MAT2000 – Algèbre II

Luc Bélair et Christophe Hohlweg

13 décembre 2011

Table des matières

Avant-propos **4**

Alphabet grec **5**

0 Rappels sur les fonctions injectives, surjectives, bijectives **7**

1 Structure de groupes **9**

1.1 Loi de composition interne, monoïdes et groupes 9

1.1.1 Loi de composition interne 9

1.1.2 Élément neutre et monoïdes 11

1.1.3 Éléments inversibles et groupes 12

1.1.4 Notation additive et multiplicative des groupes 13

1.2 Groupes : premiers exemples et règles de calcul 14

1.2.1 Exemples classiques 14

1.2.2 Table d'un groupe 16

1.2.3 Règles de calcul 17

1.3 Sous-groupes 18

1.3.1 Sous-groupes engendrés 19

1.3.2 Ordre d'un groupe, ordre d'un élément de groupe 21

1.3.3 Groupe fini et générateurs 24

1.4 Récapitulatif, questions et nouveaux exemples 24

1.4.1 Le groupe $(\mathbb{Z}, +)$ 24

1.4.2 Les groupes $(\mathbb{Z}/n\mathbb{Z},+)$ 25

1.4.3 Le groupe symétrique S_n 26

1.4.4 Les groupes diédraux 30

1.4.5 Générateurs et ordre de D_m 31

1.4.6 Conclusion 32

2 Morphismes de groupes **33**
2.1 Noyau d'un morphisme de groupes . . . 34
2.2 Composition de morphismes de groupes . . . 35
2.3 Isomorphisme de groupes . . . 35
2.4 Automorphismes intérieurs . . . 36
2.5 Groupes symétriques et théorème de Cayley . . . 37

3 Classe modulo un sous-groupe et groupes quotients **39**
3.1 Classes modulo un sous-groupe . . . 39
3.1.1 Le théorème de Lagrange . . . 41
3.1.2 Application à l'arithmétique modulaire . . . 42
3.2 Groupes quotients . . . 44
3.2.1 Sous-groupes normaux . . . 44
3.2.2 Groupe quotient . . . 45
3.2.3 Premier théorème d'isomorphisme . . . 47
3.2.4 Sous-groupes d'un groupe quotient . . . 48
3.3 Applications . . . 49
3.3.1 Groupes monogènes et cycliques . . . 49

4 Les produits directs de groupes **51**
4.1 Le produit direct externe . . . 51
4.2 Quelques isomorphismes . . . 53
4.3 Le produit direct interne . . . 54

5 La structure des groupes abéliens finis **57**
5.1 Les groupes cycliques . . . 57
5.2 Les groupes abéliens primaires . . . 58
5.3 La décomposition primaire . . . 59
5.4 La décomposition des groupes primaires . . . 61
5.5 Le théorème principal . . . 63

6 Les actions de groupes **67**
6.1 Les groupes qui opèrent sur les ensembles . . . 67
6.2 Orbites vs stabilisateurs . . . 71
6.3 Les théorèmes de Sylow . . . 73
6.4 Le groupe des isométries du cube . . . 75

7 Exercices **79**
7.1 Structure de groupes . . . 79
7.1.1 . . . 79

7.1.2 . . . 79
7.1.3 . . . 79
7.1.4 . . . 79
7.1.5 . . . 80
7.1.6 . . . 80
7.1.7 . . . 80
7.1.8 . . . 80
7.1.9 . . . 81
7.1.10 . . . 81
7.1.11 . . . 81
7.1.12 . . . 81
7.1.13 . . . 81
7.1.14 . . . 81
7.1.15 . . . 82
7.1.16 . . . 82
7.1.17 . . . 82
7.1.18 . . . 82
7.1.19 . . . 82
7.1.20 . . . 82
7.1.21 . . . 83
7.1.22 . . . 83
7.1.23 . . . 83
7.1.24 . . . 83
7.1.25 . . . 84
7.1.26 . . . 84
7.1.27 . . . 84
7.1.28 . . . 84
7.1.29 . . . 84
7.1.30 . . . 85
7.1.31 . . . 85
7.1.32 . . . 85
7.1.33 . . . 85
7.2 Morphismes de groupes . . . 85
7.2.1 . . . 85
7.2.2 . . . 85
7.2.3 . . . 86
7.2.4 . . . 86
7.2.5 . . . 86
7.2.6 . . . 86
7.2.7 . . . 87

7.2.8 . . . 87
7.3 Classe modulo un sous-groupe et groupes quotients . . . 87
7.3.1 . . . 87
7.3.2 . . . 87
7.3.3 . . . 87
7.3.4 . . . 88
7.3.5 . . . 88
7.3.6 . . . 88
7.3.7 . . . 88
7.3.8 . . . 88
7.3.9 . . . 89
7.3.10 . . . 89
7.3.11 . . . 89
7.3.12 . . . 89
7.3.13 . . . 89
7.3.14 . . . 90
7.3.15 . . . 90
7.3.16 . . . 90
7.3.17 . . . 90
7.3.18 . . . 90
7.3.19 . . . 90
7.3.20 . . . 91
7.3.21 . . . 91
7.3.22 . . . 91
7.3.23 . . . 91
7.3.24 . . . 91
7.3.25 . . . 91
7.4 Les produits directs de groupes . . . 92
7.4.1 . . . 92
7.4.2 . . . 92
7.4.3 . . . 92
7.4.4 . . . 92
7.4.5 . . . 92
7.4.6 . . . 93
7.5 La structure des groupes abéliens finis . . . 93
7.5.1 . . . 93
7.5.2 . . . 93
7.5.3 . . . 93
7.5.4 . . . 93
7.5.5 . . . 93

7.5.6 . . . 93
7.5.7 . . . 94
7.6 Les actions de groupes . . . 94
7.6.1 . . . 94
7.6.2 . . . 94
7.6.3 . . . 94
7.6.4 . . . 94
7.6.5 . . . 95
7.6.6 . . . 95
7.6.7 . . . 95
7.6.8 . . . 96
7.6.9 . . . 96
7.6.10 . . . 96
7.6.11 . . . 96
7.6.12 . . . 97
7.6.13 . . . 97
7.6.14 . . . 97
7.6.15 . . . 97
7.6.16 . . . 97
7.6.17 . . . 97
7.6.18 . . . 98
7.6.19 . . . 98
7.6.20 . . . 98
7.7 Exercices supplémentaires . . . 98
7.7.1 . . . 98
7.7.2 . . . 99
7.7.3 . . . 99
7.7.4 . . . 99
7.7.5 . . . 99
7.7.6 . . . 100
7.7.7 . . . 100

8 Solutions **101**
8.4 Les produits directs de groupes . . . 101
8.4.5 . . . 101
8.5 La structure des groupes abéliens finis . . . 102
8.5.2 . . . 102
8.5.3 . . . 103
8.5.4 . . . 104
8.6 Les actions de groupes . . . 104

8.6.1 . . . 104
8.6.2 . . . 105
8.6.3 . . . 106
8.6.4 . . . 107
8.6.6 . . . 110
8.6.7 . . . 110
8.6.8 . . . 111
8.6.9 . . . 111
8.6.10 . . . 113
8.6.11 . . . 114
8.6.12 . . . 115
8.6.13 . . . 116
8.6.15 . . . 116
8.6.17 . . . 117
8.7 Exercices supplémentaires . . . 117
8.7.1 . . . 117
8.7.2 . . . 121
8.7.3 . . . 123
8.7.4 . . . 123
8.7.6 . . . 125
8.7.7 . . . 127

Avant-propos

Ce recueil est une première version. Nous avons rassemblé des notes de cours que nous avions déjà rédigées chacun de notre côté. Nous remercions Yannick Vargas pour avoir effectué un premier travail d'harmonisation.

Nous remercions d'avance les personnes qui prendront la peine de nous signaler les erreurs de toute nature. Nous apprécions aussi tous les commentaires ; ils contribueront à améliorer les prochaines versions.

Luc Bélair et Christophe Hohlweg
Automne 2011

Alphabet grec

Α α	a	alpha	Ν ν	n	nu
Β β	b	bêta	Ξ ξ	ks	xi
Γ γ	g	gamma	Ο ο	o	omicron
Δ δ	d	delta	Π π	p	pi
Ε ε	e	epsilon	Ρ ρ	r	rhô
Ζ ζ	dz	dzéta	Σ σ	s	sigma
Η η	e	êta	Τ τ	t	tau
Θ θ	t	aspiré : thêta	Υ υ	u	upsilon
Ι ι	i	iota	Φ φ	p	aspiré : phi
Κ κ	k	kappa	Χ χ	k	aspiré : khi
Λ λ	l	lambda	Ψ ψ	ps	psi
Μ μ	m	mu	Ω ω	o	oméga

Chapitre 0

Rappels sur les fonctions injectives, surjectives, bijectives

Définition 0.1. *Soient des ensembles X, Y et une fonction $f : X \to Y$. Soient $x \in X$ et $y \in Y$.*

(1) On dit que x est un antécédent de y pour la fonction f, *exactement quand $f(x) = y$.*

(2) On dit que f est injective *si tout élément de Y a* au plus un *antécédent par f.*

(3) On dit que f est surjective *si tout élément de Y a* au moins un *antécédent par f.*

Notation. On désigne parfois par $f^*(y)$ l'ensemble de tous les antécédents de y par f, et si $B \subseteq Y$ on désigne parfois par $f^*(B)$ l'ensemble de tous les antécédents par f de tous les éléments de B.

Exemple 0.2. *Soit la fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = 2^x$. Cette fonction est injective. En effet, considérons $y \in \mathbb{R}$, et soient a, b deux antécédents possibles de y, c.-à-d. $2^a = y$ et $2^b = y$. Mais alors $2^a = 2^b$, d'où $a = b$, et donc y ne peut avoir au plus qu'un antécédent par f, tel que voulu. Cette fonction n'est pas surjective. En effet, $0 \in \mathbb{R}$ mais 0 n'a pas d'antécédent par f puisque l'équation $2^x = 0$ n'a pas de solution.*

Exemple 0.3. *Soit la fonction $f : \mathbb{C} \to \mathbb{R}$ définie par $f(a + bi) = a$. Cette fonction est surjective. En effet, soit $r \in \mathbb{R}$ alors, par exemple, $r + i$ est un antécédent de r par f puisque $f(r + i) = r$. Cette fonction n'est pas injective. En effet, par exemple, $1 \in \mathbb{R}$ a comme antécédents $1 + i$ et $1 + (0, 5)i$ et ils sont différents.*

Exemple 0.4. *Soit la fonction $f : \mathbb{R} \to \mathbb{N}$ définie par $f(x) =$ la 1^{re} décimale de x. Cette fonction n'est pas injective puisque, par exemple, $0 \in \mathbb{N}$ a comme antécédents 1 et $1/100$ et qu'ils sont différents. Cette fonction n'est pas surjective puisque, par exemple, $33 \in \mathbb{N}$ mais 33 n'a pas d'antécédent.*

Définition 0.5. *Une fonction qui établit une correspondance exacte entre les éléments de deux ensembles est appelée une* bijection *ou* fonction bijective.

Proposition 0.6. *Une fonction est bijective si et seulement si elle est à la fois injective et surjective.*

En effet, une fonction $f : X \to Y$ établit une correspondance exacte entre les éléments de X et les éléments de Y précisément quand tout élément de Y a exactement un antécédent par f, et cela se produit exactement quand f est à la fois injective et surjective, par définition de chacune des propriétés.

On désigne par Id_X la fonction identité $Id_X : X \to X$ définie par $Id_X(x) = x$.

Proposition 0.7. *Une fonction $f : X \to Y$ est bijective si et seulement si il existe une fonction $g : Y \to X$ telle que $f \circ g = Id_Y$ et $g \circ f = Id_X$.*

En effet, si f est bijective on prend la fonction $g : Y \to X$ définie par $g(x) =$ l'unique antécédent de y par f. Et si on a un g tel que $f \circ g = Id_Y$ et $g \circ f = Id_X$, alors un $y \in Y$ possède au moins un antécédent par f à savoir $g(y)$ puisque $f(g(y)) = y$, et il en possède au plus un car si x est un (autre) antécédent de y alors $g(y) = g(f(x)) = x$.

Quand une fonction f est bijective, la fonction g de la proposition précédente est nécessairement unique. On l'appelle l'inverse de f et on la note f^{-1}. On dit aussi alors que la fonction f est inversible.

Chapitre 1

Structure de groupes

Nous savons que nous pouvons multiplier et additionner des entiers, mais aussi que l'on peut additionner et multiplier des ensembles classes de congruence modulo un entier fixé. On peut se demander quel est le point commun entre ces opérations, et en particulier, quels résultats sont toujours valides lorsque nous considérons uniquement les propriétés générales de ces lois de calcul. En fait on va introduire ici de nouveaux objets mathématiques qui vont illustrer les propriétés générales de ces opérations, en se détachant du particulier.

