory of group*, Allyn & Bacon, 1965.
- [63] Schenkman E., *Group theory*, D. Van Nostrand Comp., 1965.
- [64] Schubert H., *Categories*, Springer-Verlag, 1972.
- [65] Scott W. R., *Group theory*, Prentice-Hall, 1964.
- [66] Serre J.-P., *Représentations linéaires des groupes finis*, Hermann (3^e éd.), 1978.
- [67] Shapiro L. W., *Introduction to Abstract Algebra*, McGraw-Hill, 1975.
- [68] Stewart I., *Galois theory*, Chapman & Hall, 1973.
- [69] Van der Waerden B. L., *Algebra*, vol. 1, Frederick Ungar, 1970.
- [70] Warner S., *Modern Algebra*, vol. 1, Prentice-Hall, 1965.
- [71] Warusfel A., *Structures algébriques finies*, Hachette, 1971.
- [72] Weiner L. M., *Introduction to Modern Algebra*, Harcourt, Brace & World, 1970.
- [73] Weir A. J., The Reidemeister-Schreier and Kurosh subgroup theorems, *Mathematika*, 3 (1956), p. 47-55.
- [74] Weyl H., *The classical group*, Princeton, 1939.
- [75] Wielandt H., Ein Beweis für die Existenz der Sylowgruppen, *Arch. Math.*, 10, 1959, p. 401-402.
- [76] Zassenhaus H., *The theory of group*, Chelsa (2^e éd.), 1958.
- [77] Zassenhaus H., Zum Satz von Jordan-Hölder-Schreier, *Abh. Math. Sem. Univ. Hambourg*, 10, 1934, p. 187-220.

INDEX

anneau, 14.
 automorphisme, 47.
 — intérieur, 48.

 base d'un groupe abélien libre, 278.
 Bezout (théorème de —), 97.
 Burnside (formule de —), 202.

 carré latin, 29.
 Cauchy (théorème de —), 210.
 Cayley (table de —), 27.
 Cayley (théorème de —), 51.
 centralisateur, 17.
 centre d'un groupe, 34.
 classe de congruence, d'équivalence, 23.
 — de conjugaison, 145.
 — double, 85.
 — modulo un sous-groupe, 72.
 classe de nilpotence, 249.
 commutateur, 156.
 complément, 277.
 composante p -primaire, 296.
 coproduit direct, 358.
 corps, 14.
 cycle de longueur r (ou r -cycle), 108.
 cycles disjoints, 111.

 décomposition canonique d'une permutation en un produit de cycles, 112.
 décomposition canonique d'un groupe abélien de type fini, 315.
 demi-groupe, 21.

déplacements du plan, 87.
 diviseurs élémentaires d'un groupe abélien fini, 313.

 élément neutre, 17.
 — simplifiable (à droite, à gauche), 22.
 — superflu, 267.
 — symétrique, symétrisable, 17.
 — unité, 19.
 éléments conjugués, 145.
 — permutables, 19.
 endomorphisme, 41.
 ensemble bien ordonné, 287.
 — ordonné inductif, 162.
 — quotient, 24.
 entiers congrus modulo n , 24.
 épimorphisme, 52.
 équation aux classes, 184.
 Euler (fonction d'—), 99.

 facteur direct, 277.
 famille génératrice libre, 337.
 — libre sur Z , 279.
 forme réduite d'un mot, 234-358.
 formule des indices, 78.
 Frattini (lemme de —), 212.
 (sous-groupe de —), 162.

 Gauss (théorème de —), 102.
 générateurs (ensemble de —), 35.
 générateurs d'un groupe monogène, 98.
 G-ensemble, 175.
 — homogène, 186.

groupe, 18.

- abélien, 19.
 - abélien élémentaire (p -élémentaire), 263.
 - abélien libre, 277.
 - abélien p -primaire, 295.
 - additif, 20.
 - alterné de degré n , 120.
 - caractéristiquement simple, 257.
 - circulaire, 165.
 - classique, 139.
 - commutatif, 19.
 - cyclique, 36.
 - dérivé, 156.
 - dicyclique, 205.
 - diédral de degré n , 120.
 - diédral infini, 135.
 - divisible, 323.
 - hypercyclique, 221.
 - libre, librement engendré, 337.
 - linéaire général, 27.
 - linéaire spécial, 45.
 - linéaire projectif spécial, 139.
 - mixte, 293.
 - monogène, 35.
 - multiplicatif, 19.
 - nilpotent, 244.
 - orthogonal, 45.
 - périodique, 294.
 - p -quasi cyclique, 172.
 - quotient, 137.
 - résoluble, 236.
 - simple, 138.
 - simple classique, 139.
 - simple sporadique, 139.
 - super-résoluble, 264.
 - symétrique, 25.
 - symétrique de degré n , 25.
- groupe opérant sur un ensemble, 175.
- fidèlement, 187.
 - transitivement (intransitivement), 186.
 - k -transitivement, 203.

holomorphe, 195.

homographie, 68.

homomorphisme de groupes, 41.

image d'un morphisme de groupes, 43.

image homomorphe, 43.

indice d'un sous-groupe, 76.

invariants d'un groupe abélien fini, 315.

inverse d'un élément, 19.

inverse d'un produit, 22.

isométrie, 33.

isomorphes (groupes —), 46.

isomorphisme, 45.