1.1 Loi de composition interne, monoïdes et groupes

1.1.1 Loi de composition interne

On va supposer que E est un ensemble non vide dans la suite.

Définition 1.1. *Soit E un ensemble non vide. Toute fonction $* : E \times E \to E$ est appelée* loi de composition interne sur E*. On dit aussi une* loi de composition *ou une* opération binaire *sur E.*

Notation 1. *On note $(E, *)$ l'ensemble E muni de la loi de composition interne*

$$\begin{array}{rcl} * : E \times E & \longrightarrow & E \\ (x, y) & \longmapsto & x * y \end{array}$$

En fait, cela signifie que l'on munit E de la « règle de calcul » donnée par $*$. Comme E est spécifié dans le couple $(E, *)$, on notera souvent simplement $(x, y) \mapsto x * y$.

On pourrait donner un exemple de loi de composition interne maintenant, mais au vu de la généralité de la définition, il est plus intéressant de définir quelques propriétés de ces lois pour restreindre notre champ d'étude.

Définition 1.2. *Soit E un ensemble non vide et $*$ une loi de composition interne sur E. Dans $(E,*)$ la loi $*$ est dite*

1. associative *si $x*(y*z)=(x*y)*z$, pour tout $x,y,z\in E$.*
   La paire $(E,*)$ est alors appelée un demi-groupe.
2. commutative *si $x*y=y*x$ pour tout $x,y\in E$.*

Remarque 1. *Si $*$ est associative dans $(E,*)$, on note $x*y*z$ au lieu de $(x*y)*z=(x*y)*z$. Toutes les lois ne sont pas associatives : il n'y a aucune raison pour que les deux expressions*

$$x\star(y\star z)=x\star f(y,z)=f\big(x,f(y,z)\big)$$
$$(x\star y)\star z=f(x,y)\star z=f\big(f(x,y),z\big)$$

soient en général égales pour la loi de composition interne $f:E\times E\to E$ définie par $(x,y)\mapsto x\star y$.

Exemples 1.

1. *La loi de composition interne $\star:(x,y)\mapsto xy+1$ sur $\mathbb{N}$ n'est pas associative, mais est commutative. En effet :*
   (a) *pour $x,y,z\in\mathbb{N}$, on a $(x\star y)\star z=(xy+1)\star z=(xy+1)z+1=xyz+z+1$ et $x\star(y\star z)=x\star(yz+1)=x(yz+1)=xyz+x+1$. Donc si $x=0$ et $z=1$, on a $(x\star y)\star z=2\neq 1=x\star(y\star z)$;*
   (b) *pour $x,y\in\mathbb{N}$ on a $x\star y=xy+1=yx+1=y\star x$.*
2. *Dans $\mathbb{Z}$, l'addition $+$ et la multiplication $\cdot$ sont commutatives et associatives.*
3. *Soit $n\in\mathbb{N}^*$, alors dans $\mathbb{Z}/n\mathbb{Z}$, $+$ et $\cdot$ sont associatives et commutatives (exercice).*
4. *Dans $\mathcal{M}_n(\mathbb{R})$, l'ensemble des matrices $n\times n$ à coefficients réels, l'addition est une loi associative et commutative tandis que la multiplication est une loi associative mais pas commutative (exercice).*

Définition 1.3. *Soit $*$ une loi de composition sur E et $A\subseteq E$. On dit que A est* stable *pour $*$ si pour tout $x,y\in A$ on a $x*y\in A$. On dit parfois que A* hérite *de la loi de composition de E.*

Autrement dit, A est stable pour $*$ si l'image de la restriction de la fonction $*$ à $A\times A$ est incluse dans A.

Remarque 2.

1. *Dans ce cas, $*$ est aussi une loi de composition interne sur A car la fonction*

$$\begin{array}{rcl} *:A\times A & \longrightarrow & A \\ (x,y) & \longmapsto & x*y \end{array}$$

   est bien définie. On peut donc noter $(A,*)$.

2. *L'associativité est* héréditaire *: si $*$ est associative dans E et A est stable pour $*$, alors $*$ est associative dans A. En effet, l'égalité $x*(y*z)=(x*y)*z$ est vraie pour tout $x,y,z\in E$, donc en particulier pour tout $x,y,z\in A$ sous-ensemble de E.*
3. *La commutativité est* héréditaire *: si $*$ est commutative dans E et A est stable pour $*$, alors $*$ est commutative dans A (même argument que pour l'associativité).*

Exemple 1.4. *$\mathbb{Z}^*$ est stable pour la multiplication, mais $\mathbb{Z}^*$ n'est pas stable pour l'addition, car*

$$1+(-1)=0\notin\mathbb{Z}^*.$$

1.1.2 Élément neutre et monoïdes

Chacun sait que la place de 1 pour la multiplication et de 0 pour l'addition est de la première importance : ils sont les éléments neutres de ces lois.

Définition 1.5. *Soit E un ensemble non vide et $*$ une loi de composition interne sur E.*

1. *On dit que $(E,*)$ possède un* élément neutre *si il existe $e\in E$ tel que $x*e=e*x=x$, pour tout $x\in E$.*
2. *On dit que $(E,*)$ est un* monoïde *si $*$ est associative et si $(E,*)$ possède un élément neutre.*
3. *Un monoïde $(E,*)$ est un* monoïde commutatif *si $*$ est commutative dans E.*

Remarque 3. *Si $(E,*)$ possède un élément neutre e, alors*

1. *l'élément neutre e est unique : en effet, soit e' un élément neutre alors $e=e*e'=e'*e=e'$.*
2. *Si $A\subseteq E$ est stable pour $*$, $(A,*)$ posséde un élément neutre si et seulement si $e\in A$. De plus, dans ce cas, e est l'élément neutre de $(A,*)$.*

Exemples 2.

1. *$(\mathbb{N},+)$ est un monoïde commutatif dont l'élément neutre est $e=0$.*
2. *$(\mathbb{N},\cdot)$ est un monoïde commutatif dont l'élément neutre est $e=1$.*
3. *$(\mathbb{N}^*,+)$ n'est pas un monoïde car $0\notin\mathbb{N}^*$ et 0 est l'unique élément neutre dans $(\mathbb{N},+)$.*
4. *$(\mathcal{M}_n(\mathbb{R}),\cdot)$, l'ensemble des matrices carrées $n\times n$ muni de la multiplication des matrices, est un monoïde non commutatif, l'élément neutre étant la matrice identité I_n.*

1.1.3 Éléments inversibles et groupes

En dernière instance, que dire de la division qui est associée à la multiplication et de la soustraction qui est associée à l'addition ? En fait, ces deux notions sont la manifestation de la multiplication par l'inverse d'un élément dans le cas de la multiplication, et de l'addition par l'opposé d'un élément dans le cas de l'addition. Ces notions nous amènent à la définition suivante.

Définition 1.6. *Soit E un ensemble non vide et $*$ une loi de composition interne sur E et munie d'un élément neutre e.*

1. *On dit que $x \in E$ est* inversible *(ou* symétrisable*) dans $(E, *)$ si il existe $y \in E$ tel que $x * y = y * x = e$.*
2. *On dit que $(E, *)$ est* un groupe *si $(E, *)$ est un monoïde et si tous les éléments de E sont inversibles.*
3. *Un groupe $(E, *)$ est un* groupe abélien [1]*, ou* commutatif*, si $*$ est commutative dans E.*

Exemple 1.7. *$(\mathbb{Z}, +)$ est un groupe abélien. Par contre, le monoïde $(\mathbb{Z}^*, \cdot)$ n'est pas un groupe car les seuls éléments inversibles de $\mathbb{Z}$ sont 1 et -1.*

Remarque 4. *La définition de groupe ci-dessus est redondante, on peut la simplifier. Dans la pratique, on préfère utiliser la définition de groupe réécrite comme suit : $(G, *)$ est un groupe si et seulement si*

(i) *$*$ est associative ;*

(ii) *il existe $e \in G$ tel que pour tout $x \in G$ $e * x = x$;* *(* élément neutre à gauche*) ;*

(iii) *pour tout $x \in G$ il existe $y \in G$ tel que $y * x = e$.* *(* élément inversible à gauche*).*

L'implication directe est une conséquence immédiate des définitions. Supposons maintenant que $(G, *)$ vérifie les trois conditions susmentionnées. Donc $*$ est associative. Il reste alors à montrer que $(G, *)$ possède un élément neutre et que tout élément de G est inversible.
Montrons que tout élément de G est inversible : soit $x \in G$, alors il existe $y \in G$ tel que $y * x = e$. Il reste à montrer que $x * y = e$. Comme $y \in G$, il existe également $z \in G$ tel que $z * y = e$. D'où

$$x * y = e * (x * y) = (z * y) * (x * y) = z * (y * x) * y = z * e * y = z * y = e.$$

Montrons que e est l'élément neutre : soit $x \in G$, alors il existe $y \in G$ tel que $y * x = x * y = e$. Donc

$$x * e = x * (y * x) = (x * y) * x = e * x = e.$$

1. Du mathématicien norvégien Niels H. Abel (1802-1829).

Monoïdes et groupes : Soit $(E, *)$ un monoïde dont l'élément neutre est noté e.

1. L'inverse d'un élément, si il existe, est unique : soit $x \in E$ et $y, y' \in E$ deux inverses, alors $y = y * e = y * (x * y') = (y * x) * y' = e * y' = y'$.
2. De ce fait, si $x \in E$ est inversible tel que $y * x = x * y = e$, on dit que y *est l'inverse de* x et on le note $\widetilde{x}$. De plus, $\widetilde{\widetilde{x}} = x$ et $\widetilde{e} = e$ (exercice).
3. On note l'ensemble des éléments inversibles de E

$$E^\times = \{x \in E \,|\, x \text{ est inversible}\}.$$

Proposition 1.8. *$(E^\times, *)$ est un groupe dont l'élément neutre est e. De plus, $\widetilde{x * y} = \widetilde{y} * \widetilde{x}$.*

Démonstration. Il faut montrer que
(i) $*$ est une loi de composition interne sur $E^\times$; en d'autres termes, que $E^\times$ est stable pour $*$;
(ii) $(E, *)$ est un monoïde d'élément neutre e ;
(iii) Tout élément de $E^\times$ est inversible.

Montrons (i) : il suffit de montrer que si x, y sont inversibles dans E alors $x * y$ est inversible dans E. On a

$$(\widetilde{x * y}) * (x * y) = \widetilde{y} * \widetilde{x} * x * y = e = x * y * \widetilde{y} * \widetilde{x} = (x * y) * (\widetilde{x * y})$$

Donc $x * y$ est inversible et son inverse est $\widetilde{y} * \widetilde{x}$. En particulier, comme $\widetilde{x * y}$ est aussi inversible dans $E^\times$ (d'inverse $x * y$), tout élément de $E^\times$ est inversible, ce qui montre (iii).
Montrons (ii) : on sait que $E^\times$ est stable pour $*$ donc par hérédité, $*$ est associative sur $E^\times$. Puisque $\widetilde{e} = e$ car $e * e = e$, alors $e \in E^\times$ et donc $(E^\times, *)$ est un monoïde. □

4. On peut dire alors qu'un monoïde $(E, *)$ est un groupe si et seulement si $E = E^\times$.

1.1.4 Notation additive et multiplicative des groupes

Attention, de nombreux problèmes de compréhension en théorie des groupes viennent de la méconnaissance des **conventions** suivantes.

Notation multiplicative : Sauf mention contraire, on notera les lois de groupes *multiplicativement* : $(x, y) \mapsto xy$, et on dira que ce sont des *produits*. De plus :
- on dira « Soit G un groupe » au lieu de « Soit $(G, \cdot)$ un groupe » ;
- on notera $x^{-1} = \widetilde{x}$ l'inverse de $x \in G$;
- l'élément neutre sera noté 1 ou 1_G.

Notation additive : Lorsque le groupe $(G, *)$ est un groupe abélien, on notera souvent sa loi additivement : $(x, y) \mapsto x + y$ (c'est à dire $+ = *$), et on dira que ce sont des *sommes*. De plus :
- on dira « Soit G un groupe abélien noté additivement » au lieu de « Soit $(G, +)$ un groupe » ;
- on notera $-x = \widetilde{x}$ l'inverse de $x \in G$, qui dans ce cas est appelé *l'opposé de* x ;
- l'élément neutre sera noté 0 ou 0_G.

1.2 Groupes : premiers exemples et règles de calcul

1.2.1 Exemples classiques

L'addition sur les réels : *L'addition des réels* $(a, b) \mapsto a + b$ est une loi de composition interne sur $\mathbb{R}$: $(\mathbb{R}, +)$ est un groupe abélien d'élément neutre 0. De plus, on sait que

1. $(\mathbb{N}, +)$, $(\mathbb{Z}^-, +)$, $(\mathbb{Q}^+, +)$, $(\mathbb{R}^-, +)$ et $(\mathbb{R}^+, +)$ sont des monoïdes commutatifs : ces sous-ensembles sont stables pour $+$, ils héritent alors de l'associativité et de la commutativité. Mais tous leurs éléments ne sont pas inversibles. Par exemple, l'opposé (l'inverse) de 2 n'existe pas, ni dans $(\mathbb{N}, +)$, ni $(\mathbb{Q}^+, +)$, ni dans $(\mathbb{R}^+, +)$;
2. $(\mathbb{Z}, +)$ est un groupe : il est clair que c'est un monoïde, et que tous ses éléments ont des opposés (i.e. sont inversibles) dans $\mathbb{Z}$ pour l'addition (attention, ce n'est pas vrai pour la multiplication) ;
3. $\mathbb{Z}^*$ n'est pas stable pour $+$: en effet, $1 + (-1) = 0 \notin \mathbb{Z}^*$;
4. pour $n \in \mathbb{N}^*$, on constate aussi que $(n\mathbb{Z}, +)$ est un groupe : on peut vérifier directement que $n\mathbb{Z}$ est stable pour l'addition. De plus, $0 \in n\mathbb{Z}$ donc $(n\mathbb{Z}, +)$ est un monoïde, et enfin, $nk \in n\mathbb{Z}$ est inversible dans $n\mathbb{Z}$ car son opposé est $n(-k) \in (n\mathbb{Z}, +)$.

La multiplication sur les réels : *La multiplication des réels* $(a, b) \mapsto ab$ est une loi de composition interne sur $\mathbb{R}$: $(\mathbb{R}, \cdot)$ est un monoïde commutatif. Par ailleurs, puisque $\mathbb{R}^\times = \mathbb{R}^*$, alors $(\mathbb{R}^*, \cdot)$ est un groupe abélien d'élément neutre 1. De plus, on sait que

1. $(\mathbb{N}^*, \cdot)$ et $(\mathbb{Z}^*, \cdot)$ sont des monoïdes commutatifs : ces sous-ensembles sont stables pour $\cdot$, ils héritent alors de l'associativité et de la commutativité. Mais tous leurs éléments ne sont pas inversibles. Par exemple, l'inverse de 2 n'existe pas, ni dans $\mathbb{N}$, ni dans $\mathbb{Z}$;
2. $(\mathbb{Q}^*, \cdot)$ est un groupe : il est clair que c'est un monoïde, et que tous ses éléments sont inversibles dans $\mathbb{Q}^*$ pour la multiplication (attention, $(\mathbb{Q}, \cdot)$ n'est pas un groupe mais seulement un monoïde car 0 n'est pas inversible pour la multiplication) ;
3. $\mathbb{Z}^-$ n'est pas stable pour $\cdot$: en effet, le produit de deux nombres négatifs est positif ;
4. pour $n \in \mathbb{N}^*$, on sait que $(n\mathbb{Z}, \cdot)$ est un monoïde si et seulement si $n = 1$: on vérifie directement que $n\mathbb{Z}$ est stable pour la multiplication. De plus, $1 \in n\mathbb{Z}$ si et seulement si $n = 1$.

En algèbre linéaire : Tout espace vectoriel est un groupe abélien pour l'addition des vecteurs (exercice). De plus, pour $n \in \mathbb{N}$ on constate que

1. $(\mathcal{M}_n(\mathbb{R}), +)$ est un groupe abélien ;
2. $(\mathcal{M}_n(\mathbb{R}), \cdot)$ est un monoïde (non commutatif) dont l'élément neutre est la matrice identité I_n.
3. Dans $(\mathcal{M}_n(\mathbb{R}), \cdot)$, l'ensemble des inversibles est

$$\mathrm{GL}_n(\mathbb{R}) = (\mathcal{M}_n(\mathbb{R}))^\times = \{M \in \mathcal{M}_n(\mathbb{R}) \,|\, \det(M) \neq 0\}.$$

Donc en vertu de la proposition 1.8, $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ est un groupe. On l'appelle le *groupe linéaire*. Il est non abélien si $n > 1$. De plus, $(AB)^{-1} = B^{-1}A^{-1}$ (attention, ici l'ordre de multiplication est important car la loi de composition n'est pas commutative).

Les ensembles quotients $\mathbb{Z}/n\mathbb{Z}$

1. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.
2. $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ est un monoïde commutatif, mais pas un groupe.
3. $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe abélien.

On invite le lecteur à vérifier ces propositions en exercice.

Fonctions et bijections : Soit E un ensemble non vide et $\mathcal{F}(E)$ l'ensemble des fonctions sur E.

Proposition 1.9. *$(\mathcal{F}(E), \circ)$ est un monoïde (non commutatif en général).*

Démonstration. On sait que $\circ$ est une loi de composition associative sur $\mathcal{F}(E)$ (exercice). Aussi, la fonction Id_E est l'élément neutre dans $(\mathcal{F}(E), \circ)$ qui est, de ce fait, un monoïde. □

Notons S_E l'ensemble des bijections sur E. C'est-à-dire, $S_E = (\mathcal{F}(E))^\times$. On a le résultat suivant :

Proposition 1.10. *$(S_E, \circ)$ est un groupe appelé* groupe symétrique *ou* groupe des permutations de l'ensemble *E.*

Remarque 5.

1. *Si $E = \{1 \ldots, n\}$ on note traditionnellement S_E par S_n. Ses éléments sont représentés par des matrices $2 \times n$: si $\sigma \in S_n$, on note*

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

ou, plus simplement, $\sigma(1)\sigma(2)\ldots\sigma(n)$.

2. *Les groupes symétriques sont fondamentaux en mathématiques, nous les étudierons en détails dans ce cours.*

3. *Soit E un espace vectoriel, alors l'ensemble des applications linéaires bijectives sur E, noté* $\mathrm{GL}(E)$*, est un sous-ensemble de S_E. Comme la composée d'applications linéaires est linéaire, on peut montrer que* $(\mathrm{GL}(E), \circ)$ *est un groupe appelé* groupe linéaire sur E*. On verra plus tard, avec la notion* d'isomorphisme de groupes*, que c'est le "même" groupe que* $\mathrm{GL}_n(\mathbb{R})$ *si E est un espace vectoriel réel de dimension n.*

1.2.2 Table d'un groupe

On peut représenter un monoïde, ou un groupe, par sa *table de multiplication* : c'est une matrice (qui peut être infinie) telle que chaque ligne et chaque colonne est indexé par un élément ; à l'intersection de la ligne x et de la colonne y, on met le produit de x par y.

Exemple 1.11. *Soit $E = \{1, 2, 3\}$, alors les éléments de S_3 sont*

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 123 \qquad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = 213 \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = 132$$

$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = 321 \qquad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = 231 \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = 312.$$

Le produit de σ_1 avec τ_2 est

$$\sigma_1 \circ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \sigma_1(\tau_2(1)) & \sigma_1(\tau_2(2)) & \sigma_1(\tau_2(3)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_1.$$

La table de multiplication de S_3 est

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

.

On remarque que S_3 n'est pas abélien car $\tau_1 \circ \tau_2 \neq \tau_2 \circ \tau_1$. On peut clairement voir dans la table de multiplication les inverses de chaque élément : l'inverse de l'élément x est y si l'intersection de la ligne x avec la colonne y est e.

1.2.3 Règles de calcul

Soit G un groupe.

Inverse du produit d'éléments : On a déjà vu plus haut que si $x, y \in G$ alors $(xy)^{-1} = y^{-1}x^{-1}$. Plus généralement, si $x = x_1 x_2 \dots x_n \in G$ alors $x^{-1} = x_n^1 \dots x_2^{-1} x_1^{-1}$.
Attention, comme le groupe n'est pas forcément abélien, $(xy)^{-1} = y^{-1}x^{-1} \neq x^{-1}y^{-1} = (yx)^{-1}$ en général. En effet, sinon $xy = yx$ car $(x^{-1})^{-1} = x$.

Exemple 1.12. *On prend dans* $\mathrm{GL}_2(\mathbb{R})$ *les matrices*

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

Alors

$$xy = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \neq yx = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}.$$

De surcroît, leurs inverses ne peuvent être égaux.

Remarque 6. *Par contre, si G est un groupe abélien noté additivement, il faut savoir que l'opposé de $x + y$ est $-x - y = -y - x$.*

Puissance d'éléments : Soit $x \in G$ et $n, m \in \mathbb{N}$ alors l'associativité de l'opération du groupe G permet de définir le produit x^n comme suit

$$x^n = x^{n-1}x = \underbrace{xx \cdots x}_{n \ fois}.$$

Par convention, $x^0 = e$. En notation additive, cela s'écrit

$$nx = \underbrace{x + x + \cdots + x}_{n \ fois}.$$

De plus,

$$x^n x^m = x^{n+m}.$$

Ou en notation additive : $nx + ny = n(x + y)$.

Remarque 7. *Attention, si le groupe G n'est pas commutatif, $(xy)^n \neq x^n y^n$. On peut seulement affirmer que*

$$(xy)^n = \underbrace{xyxy \cdots xy}_{2n \ termes}.$$

Il est pratique de considérer aussi les puissances négatives : pour $n \in \mathbb{Z}, n < 0$, on définit x^n par $x^n = (x^{-1})^{|n|}$. On vérifie qu'on a aussi pour tous $m, n \in \mathbb{Z}$, $x^n x^m = x^{n+m}$.

Proposition 1.13. *Soit G un groupe, $n \in \mathbb{Z}$ et $x \in G$ alors $(x^n)^{-1} = x^{-n}$.*

Démonstration. Puisque $x^{-n}x^n = x^{-n+n} = x^0 = e = x^n x^{-n}$, donc $(x^n)^{-1} = x^{-n}$. □

Remarque 8. *En notation additive, on a $-(nx) = (-n)x$.*

1.3 Sous-groupes

On a vu précédemment que pour montrer que $(\mathbb{Q}^*, \cdot)$ est un groupe, il suffisait de montrer que $\mathbb{Q}^*$ est stable pour la multiplication et que les inverses des éléments de $\mathbb{Q}^*$ sont aussi dans $\mathbb{Q}^*$: c'est la notion de sous-groupe.

Définition 1.14. *Soit G un groupe et $H \subseteq G$. On dit que H est un* sous-groupe de G *si*

(i) H est non vide ;

(ii) H est stable pour la loi de G ;

(iii) pour tout $x \in H$, $x^{-1} \in H$.

Notation 2. *Si H est un sous-groupe de G, on note $H \leq G$.*

Remarque 9.
(a) $H = \{e\}$ et G sont des sous-groupes de G. Un sous-groupe différent de G et de $\{e\}$ est appelé sous-groupe propre.
(b) Pour montrer (i) il suffit de montrer que $e \in H$.
(c) Pour montrer que $(E, *)$ est un groupe, il est souvent plus facile de montrer que c'est un sous-groupe d'un groupe déjà connu, comme le fait la proposition suivante.

Proposition 1.15. *Soit G un groupe et $H \leq G$ alors H est un groupe pour la loi induite par G.*

Démonstration. H est stable donc la loi de G induite sur H est associative. De plus, puisque H est non vide, il existe $x \in H$. (ii) et (iii) impliquent alors que $e = xx^{-1} \in H$. Donc H est un monoïde. (iii) implique que $H^\times = H$. □

Exemple 1.16.

1. $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$;
2. $(\mathbb{Q}^*, \cdot) \leq (\mathbb{R}^*, \cdot)$;
3. *Soit E un espace vectoriel, on a alors* $\mathrm{GL}(E) \leq S_E$.

4. *Pour un groupe G, l'ensemble*

$$Z(G) = \{x \in G \,|\, gx = xg \text{ pour tout } g \in G\}$$

est un sous-groupe de G appelé le centre du groupe *G. C'est en fait un groupe abélien. En effet, $eg = ge = g$ pour tout $g \in G$ donc $e \in Z(G)$ (et donc $Z(G)$ est non-vide). Soit $x, y \in G$ et $g \in G$, alors $(xy)g = x(yg) = x(gy) = (xg)y = g(xy)$ donc $xy \in Z(G)$ et $Z(G)$ est stable pour la loi induite par G. Finalement, si $x \in Z(G)$ et $g \in G$, alors*

$$gx = xg \Longrightarrow x^{-1}(gx)x^{-1} = x^{-1}(xg)x^{-1} \Longrightarrow x^{-1}g = gx^{-1}.$$

Donc $x^{-1} \in Z(G)$. Donc $Z(G) \leq G$. De plus, si $x, g \in Z(G)$ alors $xg = gx$ par définition, donc $Z(G)$ est abélien.