1^{er} théorème d'—, 83.

2^e théorème d'—, 153.

3^e théorème d'—, 155.

Jordan-Hölder (suite de —), 229.

(théorème de —), 231.

Klein (groupe de —), 57.

Lagrange (théorème de —), 75.

loi de composition interne, 17.

— associative, 17.

— commutative, 17.

loi quotient, 80.

longueur d'un cycle, 108.

longueur d'une suite de composition, 225.

longueur finie, infinie (groupe de —), 232.

longueur d'un mot, 330.

module (A-module), 269.

monoïde, 21.

— libre, 331.

monomorphisme de groupes, 51.

morphisme de groupes, 41.

— nul, 44.

mot, 330.

— réduit, 334-359.

— vide, 330.

mots adjacents, 331.

— élémentairement équivalents, 357.

— équivalents, 332-358.

normalisateur, 146.

noyau d'un morphisme de groupes, 43.

noyau de l'action d'un groupe sur un ensemble, 176.

opposé (élément), 20.

orbite (G-orbite), 179.

— ponctuelle, 184.

σ -orbite, 107.

- ordre d'un élément, 36.
 - d'un groupe fini, 19.
- partie génératrice, 35.
 - libre, 337.
- permutation, 25.
 - circulaire, 109.
 - paire (impaire), 118.
 - à support fini, 168.
- p -groupe, 295.
 - abélien, 295.
 - fini, 210.
 - de Prüfer, 172.
- Poincaré (théorème de —), 77.
- présentation d'un groupe, 342.
- présentation finie (groupe de —), 345.
- produit de deux éléments, 19.
 - de n éléments, 20.
- produit direct de groupes, 54.
- produit libre de groupes, 358.
- produit semi-direct de sous-groupes, 191.
 - de groupes, 192.
- propriété universelle d'un groupe abélien libre, 284.
 - d'un groupe libre, 338.
 - d'un groupe quotient, 147.
 - d'un produit direct de groupes, 60.
 - d'un produit libre de groupes, 360.
 - d'une somme directe de groupes abéliens, 272.
- quaternions (groupe des —), 27.
- quotient d'une suite de composition, 225.
- Rado (lemme de —), 302.
- raffinement d'une suite de composition, 226.
- rang d'un groupe abélien libre, 282.
 - d'un groupe libre, 345.
- relation d'équivalence compatible avec une loi de composition, 79-80.
- relation de conjugaison, 145.
- représentation matricielle d'un groupe, 66.
 - linéaire d'un groupe, 196.
- rotations, 143.
- Schreier (théorème de —), 227.
- signature d'une permutation, 115.
- similitude, 33.
- simplification (règle de —), 22.
- somme de deux éléments, 19.
 - de sous-groupes, 39.
 - directe de sous-groupes d'un groupe abélien, 39.
- sous-ensemble des points fixes d'un G -ensemble, 187.
- sous-groupe, 29.
 - caractéristique, 157.
 - d'isotropie, 179.
 - distingué, 136.
 - de Frattini, 162.
 - d'un groupe quotient, 150.
 - engendré par une partie d'un groupe, 34.
 - maximal, 159.
 - normal, 136.
 - normal maximal, 159.
 - propre, 30.
 - sous-normal, 254.
 - torsion (de —), 294.
- stabilisateur, 179.
- suite centrale, 243.
 - centrale ascendante, 247.
 - centrale descendante, 245.
- suite de composition, 225.
- suite normale, 237.
 - normale monogène, 264.
- suite principale, 258.
- suites de composition équivalentes, 226.
- support d'un cycle, 108.
 - d'une permutation, 106.
- Sylow (p -sous-groupe de —), 210.
 - (1^{er} théorème de —), 205.
 - (3^e, théorème de —), 210.
- torsion (groupe de —), (groupe sans —), 293.
- translation à gauche (à droite), 50.
- transposition, 109.
- transversale à droite (à gauche), 348.
 - de Schreier, 353.
- type fini (groupe de —), 35.
- Zassenhaus (lemme de —), 227.
- Z -module, 269.
 - injectif, 325.
 - projectif, 292.
- Zorn (axiome de —), 162.

Imprimé en France
Imprimerie des Presses Universitaires de France
73, avenue Ronsard, 41100 Vendôme
Septembre 1984 — N° 29 872

Mouyn