Remarque. *G est abélien si et seulement si $Z(G) = G$.*

Proposition 1.17. *Les seuls sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{N}$.*

Démonstration. Exercice. □

Proposition 1.18. *Soit G un groupe.*

1. *Soit $H \subseteq G$, alors H est un sous-groupe de G si et seulement si $e \in H$ et pour tout $x, y \in H$ on a $xy^{-1} \in H$.*
2. *Si $H \leq G$ et $K \leq H$ alors $K \leq G$ (la relation $\leq$ est transitive).*
3. *L'intersection non vide d'une famille de sous-groupes de G est un sous-groupe de G.*

Démonstration. Exercice. □

1.3.1 Sous-groupes engendrés

Dans le groupe $\mathbb{Z}$ avec l'addition, tout élément s'écrit $x = x1$ (notation additive). Autrement dit $\mathbb{Z}$ est *engendré* par 1 : c'est le plus petit sous-groupe de $\mathbb{Z}$ qui contient 1 en vertu de la proposition 1.17.

Définition 1.19. *Soit G un groupe et $S \subseteq G$.*

1. *On note $\langle S \rangle$ l'intersection de tous les sous-groupes de G qui contiennent S. C'est un sous-groupe de G (proposition 1.18) appelé* sous-groupe engendré par *S.*
2. *Si $G = \langle S \rangle$, on dit que G est engendré par S et que S est une* partie génératrice de *G. Les éléments de S sont appelé* générateurs de *G.*
3. *Si $S = \{s\}$ alors on note $\langle s \rangle$ le sous-groupe engendré par $s \in G$. Si $G = \langle s \rangle$ on dit que G est* monogène.

Cette définition correspond plus ou moins à notre intuition ; la proposition suivante devrait clarifier le lien entre cette définition et notre intuition.

Proposition 1.20. *Soit G un groupe et $S \subseteq G$.*

1. *Dans $\mathcal{P}(G)$ ordonné par l'inclusion, $\langle S \rangle$ est le plus petit sous-groupe de G contenant S.*
2. *Si $S = \emptyset$ alors $\langle S \rangle = \{e\}$, et si $S \neq \emptyset$ alors*

$$\langle S \rangle = \{x_1 \dots x_n \,|\, n \in \mathbb{N}^* \ x_i \in S \text{ ou } x_i^{-1} \in S \text{ pour tout } 1 \leq i \leq n\}.$$

Les éléments de $\langle S \rangle$ sont les produits constitués de générateurs ou de leurs inverses.

Démonstration.
(1) Il faut montrer que $\langle S \rangle$ est le plus petit élément dans l'ensemble

$$\Lambda = \{H \in \mathcal{P}(G) \,|\, H \leq G, \ S \subseteq H\}.$$

Par définition, si $H \in \Lambda$, alors H apparaît dans l'intersections de tous les sous-groupes de G qui contiennent S. En d'autres termes, $\langle S \rangle \subseteq H$. Donc $\langle S \rangle \in \Lambda$ est bien le plus petit élément de l'ensemble Λ de tous les sous-groupes de G qui contiennent S.

(2) Soit $S \neq \emptyset$. Posons $H = \{x_1 \dots x_n \,|\, n \in \mathbb{N}^* \ x_i \in S \text{ ou } x_i^{-1} \in S \text{ pour tout } 1 \leq i \leq n\}$. On remarque que $S \subseteq H$ et si $s \in S$ alors $e = ss^{-1} \in H$. Soit $y = y_1 \dots y_n$ et $z = z_1 \dots z_m$ des éléments de H, où $y_i, z_j \in S$ ou $z_i^{-1}, z_j^{-1} \in S$. Alors

$$yz^{-1} = y_1 \dots y_n z_m^{-1} \dots z_1^{-1}.$$

Puisque $y_i z_j \in S$ ou $z_i^{-1}, z_j^{-1} \in S$, yz^{-1} est bien le produit d'élément de S ou de leurs inverses. Ainsi $xy^{-1} \in H$. On en déduit en vertu de la proposition 1.18 que $H \leq G$, d'où $H \in \Lambda$. En vertu de (1) on sait donc que $\langle S \rangle \subseteq \Lambda$. Montrons maintenant l'inclusion inverse. Soit $K \in \Lambda$ et $x = x_1 \dots x_n \in H$ avec $x_i \in S \subseteq K$ ou $x_i^{-1} \in S \subseteq K$. Donc, puisque K est un groupe, $x_i = (x_i^{-1})^{-1} \in K$ pour tout $1 \leq i \leq n$. D'où $x = x_1 \dots x_n \subseteq K$. On en conclut que $H \subseteq K$. Donc H est le plus petit élément de Λ pour l'inclusion. Autrement dit, $H = \langle S \rangle$ par (1). □

Remarque 10. *En notation additive on a*

$$\langle S \rangle = \{x_1 + \dots + x_n \,|\, n \in \mathbb{N}^* \ x_i \in S \text{ ou } -x_i \in S \text{ pour tout } 1 \leq i \leq n\} \cup \{e\}.$$

Exemples 3.

1. *$\mathbb{Z} = \langle 1 \rangle$ est un groupe monogène pour l'addition. En effet, si $n \in \mathbb{Z}$ est positif, alors*

$$n = \underbrace{1 + 1 + \dots + 1}_{n \text{ fois}};$$

et si $n \in \mathbb{Z}$ est négatif, on a

$$n = \underbrace{(-1) + (-1) + \dots + (-1)}_{|n| \text{ fois}}.$$

2. *$n\mathbb{Z} = \langle n \rangle$ est aussi un groupe monogène pour l'addition.*
3. *$\mathbb{Z}/n\mathbb{Z} = \langle 1 + n\mathbb{Z} \rangle = \langle \overline{1} \rangle$ est encore un groupe monogène (pour l'addition).*
4. *$S_3 = \langle \tau_1\tau_2 \rangle$ car $\tau_3 = \tau_1\tau_2\tau_1 = \tau_2\tau_1\tau_2$; $\sigma_1 = \tau_1\tau_2$ et $\sigma_2 = \tau_2\tau_1$ (ici les générateurs sont leurs propres inverses donc il faut savoir que tous les produits peuvent s'exprimer avec seulement les générateurs). D'où $S_3 = \{e\tau_1\tau_2\tau_1\tau_2\tau_2\tau_1\tau_1\tau_2\tau_1\}$.*
5. *$S_3 = \langle \tau_1\sigma_1 \rangle$ car $\tau_2 = \sigma_1\tau_1$, $\tau_3 = \tau_1\sigma_2$ et $\sigma_2 = \sigma_1^2 = \sigma_1^{-1}$.*
   Convention : *dans S_n on omet le symbole de la composition des fonctions $\circ$ et on écrit la loi multiplicativement.*

Remarque 11.

1. *L'expression d'un élément comme produit de générateurs n'est pas unique ; par exemple, $\tau_3 = \tau_1\tau_2\tau_1 = \tau_2\tau_1\tau_2$ dans S_3 ou $\overline{1} = \overline{1} + \overline{1} + \overline{1} + \overline{1}$ dans $\mathbb{Z}/3\mathbb{Z}$ (noté additivement). On appelle ces expressions des* relations du groupe.
2. *La partie génératrice d'un groupe n'est pas en général unique : $\langle G \rangle = G$.*

Proposition 1.21. *Soit $G = \langle s \rangle$ un groupe monogène, alors G est un groupe abélien et*

$$G = \{s^n \,|\, n \in \mathbb{Z}\}.$$

De plus, la fonction

$$\begin{array}{rccc} f : \mathbb{Z} & \to & \langle x \rangle \\ k & \mapsto & x^k \end{array}$$

est surjective et vérifie $f(k+l) = f(k)f(l)$.

Démonstration. Exercice. □

1.3.2 Ordre d'un groupe, ordre d'un élément de groupe

Définition 1.22. *Soit G un groupe.*

1. *On dit que G est un* groupe fini *si G est fini en tant qu'ensemble.*
2. *Si G est un groupe fini, le cardinal $|G|$ de G est appelé l'* ordre de G.
3. *L'ordre de l'élément $x \in G$ est l'ordre du groupe (monogène) $\langle x \rangle$: on le note $ordre(x)$.*
   Si ce groupe est infini, on dit que l'ordre de x est infini : $ordre(x) = \infty$.
   Si il est fini, $ordre(x) = |\langle x \rangle|$. Le groupe monogène fini $\langle x \rangle$ est alors appelé groupe cyclique.

Avant de donner des exemples, il est bon de faire quelques remarques (qui guideront ainsi nos calculs).

Remarque 12.

(a) Si G est fini et $x \in G$, alors $ordre(x) \leq |G|$. En effet $ordre(x) = |\langle x \rangle|$ et $\langle x \rangle \subseteq G$.

(b) L'élément neutre e est le seul élément d'ordre 1. En effet, $|\langle e \rangle| = |\{e\}| = 1$; et réciproquement, si $ordre(x) = 1 = |\langle x \rangle|$ alors $\langle x \rangle = \{x\}$ mais puisque tout sous-groupe contient e, $e \in \langle x \rangle$ et donc $x = e$.

(c) Dans $(\mathbb{Z}, +)$, tous les éléments non nuls sont d'ordre infini et $ordre(0) = 1$! En effet si $n \neq 0$, alors $n\mathbb{Z} = \langle n \rangle$ est en bijection avec $\mathbb{Z}$ et est donc, de ce fait, infini.

(d) Si G contient un élément d'ordre infini x, alors G contient un sous-ensemble infini : $\langle x \rangle$. Donc G est infini.

(e) Les éléments d'ordre 2 dans un groupe G, c'est-à-dire $x \in G$ tel que $x^2 = e$, sont des involutions.

(f) $ordre(x) = ordre(x^{-1})$ (exercice).

Le résultat suivant est une caractérisation très importante de l'ordre d'un élément.

Proposition 1.23. *Soit G un groupe et $x \in G$ un élément d'ordre fini. Alors $ordre(x)$ est le plus petit entier positif $n \in \mathbb{N}^*$ tel que $x^n = e$. En outre, le groupe cyclique $\langle x \rangle$ s'écrit*

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}.$$

Démonstration. On sait que

$$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$$

Comme x est d'ordre fini, l'ensemble $\{x^k \mid k \in \mathbb{Z}\}$ l'est aussi. Donc il existe p, q tel que $p > q$ et $x^p = x^q$. En effet, sinon $x^p = x^q$ impliquerait que $p = q$ et donc que la fonction

$$\begin{array}{ccc} \mathbb{Z} & \to & \langle x \rangle \\ k & \mapsto & x^k \end{array}$$

serait injective, et donc bijective. D'où $\langle x \rangle$ serait infini, ce qui contredirait notre hypothèse.

Puisque $x^p = x^q$, on constate donc que $x^{p-q} = e$ et $p - q > 0$. L'ensemble $\{k \in \mathbb{N}^* \mid x^k = e\} \subseteq \mathbb{N}$ est donc non vide, il admet donc un plus petit élément n. Il s'ensuit que $x^n = e$ et

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$$

et donc que $ordre(x) = |\langle x \rangle| = n$. □

Remarque 13. *Il est maintenant bien plus facile de calculer l'ordre d'un élément, il suffit de compter le nombre de fois où il faut le multiplier par lui-même jusqu'à obtenir l'identité e.*

Exemples 4.

1. *S_3 est d'ordre 6 : $|S_3| = 6$.*
2. *Dans S_3, on a : $ordre(e) = 1$, $ordre(\tau_1) = ordre(\tau_2) = ordre(\tau_3) = 2$ (ce sont des involutions) et $ordre(\sigma_1) = ordre(\sigma_3) = 3$. Ainsi dans S_3, $\sigma_1 \neq e$, $\sigma_1^2 = \sigma_2 \neq e$ mais $\sigma_1^3 = e$ donc $ordre(\sigma_1) = 3$.*
3. *$\mathbb{Z}/n\mathbb{Z}$ est d'ordre n.*
4. *Dans $\mathbb{Z}/6\mathbb{Z}$, $ordre(\overline{0}) = 1$, $ordre(\overline{1}) = ordre(\overline{5}) = 6$, $ordre(\overline{2}) = ordre(\overline{4}) = 3$ et $ordre(\overline{3}) = 2$ (c'est une involution).*

Notez bien que dans nos exemples, l'ordre d'un élément divise l'ordre du groupe ! On montrera plus tard que cela est vrai en général.

Si on calculait l'ordre de S_4, S_5, etc. on s'apercevrait que

Proposition 1.24. *Soit $n \in \mathbb{N}^*$, alors $|S_n| = n!$.*

Mais montrons d'abord un résultat un peu plus général.

Lemme 1.25. *Soit E et F deux ensembles de cardinal n, alors l'ensemble $\mathcal{B}(E, F)$ des bijection de E dans F est de cardinal $n!$.*

La proposition est une conséquence immédiate du lemme (poser $E = F = \{1 \dots, n\}$).

Démonstration du lemme. On montre le lemme par récurrence sur n. Si $n = 1$ il y a une et une seule fonction $E = \{x\} \to F = \{y\}$, qui est clairement bijective. Donc $\mathcal{B}(E, F) = 1 = 1!$ dans ce cas.

Supposons maintenant la propriété vraie pour $n - 1 \geq 1$: si E' et F' sont deux ensembles de cardinal $n - 1$, alors $|\mathcal{B}(E', F')| = (n - 1)!$.

Soit $x \in E$. Alors, pour tout $y \in F$, on a $|E \setminus \{x\}| = |F \setminus \{y\}| = n - 1$. Donc par récurrence, $|\mathcal{B}(E \setminus \{x\}, F \setminus \{y\})| = (n - 1)!$ pour tout $y \in F$. Si $\alpha \in \mathcal{B}(E \setminus \{x\}, F \setminus \{y\})$ alors la fonction $f : E \to F$ tel que $f|_{E\setminus\{x\}} = \alpha$ et $f(x) = y$ est une bijection de E dans F (à vérifier). Donc pour tout $y \in F$, il y a $(n - 1)!$ bijection de E dans F tel que $f(x) = y$. C'est-à-dire que l'ensemble $A_y = \{f \in \mathcal{B}(E, F) \,|\, f(x) = y\}$ est de cardinal $(n - 1)!$ pour tout $y \in F$. On peut vérifier que $\{A_y \,|\, y \in F\}$ est une partition de l'ensemble $\mathcal{B}(E, F)$ (exercice). D'où

$$|\mathcal{B}(E, F)| = \sum_{y \in F} |A_y| = \sum_{y \in F} (n - 1)! = |F| \cdot (n - 1)! = n(n - 1)! = n!.$$

Donc la propriété est vraie au rang n, le lemme est donc vrai pour tout $n \in \mathbb{N}^*$. □

1.3.3 Groupe fini et générateurs

Soit G un groupe et $x \in G$. Si $ordre(x) = n$ est fini, alors $x^{-1} = x^{n-1}$. En effet,

$$x^{n-1}x = x^n = e = xx^{n-1}.$$

En particulier, si G est un groupe fini engendré par S, alors tous les générateurs sont d'ordre fini et $s^{-1} = s^{ordre(s)-1}$ pour tout $s \in S$. Donc en vertu de la proposition 1.20, $x \in G$ s'écrira comme un produit de générateurs : $x = x_1 \dots x_m$ avec $x_i \in S$ (on n'a plus besoin de considérer aussi les inverses des générateurs). En effet, il suffit de partir d'un produit constitué de générateurs et de leurs inverses, puis pour $s \in S$ il suffit de remplacer chaque inverse s^{-1} par le mot $s^{ordre(s)-1}$.

Exemple 1.26. *On considère S_3 engendré par $\tau_1 = 213$ et $\sigma_1 = 231$. Alors $321 = \tau_1\sigma_1^{-1}$. Mais σ_1 est d'ordre 3, alors $\sigma_1^{-1} = \sigma_1^2$. D'où on obtient pour $321 \in S_3$ un mot en τ_1 et σ_1 (et non pas leurs inverses) :*

$$321 = \tau_1\sigma_1\sigma_1.$$

1.4 Récapitulatif, questions et nouveaux exemples

Que pouvons-nous déjà dire au sujet des ensembles et lois de compositions que nous connaissons dans le cadre de la théorie des groupes ?

1.4.1 Le groupe $(\mathbb{Z}, +)$

Le groupe $\mathbb{Z}$ muni de l'addition est un groupe abélien d'ordre infini. On sait *classifier* les sous-groupes et générateurs de $\mathbb{Z}$.

Ordre des éléments de $\mathbb{Z}$: On a vu que $\mathbb{Z}$ est d'ordre infini et que tous les entiers non nuls sont d'ordre infini.

Les sous-groupes de $\mathbb{Z}$: On a vu que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Générateurs particuliers de $\mathbb{Z}$: Les seuls générateurs de $\mathbb{Z}$ qui l'engendrent en tant que groupe monogène sont 1 et -1 : si $n \in \mathbb{Z}$ est tel que $\mathbb{Z} = \langle n \rangle = n\mathbb{Z}$, alors tout entier est multiple de n, ce qui implique $n = \pm 1$.

Générateurs particuliers des sous-groupes de $\mathbb{Z}$: Les générateurs du sous-groupe $n\mathbb{Z}$ qui l'engendrent en tant que groupe monogène sont $\pm n$ pour les mêmes raisons que ci-dessus. On peut donc dire que l'ensemble des sous-groupes de $\mathbb{Z}$ est en bijection avec $\mathbb{N}$.

Question : Comme on vient de le voir, on connaît très bien la structure du groupe $\mathbb{Z}$ muni de l'addition. Pouvons-nous décrire aussi bien d'autres groupes ?

1.4.2 Les groupes $(\mathbb{Z}/n\mathbb{Z},+)$

Soit $n \in \mathbb{N}^*$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition est un groupe abélien d'ordre fini n. On va *classifier* les sous-groupes et générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Ordre des éléments de $(\mathbb{Z}/n\mathbb{Z},+)$:

Proposition 1.27. *Soit $x \in \mathbb{Z}$ et $d = pgcd(x,n)$, alors $ordre(\overline{x}) = n/d$.*

Démonstration. Soit $k = n/d \in \mathbb{N}$ On peut prendre $0 \leq a \leq n-1$ tel que $\overline{a} = \overline{x}$ car dans ce cas, $\text{pgcd}(a,n) = \text{pgcd}(x,n)$ car $x = a + \alpha n$, $\alpha \in \mathbb{Z}$. On veut montrer que $ordre(\overline{x}) = ordre(\overline{a}) = k$.

(a) Posons $l = a/d$, alors $\text{pgcd}(k,l) = 1$. En effet, si d' divise k et l, alors $d'd$ divise n et a. Or $d = \text{pgcd}(a,n)$, donc $d' = 1$.

(b) On a (notation additive)

$$k\overline{x} = k\overline{a} = \overline{ka} = \overline{kdq} = \overline{nd} = \overline{0}\,.$$

(c) Il suffit donc de montrer qu'en vertu de la proposition 1.23, k est minimum pour cette propriété. Si $q \leq k$ tel que $q\overline{a} = \overline{0}$ alors $qld = qa = bn = bkd$ avec $b \in \mathbb{Z}$. Donc $ql = bk$. Comme k et l sont premiers entre eux, on obtient envertu du lemme de Gauss que $k|q$ donc $k = q$ car $q \leq k$. □

Remarque 14. *Ainsi l'ordre des éléments de $\mathbb{Z}/n\mathbb{Z}$ divise l'ordre de $\mathbb{Z}/n\mathbb{Z}$. On verra dans le chapitre 3 que cette propriété est vraie pour tout groupe fini : c'est le théorème de Lagrange (voir Chapitre 3).*

Exemple 1.28. *L'ordre de $\overline{30}$ dans $(\mathbb{Z}/42\mathbb{Z},+)$ est $42/pgcd(30,42) = 7$.*

Les sous-groupes de $(\mathbb{Z}/n\mathbb{Z},+)$:

Proposition 1.29. *Les seuls sous-groupes de $(\mathbb{Z}/n\mathbb{Z},+)$ sont les $\langle\overline{k}\,\rangle$ tel que k divise n (et d'ordre n/k). En particulier, la fonction $k\mathbb{Z} \mapsto \langle k\rangle$ est une bijection entre l'ensemble des sous-groupes $k\mathbb{Z}$ de $\mathbb{Z}$ tel que $k|n$ et l'ensemble des sous-groupes de $(\mathbb{Z}/n\mathbb{Z},+)$.*

Démonstration. Soit H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$. Considérons $K = \{x \in \mathbb{Z} \,|\, \overline{x} \in H\}$. Montrons que K est un sous-groupe de $(\mathbb{Z}, +)$ contenant $n\mathbb{Z}$.

Tout d'abord, observons que K est non vide car $0 \in K$, car $\overline{0} \in H$. De même, puisque $\overline{n} = \overline{0}$, on obtient que $n \in K$. Soit $x, y \in K$ alors $\overline{x - y} = \overline{x} - \overline{y} \in H$ car H est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Donc $K \leq \mathbb{Z}$.

Comme K est un sous-groupe de $\mathbb{Z}$, on sait qu'il existe $k \in \mathbb{N}$ tel que $K = k\mathbb{Z}$. Puisque $n \in K = k\mathbb{Z}$ et $n\mathbb{Z} = \langle n \rangle$ est le plus petit sous-groupe contenant n, on a $n\mathbb{Z} \subseteq k\mathbb{Z}$.

Donc tout élément de $y \in K$ s'écrit $y = qk$ et donc tout élément de H s'écrit $\overline{y} = q\overline{d}$. D'où $K = \langle \overline{k} \rangle$.

Puisque $n\mathbb{Z} \subseteq k\mathbb{Z}$, on a $k|n$ et donc $\text{pgcd}(n, k) = k$. En vertu de la proposition 1.27, on a

$$|H| = |\langle \overline{k} \rangle| = ordre(\overline{k}) = n/k.$$

On vérifiera en exercice la dernière partie de la proposition. □

Remarque 15. *La technique de la preuve ci-dessus est la même que celle que l'on utilisera pour déterminer les sous-groupes des groupes quotients dans le chapitre 3.*

Générateurs particuliers de $\mathbb{Z}/n\mathbb{Z}$:

Corollaire 1.30. *Soit $n \in \mathbb{N}$, alors*

1. *$\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $pgcd(x, n) = 1$.*
2. *$(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Exercice. □

1.4.3 Le groupe symétrique S_n

Soit $n \in \mathbb{N}^*$. Nous allons étudier plus en détail le groupe symétrique S_n. On sait que S_n muni de la composition des fonctions est un groupe d'ordre $n!$ et non abélien en général. C'est notre premier exemple de groupe fini non abélien (le groupe linéaire est un groupe infini non abélien).

Comme nous allons le voir plus tard au chapitre suivant, tout groupe fini est une copie d'un sous-groupe d'un groupe symétrique (théorème de Cayley [2]). La question de trouver TOUS les sous-groupes d'un groupe symétrique est donc étroitrement liée à la classification de TOUS les groupes finis !

Voici ce que nous pouvons dire au sujet du groupe symétrique. Pour cela, nous allons développer deux outils combinatoires : les inversions et les cycles d'une permutation.

2. Arthur Cayley, 1821-1895.

Générateurs particuliers de S_n et transpositions

Définition 1.31.

1. *Une* inversion d'une permutation $\sigma \in S_n$ *est un couple* (i,j) *tel que :*
$$1 \leq i < j \leq n \quad et \quad \sigma(i) > \sigma(j).$$
2. *Le nombre d'inversions de la permutation* $\sigma \in S_n$ *est appelé la* longueur de σ. *Ce nombre est noté :*
$$\ell(\sigma) = \{(i,j) \,|\, 1 \leq i < j \leq n \text{ et } \sigma(i) > \sigma(j)\}.$$

Exemple 1.32.

1. $\ell(e) = \ell(12\dots n) = 0$ *et* $\ell(\sigma) = 0$ *si et seulement si* $\sigma = e$. *En effet, si* $\ell(\sigma) = 0$ *alors on doit avoir* $\sigma(1) < \sigma(2) < \cdots < \sigma(n)$. *Donc* $\sigma = 12\dots n = e$.
2. *Les inversions de* $\sigma = 24513$ *sont* $(1,4)$, $(2,4)$, $(2,5)$, $(3,4)$ *et* $(3,5)$, *donc* $\ell(\sigma) = 5$.
3. *Dans* S_3, *on a* $\ell(123) = \ell(e) = 0$; $\ell(213) = \ell(\tau_1) = 1$; $\ell(132) = \ell(\tau_2) = 1$;
$\ell(231) = \ell(\sigma_1) = \ell(\tau_1\tau_2) = 2$; $\ell(312) = \ell(\sigma_2) = \ell(\tau_2\tau_1) = 2$; *et* $\ell(321) = \ell(\tau_3) = \ell(\tau_1\tau_2\tau_1) = 3$.

On observe dans ce dernier exemple que le nombre d'inversion de $\sigma \in S_3$ est égal au nombre minimal de générateurs $\tau_1\tau_2$ dont on a besoin pour écrire σ. Nous allons démontrer que ce phénomène est vraie pour tout $n \in \mathbb{N}$.

Définition 1.33. *Soit* $1 \leq i < n$, *la* transposition adjacente τ_i *est la permutation qui échange* i *et* $i+1$ *et laisse fixe tout* $j \in \{1\dots n\} \setminus \{i, i+1\}$. *En d'autres termes :*
$$\tau_i(i) = i+1; \quad \tau_i(i+1) = i; \quad \tau_i(j) = j \text{ pour tout } j \in \{1\dots n\} \setminus \{i, i+1\}.$$

Remarque 16. *Les transpositions sont des involutions : ordre*$(\tau_i) = 2$, *c'est-à-dire* $\tau_i^{-1} = \tau_i$.

Théorème 1.34. *Toute permutation* $\sigma \in S_n$ *est un produit de* $\ell(\sigma)$ *transpositions adjacentes.*

Avant de montrer ce théorème, donnons un exemple et énonçons un lemme.

Exemple 1.35. *Soit* $\sigma = 24513 \in S_5$. *Puisque multiplier à gauche par* τ_i *revient à échanger* $\sigma(i)$ *et* $\sigma(i+1)$ *dans le mot* σ, *on obtient :*
$$24513 = 24153\ \tau_3 = 21453\ \tau_2\tau_3 = 12453\ \tau_1\tau_2\tau_3 = 12435\ \tau_4\tau_1\tau_2\tau_3 = \tau_3\tau_4\tau_1\tau_2\tau_3.$$

Remarquer dans l'exemple précédent que multiplier par τ_i revient à augmenter ou diminuer la longueur par 1 !

Lemme 1.36. *Soit* $\sigma \in S_n$ *et* $1 \leq i < n$, *alors* $\ell(\sigma\tau_i) = \ell(\sigma) \pm 1$. *Plus précisement,*
$$\ell(\sigma\tau_i) = \begin{cases} \ell(\sigma) + 1 & si\ \sigma(i) < \sigma(i+1) \\ \ell(\sigma) - 1 & si\ \sigma(i) > \sigma(i+1) \end{cases}.$$

Démonstration. Écrivons $\sigma = a_1 a_2 \dots a_n$ où $a_i = \sigma(i)$. On a alors $\alpha = \sigma\tau_i = a_1 \dots a_{i-1} a_{i+1} a_i a_{i+2} \dots a_n$, i.e α s'obtient à partir de σ en y échangeant la i-ème et la $i+1$-ème lettre.

Premièrement, observons que toute inversion $(k,l) \neq (i,i+1)$ de σ correspond à une inversion $(k',l') \neq (i,i+1)$ de α et vice versa. Par exemple si (i,k) est une inversion de α alors $(i+1,k)$ est une inversion de α car $a_i = \sigma(i) = \alpha_{i+1}$ et $\sigma(k) = \alpha_k$. En d'autres termes, le nombre d'inversions de σ différentes de $(i,i+1)$ est égal au nombre d'inversions de α différentes de $(i,i+1)$.

Si $a_i = \sigma(i) < \sigma(i+1) = a_{i+1}$, alors $(i,i+1)$ n'est pas une inversion de σ. Mais puisque $\alpha(i) = a_{i+1} > a_i = \alpha(i+1)$, alors $(i,i+1)$ est une inversion de α. Dans ce cas, α a une inversion de plus que σ.

Si par contre $a_i = \sigma(i) > \sigma(i+1) = a_{i+1}$, alors $(i,i+1)$ est une inversion de σ. Mais puisque $\alpha(i) = a_{i+1} < a_i = \alpha(i+1)$, alors $(i,i+1)$ est une inversion de α. Dans ce cas, α a une inversion de moins que σ. □

Démonstration du théorème 1.34. Par récurrence sur $\ell(\sigma)$. Si $\ell(\sigma) = 0$, alors $\sigma = e$ est l'identité, qui correspond au produit vide.

Supposons $\ell(\sigma) > 0$, alors $\sigma \neq e$. Il existe donc i tel que $\sigma(i) > \sigma(i+1)$. Ainsi en vertu du lemme 1.36, $\ell(\sigma\tau_i) = \ell(\sigma) - 1 < \ell(\sigma)$. Par hypothèse de récurrence, $\sigma\tau_1$ est égal à un produit de $\ell(\sigma\tau_i)$ transpositions adjacentes. Donc $\sigma = \sigma\tau_i\tau_i^{-1} = (\sigma\tau_i)\tau_i$ (car τ_i est une involution) est un produit de $\ell(\sigma)$ transpositions adjacentes. □

Signature d'une permutation : On considère la fonction

$$\begin{aligned} \epsilon : S_n &\to \{\pm 1\} \\ \sigma &\mapsto (-1)^{\ell(\sigma)}. \end{aligned}$$

Définition 1.37. *Le nombre $\epsilon(\sigma)$ est appelé* signature de la permutation σ.

Corollaire 1.38. *$\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$, pour tout $\sigma\tau \in S_n$.*

Démonstration. Il suffit de montrer que

$$(\star) \quad \ell(\sigma\tau) \equiv \ell(\sigma) + \ell(\tau) \pmod 2.$$

En effet, on aura alors $k \in \mathbb{Z}$ tel que $\ell(\sigma\tau) = \ell(\sigma) + \ell(\tau) + 2k$ et donc que

$$\epsilon(\sigma\tau) = (-1)^{\ell(\sigma\tau)} = (-1)^{\ell(\sigma)+\ell(\tau)+2k} = (-1)^{\ell(\sigma)}(-1)^{\ell(\tau)}((-1)^2)^k = \epsilon(\sigma)\epsilon(\tau).$$

L'égalité $(\star)$ est laissée en exercice. □

Ordre et cycles d'une permutation

La notion de cycle est fondamentale dans le groupe symétrique. C'est une nouvelle façon d'écrire les permutations qui va aussi nous permettre de calculer, entre autres, leurs ordres.

Définition 1.39. *Soit $2 \leq p \leq n$. Une permutation $\sigma \in S_n$ est appelée un* p-cycle *si il existe p entiers $1 \leq a_1 \ldots, a_p \leq n$ distincts tel que*

$$\sigma(a_1) = a_2, \ldots, \sigma(a_j) = a_{j+1}, \ldots, \sigma(a_p) = a_1$$

et $\sigma(a) = a$ si $a \notin \{a_1 \ldots, a_p\}$.

Notation 3. *Un p-cycle se note $\sigma = (a_1, a_2 \ldots, a_p)$.*

Exemple 1.40. *La permutation*

$$\sigma = 24351 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = (1, 2, 4, 5)$$

est un 4-cycle dans S_5 car $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(4) = 5$ et $\sigma(5) = 1$; de plus, $\sigma(3) = 3$.

Remarque 17.

1. *On dit parfois que e est l'unique 1-cycle.*
2. *Les p-cycles sont appelés* cycles.
3. *p est souvent appelé la* longueur du p-cycle.
4. *Une* transposition *est par définition un 2-cycle.*
5. *La transposition adjacente τ_i est donc un 2-cycle qui s'écrit $\tau_i = (i, i+1)$.*
6. *Une* permutation circulaire *de S_n est un n-cycle.*

Exemple 1.41. *Reprenons l'exemple précédent : $\sigma = 24351 = (1, 2, 4, 5)$. Alors $\sigma^{-1} = 51324 = (1, 5, 4, 2)$ (on lit le cycle à l'envers). Donc σ^{-1} est aussi un 4-cycle. Notons que $\sigma^2 = 45312$ n'est pas un cycle car $\sigma^2(1) = 4$, $\sigma^2(4) = 1$, $\sigma^2(2) = 5$ et $\sigma^2(5) = 2$. Donc le produit de cycles n'est pas forcément un cycle (l'ensemble des cycles n'est pas stable). Par ailleurs, on voit que $\sigma^3 = \sigma^{-1}$ donc $ordre(\sigma) = 4$, i.e. la longueur du cycle.*

Proposition 1.42. *Soit $\sigma = (a_1 \ldots, a_p) \in S_n$ un p-cycle, alors*

1. *$\sigma^{-1} = (a_1, a_p, a_{p-1} \ldots a_2)$ est un p-cycle ;*
2. *$ordre(\sigma) = p$.*

Démonstration. Exercice. □

Définition 1.43. *Soit $2 \leq p, q \leq n$. On dit que les cycles $(a_1 \ldots, a_p)$ et $(b_1 \ldots, b_q)$ sont* à support disjoint *ou simplement* disjoints *si $\{a_1 \ldots, a_p\} \cap \{b_1 \ldots, b_q\} = \emptyset$.*

Exemple 1.44. *Les cycles* $(1,5,4)$ *et* $(2,3)$ *sont à support disjoint tandis que* $(1,5,2)$ *et* $(2,6,3)$ *ne le sont pas car* $2 \in \{1,2,5\} \cap \{2,3,6\}$.

Proposition 1.45. *Deux cycles à support disjoint commutent : si* σ *et* τ *sont à support disjoint, alors* $\sigma\tau = \tau\sigma$.

Démonstration. Exercice. □

Théorème 1.46. *Toute permutation différente de l'identité s'écrit de manière unique, à l'ordre des facteurs près, comme produit de cycles à support disjoint (et donc qui commutent).*

Nous n'allons pas démontrer ce théorème, mais l'illustrer par la décomposition d'une permutation particulière. La démonstration est proposée en exercice (ou voir [1]).

Exemple 1.47. *Prenons* $\sigma = 729158436 \in S_9$. *Nous partons de* 1 *et écrivons les images sous* σ, σ^2, *etc. jusqu'à ce qu'on retrouve* 1 *: ceci nous donne le cycle* $(1,7,4)$. *Continuant avec* 2, *le plus petit entier qui n'est pas apparu jusqu'ici, nous voyons que* $\sigma(2) = 2$, *c'est-à-dire que* 2 *est* point fixe *de* σ. *Nous continuons avec* 3, *ce qui nous donne le cycle* $(3,9,6,8)$. *Le seul nombre qui reste est* 5, *qui est point fixe. D'où la décomposition*

$$\sigma = (1,7,4)(3,9,6,8) = (3,9,6,8)(1,7,4).$$

L'unicité de la décomposition provient de l'unicité des cycles qui la compose.

Corollaire 1.48. *Soit* $\sigma = c_1 \dots c_k \in S_n$ *une permutation en cycle décomposée en cycles disjoints, alors* $ordre(\sigma) = ppcm(ordre(c_1), ordre(c_2), ordre(c_3) \dots, ordre(c_k))$.

Démonstration. Exercice. □

Exemple 1.49. *Avec* $\sigma = 729158436 \in S_9$ *comme dans l'exemple précédent, on obtient* $ordre(\sigma) = 12$ *qui est le plus petit commun multiple de la longueur des cycles dans la décomposition de* σ.

1.4.4 Les groupes diédraux

Pour terminer, nous allons donner un exemple de groupe provenant de la géométrie. L'exposé de ces résultats fait appel à une connnaissance de base de la géométrie du plan.

Soit $m \in \mathbb{N}$, $m \geq 3$, et P_m le polygone plan régulier convexe à m sommets $A_0 \dots, A_{m-1}$ inscrit dans le cercle unité de centre O.

Définition 1.50. *Le* groupe diédral D_m *est le groupe des isométries du plan qui préserve* P_m.

Exemple 1.51. *1.* D_3 *est le groupe des isométries du triangle,* D_4 *celui du carré,* D_5 *celui du pentagone et ainsi de suite.*

2. *Si $f \in D_4$ alors f doit être une permutation des sommets $A_0 = A_4, A_1, A_2, A_3$. Donc les seuls éléments de D_4 sont : Id, la rotation r de centre 0 qui envoie A_0 sur A_1, la rotation r^2 de centre 0 qui envoie A_0 sur A_2, la rotation r^3 de centre 0 qui envoie A_0 sur A_3. On remarque que $r^4(A_0) = A_4 = A_0$ donc $r^4 = Id$; mais aussi s la symétrie orthogonale d'axe OA_0, t la symétrie orthogonale d'axe la médiatrice à $[A_0, A_1]$, s' la symétrie orthogonale d'axe OA_1 et t' la symétrie orthogonale d'axe la médiatrice à $[A_1, A_2]$. On observe que*

$$t = rs \quad s' = r^2 s \quad , t' = r^3 s.$$

Donc $D_4 = \{Id, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$ est d'ordre $2 \cdot 4 = 8$.

1.4.5 Générateurs et ordre de D_m

Soit s la symétrie orthogonale d'axe OA_0 et r la rotation de centre O et d'angle $2\pi/m$. Donc

$$s(0) = 0 \quad \text{et} \quad s(A_i) = A_{m-i}, \text{ pour tout } 1 \leq i \leq m-1$$

$$r(A_i) = A_{i+1}, \text{ pour tout } 1 \leq i \leq m-1, \text{ et } r(A_{m-1}) = A_0.$$

Donc s et r préservent P_m, d'où on a le

Théorème 1.52. *Soit $m \in \mathbb{N}$, $m \geq 3$, alors*

1. *$s, r \in D_m$. De plus, $ordre(s) = 2, ordre(r) = m$, et $srs = r^{-1}$.*
2. *$D_m = \langle r, s \rangle = \{r^k, sr^k \mid 0 \leq k \leq m-1\}$ est un groupe d'ordre $2m$.*

Démonstration. (1) La première partie de la proposition est une conséquence de ce qui précède. Pour ce qui est de la deuxième partie : par définition, une symétrie vérifie $s^2 = Id$ et $s \neq Id$ donc $ordre(s) = 2$. De plus, puisque $r^m(A_i) = A_i$, r^m ($m \geq 3$) fixe au moins trois points du plan, donc $r^m = Id$ et $r, r^2 \ldots, r^{m-1} \neq Id$ donc $ordre(r) = m$ (le fait qu'une rotation d'angle $2\pi/m$ est d'ordre m est un résultat bien connu et que l'on vient de redémontrer). Maintenant : en posant $A_m = A_0$ on a

$$rsrs(A_i) = rsr(A_{m-i}) = rs(A_{m-i+1}) = r(A_{i-1}) = A_i$$

Ainsi $rsrs$ fixe plus de trois points du plan, donc $rsrs = Id$. D'où la relation $srsr = Id$.
(2) Les seules isométries qui préservent P_m sont :
(i) Les rotations d'angles $2k\pi/m$, c'est-à-dire, les r^k ($Id = r^0$).
(ii) Les symétries d'axe OA_k et celles passant par les médiatrices des segments $[A_i, A_{i+1}]$ (qui peuvent être les mêmes, selon que si m est pair ou impair) : c'est à dire les sr^{m-k}. D'où le résultat. □

Remarque 18. *Comme la relation $rsrs = Id$ suffit à construire D_m pour peu que l'on sache que $s^2 = Id$ et $r^m = Id$, on dit que D_m est* présenté par les générateurs s, r et les relations $s^2 = r^m = srsr = e$, *que l'on note*

$$D_m = \langle s, r \mid s^2 = r^m = srsr = e \rangle.$$

1.4.6 Conclusion

Trouver les plus petits ensembles de générateurs d'un groupe et tous ses sous-groupes est un problème difficile qui a motivé et motive toujours les chercheurs en théorie des groupes. Une des tâches des algébristes du XXe siècle a été de classifier tous les groupes finis (voir l'atlas des groupes finis [2]).

Nous allons développer dans la suite du cours quelques-unes des techniques de base développées pour répondre à ces questions : morphismes de groupes, classes d'isomorphisme, groupes quotients, etc.

Par exemple, nous allons voir que si un groupe est monogène, alors c'est *une copie de* $\mathbb{Z}$ si il est infini ou c'est *une copie de* $\mathbb{Z}/n\mathbb{Z}$ si il est fini. Nous aurons alors classifié tous les groupes monogènes (et par ricochet aussi leurs sous-groupes et générateurs) !

Chapitre 2

Morphismes de groupes

On a vu auparavant des exemples de fonctions entre groupes qui respectaient les lois de composition de ces groupes, par exemple pour la signature d'une permutation. Ces fonctions spécifiques sont de première importance dans l'étude des groupes.

Définition 2.1. *Soit $(G, \cdot)$ et $(G', *)$ deux groupes. Un* morphisme *(ou* homomorphisme*)* de groupes *de G dans G' est une fonction $f : G \to G'$ qui vérifie*

$$f(x \cdot y) = f(x) * f(y), \text{ pour tous } x, y \in G.$$

On note $Hom(G, G')$ l'ensemble des morphismes de groupes de G dans G'.
On note $End(G)$ l'ensemble des morphismes de groupes de G dans lui-même, dont les éléments sont appellés endomorphismes.

Exemples 5.

1. *L'ensemble $C_2 = \{\pm 1\}$ est un groupe pour la multiplication, la signature $\epsilon : S_n \to C_2$ est donc un morphisme de groupes surjectif (que l'on appelle parfois* épimorphisme*).*
2. *Si $H \subseteq G$, l'inclusion $i : H \to G$ définie par $i(g) = g$ est un morphisme de groupes injectif (que l'on appelle parfois* monomorphisme*).*
3. *Si $n \in \mathbb{N}^*$, la fonction $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $\pi(k) = k + n\mathbb{Z} = \overline{k}$ est un morphisme de groupes surjectif (épimorphisme) appelé* surjection canonique.
4. *La fonction $f : \mathbb{Z}/2\mathbb{Z} \to C_2$ définie par $f(\overline{0}) = 1$ et $f(\overline{1}) = -1$ est un morphisme de groupes bijectif (que l'on appelle un* isomorphisme*) : en effet $f(\overline{0} + \overline{1}) = f(\overline{1}) = -1 = 1 \cdot (-1) = f(\overline{0})f(\overline{1})$; $f(\overline{0} + \overline{0}) = f(\overline{0}) = 1 = 1 \cdot 1 = f(\overline{0})f(\overline{0})$ et $f(\overline{1} + \overline{1}) = f(\overline{0}) = 1 = (-1) \cdot (-1) = f(\overline{1})f(\overline{1})$. Donc* additionner *dans $\mathbb{Z}/2\mathbb{Z}$ est la même chose que de* multiplier *dans C_2 !*

Proposition 2.2. *Soit $f \in Hom(G, G')$ alors*

1. *$f(e_G) = e_{G'}$;*
2. *$f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G$;*
3. *$H \leq G$ entraîne $f(H) \leq G'$;*
4. *$H' \leq G'$ entraîne $f^*(H') \leq G$, où $f^*(H')$ est l'ensemble de tous les antécédents de tous les éléments de H'.*

Démonstration.

1. Pour tout $x \in G$ on a $f(x) = f(xe_G) = f(x) * f(e_G)$. Comme $f(x) * e_{G'} = f(x)$, on obtient par identification que $f(x) * f(e_G) = f(x) * e_{G'}$, puis en multipliant à gauche par l'inverse de $f(x)$ on trouve $f(e_G) = e_{G'}$.
2. Soit $x \in G$. Comme $e_{G'} = f(e_G) = f(xx^{-1}) = f(x) * f(x^{-1})$ et de même $e_{G'} = f(x^{-1}) * f(x)$, on en déduit que $f(x^{-1}) = f(x)^{-1}$ l'inverse de $f(x)$ dans G'.
3. Soit $H \leq G$ et soit $y_1, y_2 \in f(H)$. Notons que $e_{G'} = f(e_G) \in f(H)$ car $H \leq G$. Alors il existe $x_1, x_2 \in H$ tel que $f(x_1) = y_1$ et $f(x_2) = y_2$. Ainsi, puisque $x_1 x_2^{-1} \in H$ on obtient en vertu de (2) que
$$y_1 * y_2^{-1} = f(x_1) * f(x_2)^{-1} = f(x_1) * f(x_2^{-1}) = f(x_1 x_2^{-1}) \in f(H).$$
Donc $f(H) \leq G'$.
4. Exercice.

□

Remarque 19. *Si $f : G \to G'$, alors $Im(f) = f(G)$ est un sous-groupe de G'.*

2.1 Noyau d'un morphisme de groupes

Définition 2.3. *Soit $f \in Hom(G, G')$, le* noyau *de f est le sous-groupe de G formé des antécédents de $e_{G'}$ par f, et est noté* $\ker(f)$.

Exemple 2.4. Le groupe alterné. *Soit $n \in \mathbb{N}^*$, on considère la signature de S_n, $\epsilon_n : S_n \to C_2$. Le noyau* $\ker(\epsilon_n)$ *de la signature est un sous-groupe de S_n appelé le* groupe alterné *et noté A_n.*

Proposition 2.5. *Si $f : G \to G'$ est un morphisme de groupes, on a*

1. *f est injective si et seulement si* $\ker(f) = \{e_G\}$;
2. *f est surjective si et seulement si $Im(f) = G'$.*

Démonstration. Supposons d'abord f injective. Soit $x \in \ker(f)$, alors $f(x) = e_{G'} = f(e_G)$. Comme f est injective, $x = e_G$. Supposons maintenant que $\ker(f) = \{e_G\}$. Soit $x_1, x_2 \in G$ tel que $f(x_1) = f(x_2)$, alors $e_{G'} = f(x_1) * f(x_2)^{-1} = f(x_1 x_2^{-1})$. Donc $x_1 x_2^{-1} \in \ker(f) = \{e_G\}$ d'où $x_1 = x_2$. □

2.2 Composition de morphismes de groupes

Proposition 2.6. *Soit $f \in Hom(G, G')$ et $g \in Hom(G', G'')$ deux morphismes de groupes, alors $g \circ f \in Hom(G, G'')$ est un morphisme de groupes.*

Démonstration. Notons $(G, \cdot)$, $(G', *)$ et $(G'', \star)$. Il est clair que $g \circ f$ est une fonction de G dans G''. Soit $a, b \in G$, montrons que $(g \circ f)(ab) = (g \circ f)(a) \star (g \circ f)(b)$. Puisque f et g sont des morphismes de groupes on obtient : $(g \circ f)(ab) = g(f(ab)) = g(f(a) * f(b)) = g(f(a)) \star g(f(b)) = (g \circ f)(a) \star (g \circ f)(b)$. □

On en déduit immédiatement le résultat suivant :

Corollaire 2.7. *$(End(G), \circ)$ est un monoïde.*

2.3 Isomorphisme de groupes

Définition 2.8. *Un morphisme de groupes $f \in Hom(G, G')$ est un* isomorphisme de groupes *si la fonction f est inversible. Un isomorphisme de G dans G est appelé un* automorphisme *de G. L'ensemble des automorphismes est noté $Aut(G)$.*

Exemple 2.9. *Le morphisme de groupes $f : \mathbb{Z}/2\mathbb{Z} \to C_2$ défini par $f(\overline{0}) = 1$ et $f(\overline{1}) = -1$ est un isomorphisme. La fonction $g : \mathbb{Z}/2\mathbb{Z} \to C_2$ définie par $g(\overline{0}) = -1$ et $g(\overline{1}) = 1$ n'en est pas un : c'est une bijection, mais ce n'est pas un morphisme de groupes !*
L'identité Id_G est un isomorphisme.

Proposition 2.10.

1. *Soit $f \in Hom(G, G')$ un isomorphisme, alors $f^{-1} \in Hom(G', G)$ est aussi un isomorphisme.*
2. *$Aut(G) = (End(G))^\times$ est un groupe pour la composition.*
3. *$Aut(G) \leq S_G$.*

Démonstration. Il faut seulement montrer que f^{-1} est un morphisme de groupes : soit $a', b' \in G'$ alors comme f est un morphisme de groupes on a

$$a' * b' = f(f^{-1}(a')) * f(f^{-1}(b')) = f(f^{-1}(a) \cdot f^{-1}(b)) \implies f^{-1}(a' * b') = f^{-1}(a) \cdot f^{-1}(b).$$

(2) et (3) sont des conséquences immédiates de ce qui précède. □

Remarque 20.

1. *Un morphisme de groupes f est un isomorphisme si et seulement si f est un morphisme de groupes bijectif. C'est-à-dire si et seulement si $Im(f) = G$ et $\ker(f) = \{e\}$.*
2. *Une fonction bijective n'est pas forcément un isomorphisme : il faut qu'elle soit aussi un morphisme de groupes.*

Définition 2.11. *On dit que deux groupes G et G' sont* isomorphes *si il existe au moins un isomorphisme de groupes $f : G \to G'$. On dit alors que G et G' sont dans la même* classe d'isomorphisme *et on note $G \simeq G'$.*

Remarque 21.

1. *La relation $\simeq$ est une relation d'équivalence (sur l'ensemble des groupes contenus dans un ensemble donné).*
2. *Cette notion est d'extrême importance, car elle signifie que si $G \simeq G'$, alors G et G' ont* exactement les mêmes propriétés algébriques. *Par exemple, G est abélien si et seulement si G' est abélien (à vérifier).*
3. *(Exercice) Soit $f : G \to G'$ un morphisme de groupes injectif alors*
   (a) $G \simeq f(G) = Im(f)$;
   (b) $ordre(f(x)) = ordre(x)$ pour tout $x \in G$.
   Par ailleurs ces résultats sont valides pour tout isomorphisme.
4. *(Exercice) Si $G \simeq G'$, alors pour tout $q \in \mathbb{N}^*$, le nombre d'éléments de G d'ordre q est égal au nombre d'élément de G' d'ordre q.*
5. *Soit G et G' deux groupes isomorphes, alors G et G' ont le même ordre : il existe une bijection entre eux et donc leurs cardinaux sont égaux (le cardinal d'un groupe est son ordre).*
6. *La réciproque n'est pas vraie car S_3 et $\mathbb{Z}/6\mathbb{Z}$ ont le même ordre mais ne sont pas isomorphes ; $\mathbb{Z}/6\mathbb{Z}$ possède 2 éléments d'ordre 6 tandis que S_3 n'en possède pas ! On pourrait aussi tout simplement dire que $\mathbb{Z}/6\mathbb{Z}$ est abélien tandis que S_3 ne l'est pas.*

2.4 Automorphismes intérieurs

Soit G un groupe et $g \in G$. La fonction

$$\begin{array}{rccc} \varphi_g : G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array}$$

est un automorphisme de groupe appelé *automorphisme intérieur de G*. En effet,

(i) φ_g est un endomorphisme : soit $x, y \in G$ alors

$$\varphi_g(xy) = gxyg^{-1} = gxeyg^{-1} = gx(g^{-1}g))yg^{-1}) = (gxg^{-1})(gyg^{-1}).$$

(ii) φ_g est inversible d'inverse $(\varphi_g)^{-1} = \varphi_{g^{-1}}$: pour $x \in G$ on a

$$\varphi_{g^{-1}} \circ \varphi_g(x) = \varphi_{g^{-1}}(gxg^{-1}) = g^{-1}(gxg^{-1})(g^{-1})^{-1} = g^{-1}(gxg^{-1})g = x = g(g^{-1}xg)g^{-1} = \varphi_g \circ \varphi_{g^{-1}}(x).$$

Donc $\varphi_{g^{-1}} \circ \varphi_g = \varphi_g \circ \varphi_{g^{-1}} = Id_G$.
On note $\mathrm{Int}\,(G)$ le groupe des automorphismes intérieurs de G.

Proposition 2.12. *Soit G un groupe. Alors $Int\,(G) \leq Aut\,(G)$.*

Démonstration. Exercice. □

2.5 Groupes symétriques et théorème de Cayley

Proposition 2.13. *Soit E un ensemble non vide.*

1. *Si F est un ensemble équipotent à E, alors $S_E \simeq S_F$;*
2. *Si $|E| = n$, alors $S_E \simeq S_n$.*

Démonstration. Soit $f : E \to F$ une bijection, f existe car E et F sont équipotents. Il suffit de montrer que la fonction

$$\begin{array}{rcl} \alpha : S_E & \to & S_F \\ g & \mapsto & f \circ g \circ f^{-1} \end{array}$$

est un isomorphisme de groupes. Soit

$$\begin{array}{rcl} \beta : S_F & \to & S_E \\ h & \mapsto & f^{-1} \circ h \circ f. \end{array}$$

Alors pour $g \in S_E$ on a

$$\beta \circ \alpha(g) = \beta(f \circ g \circ f^{-1}) = f^{-1} \circ (f \circ g \circ f^{-1}) \circ f = g.$$

Donc $\beta \circ \alpha = Id_{S_E}$. De même, on montre que $\alpha \circ \beta = Id_{S_F}$. Donc α est inversible et $\alpha^{-1} = \beta$
Il reste donc à montrer que α est un morphisme de groupe : soit $g, g' \in S_E$, alors

$$\alpha(g \circ g') = f \circ g \circ g' \circ f^{-1} = f \circ g \circ Id_E g' \circ f^{-1} = f \circ g \circ Id_E \circ g' \circ f^{-1} = (f \circ g \circ f^{-1}) \circ (f \circ g' \circ f^{-1}) = \alpha(g) \circ \alpha(g').$$

□

Le théorème qui suit explique l'importance du groupe symétrique.

Théorème 2.14 (Théorème de Cayley)**.** *Tout groupe G est isomorphe à un sous-groupe de S_G, le groupe de ses permutations.*

Démonstration. Il suffit de construire un morphisme de groupes injectif $f : G \to S_G$. Soit $g \in G$, la fonction

$$\begin{array}{rccc} f_g : G & \to & G \\ x & \mapsto & gx \end{array}$$

est une bijection, appelée *translation à gauche par* g (exercice). En outre, $f_g \in S_G$ et son inverse est $(f_g)^{-1} = f_{g^{-1}}$. Donc la fonction

$$\begin{array}{rccc} f : G & \to & S_G \\ g & \mapsto & f_g \end{array}$$

est bien définie.
(i) f est un morphisme de groupes : soit $g, h \in G$, alors $f(g) \circ f(h) = f_g \circ f_h = f_{gh} = f(gh)$ (exercice).
(ii) f est injective : soit $g \in \ker(f)$ alors $f_g = Id_G : x \mapsto x$. Donc $gx = x$ pour tout $x \in G$, d'où $g = e$ et f est injective. □

Exemple 2.15. *Comme* $|\mathbb{Z}/3\mathbb{Z}| = 3$*, alors* $\mathbb{Z}/3\mathbb{Z}$ *est isomorphe au sous-groupe de* S_3 *engendré par* $\sigma_1 = 231 = (123)$ *qui est le seul sous-groupe d'ordre* 3 *dans* S_3*.*

Chapitre 3

Classe modulo un sous-groupe et groupes quotients

Dans ce chapitre, nous allons développer deux outils très puissants pour l'étude des groupes : le théorème de Lagrange [1] et le premier théorème d'isomorphisme. Nous généraliserons aussi la construction du quotient $(\mathbb{Z}, +)$ par son sous-groupe $(n\mathbb{Z}, +)$, qui donne le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Nous montrerons alors que l'étude des groupes cycliques et monogènes revient à étudier les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$.

3.1 Classes modulo un sous-groupe

Rappelons la relation de congruence modulo n dans $\mathbb{Z}$:

$$a \equiv b \pmod{n} \text{ si et seulement si } (-a) + b \text{ appartient à } n\mathbb{Z}.$$

Dans la notation multiplicative, ceci ce traduit par :

$$a \equiv b \pmod{n} \text{ si et seulement si } a^{-1}b \text{ appartient à } n\mathbb{Z}.$$

On arrive alors à poser la définition suivante :

Définition 3.1. *Soit G un groupe et $H \leq G$. On définit sur G la relation suivante :*

$$x \equiv y \pmod{H} \iff x^{-1}y \in H.$$

Elle est appelée congruence à gauche modulo H.

Proposition 3.2. *Soit G un groupe et $H \leq G$.*

1. Joseph Louis Lagrange, 1736-1813.

1. $\equiv$ *est une relation d'équivalence ;*
2. *la classe d'équivalence de* $x \in G$ *est* $xH = \{xh \,|\, h \in H\}$. *Elle est appelée* classe à gauche modulo H.

Notation 4.

1. *On note* G/H *l'ensemble quotient pour la relation de congruence à gauche modulo* H.
2. *Si* x *appartient à* G *et* $\equiv$ *est une relation d'équivalence sur* G, *on note par* $\bar{x}_{\equiv}$ *ou bien par* $\bar{x}$ *la classe d'équivalence de* x *dans* G *:*

$$\bar{x} = \bar{x}_{\equiv} = \{y \in G \,|\, x \equiv y\}.$$

Remarque 22. *Soit* G *un groupe et* $H \leq G$.

(a) Si G *est noté additivement, on retrouve alors la notation* $x + H$ *pour la classe d'équivalence de* x *modulo* H. *Si* $G = \mathbb{Z}$ *et* $H = n\mathbb{Z}$ *alors la classe de* $k \in \mathbb{Z}$ *est* $k + n\mathbb{Z}$ *; et l'ensemble quotient est bien* $\mathbb{Z}/n\mathbb{Z}$.

(b) Soit $x \in G$ *alors* $xH = H$ *si et seulement si* $h \in H$ *;*
De plus $xH = yH \iff x^{-1}yH = H \iff y^{-1}xH = H \iff x^{-1}y \in H$ *(exercice).*

(c) On définit une congruence à droite modulo H *par*

$$x \equiv_d y \iff xy^{-1} \in H.$$

La classe d'équivalence de $x \in G$ *est* $Hx = \{hx \,|\, h \in H\}$ *et est appelée* classe à droite modulo H. *L'ensemble quotient est alors noté* $H\backslash G$. *Lorsqu'il n'existe pas de confusion, on note par* $\bar{x}$ *la classe d'équivalence de* x *dans* G *donnée par la relation* $\equiv_d$.
Notons que : $y \in xH \iff y^{-1} \in Hx^{-1}$.

(d) Si G *est abélien, alors* $xH = Hx$ *pour tout* $x \in G$.

(e) Si G *n'est pas abélien, ce n'est plus vrai. En effet, si* $G = S_3$, $H = \langle \tau_1 \rangle$ *avec* $\tau_1 = 213$, *et* $x = \sigma_1 = 231$ *alors*

$$xH = \{213, 321\} \quad et \quad Hx = \{231, 132\}.$$

On voit bien que $xH \neq Hx$.

(f) Un sous-groupe tel que $xH = Hx$ *pour tout* $x \in H$ *est appelé* sous-groupe normal. *C'est dans le cas des sous-groupes normaux que l'ensemble quotient sera alors muni d'une structure de groupe ; on y reviendra plus tard dans ce chapitre.*

Démonstration de la proposition 3.2. Il faut montrer que $\equiv$ est transitive, symétrique et réflexive. Soit $x, y, z \in G$ alors

- $\equiv$ est réflexive : $x^{-1}x = e \in H$ car $H \leq G$, donc $x \equiv x$;
- $\equiv$ est symétrique : si $x \equiv y$ alors $y^{-1}x = (x^{-1}y)^{-1} \in H$ car $H \leq G$, donc $y \equiv x$;

- $\equiv$ est transitive : si $x \equiv y$ et $y \equiv z$ alors $x^{-1}y \in H$ et $y^{-1}z \in H$, donc puisque H est stable on a

$$x^{-1}z = x^{-1}yy^{-1}z \in H \quad \Longrightarrow \quad x \equiv z.$$

Il reste à montrer que la classe $\bar{x}_{\equiv}$ de x est $xH = \{xh \,|\, h \in H\}$. Soit $y \in xH$, alors il existe $h \in H$ tel que $y = xh$. Donc $x^{-1}y = h \in H$ et il s'ensuit que $x \equiv y$ et $y \in \bar{x}_{\equiv}$. Donc $xH \subseteq \bar{x}_{\equiv}$.

Réciproquement, soit $y \in \bar{x}_{\equiv}$, i.e. $x \equiv y$, alors $h = x^{-1}y \in H$. Il existe alors $h \in H$ tel que $y = xh$, ce qui prouve l'égalité des ensembles. □

Étudions maintenant l'ensemble quotient.

Proposition 3.3. *Soit G un groupe et $H \leq G$, alors*

1. *pour tout $x \in G$, xH, Hx et H ont même cardinal.*
2. *Les ensembles quotients G/H et $H\backslash G$ sont en bijection.*

Démonstration. (1) Soit $x \in H$, alors la fonction $h \mapsto xh$ est une bijection de H sur xH (exercice).
(2) Soit $xH \in G/H$, posons $f(xH) = Hx^{-1}$. Montrons que $f : G/H \to H\backslash G$ est une fonction **bien définie**. C'est-à-dire, montrons que si $xH = yH$ alors $Hx^{-1} = Hy^{-1}$. Or on sait que

$$(\star) \quad xH = yH \iff x^{-1}y \in H \iff H = Hx^{-1}y \iff Hy^{-1} = Hx^{-1}.$$

Ce qui montre que f est bien définie. Montrons que f est une bijection :

- f est injective : $f(xH) = f(yH) \iff Hy^{-1} = Hx^{-1} \iff xH = yH$ par $(\star)$.
- f est surjective : si $Hx \in H\backslash G$, alors $f(x^{-1}H) = H(x^{-1})^{-1} = Hx$. □

On peut alors donner la définition suivante.

Définition 3.4. *Soit G un groupe et $H \leq G$.* L'indice de H dans G, *noté $[G : H]$, est le cardinal de l'ensemble G/H (qui est égal au cardinal de $H\backslash G$). Si G/H est un ensemble fini, on dit que* H est d'indice fini dans G.

Exemple 3.5. *$[\mathbb{Z} : n\mathbb{Z}] = n$. L'indice peut être fini alors que G et H sont infinis !*

3.1.1 Le théorème de Lagrange

Soit $n \in \mathbb{N}^*$ tel que $x^n = e$. Alors $ordre(x)$ divise n. En effet, en effectuant la division euclidienne de n par $ordre(x)$ on obtient $n = ordre(x)q + r$ avec $0 \leq r < ordre(x)$. Donc

$$e = x^n = (x^{ordre(x)})^q x^r = x^r.$$

Mais comme $ordre(x)$ est le plus petit entier positif tel que $x^{ordre(x)} = e$, on a forcément $r = 0$ et donc $n = ordre(x)q$.

On peut se demander comment trouver un tel n au départ, surtout si on ne connaît pas l'ordre de x. En regardant tous les exemples de groupes finis des chapitres 1 et 2, on peut observer que les ordres des éléments divisent l'ordre du groupe. Ce résultat est général.

Théorème 3.6 (Théorème de Lagrange)**.** *Soit G un groupe fini et $H \leq G$ alors*

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

En particulier, l'ordre de tout sous-groupe de G divise l'ordre de G et l'ordre de tout élément de G divise l'ordre de G.

Démonstration. Comme $\equiv$ est une relation d'équivalence, G/H est une partition de G. On obtient alors

$$|G| = \sum_{xH \in G/H} |xH| = \sum_{xH \in G/H} |H| = |G/H||H| = |H|[G : H].$$

Puisque l'ordre de $x \in G$ est l'ordre du sous-groupe $\langle x \rangle$, on obtient bien l'ordre de tout élément de G divise $|G|$. □

Corollaire 3.7. *Soit G un groupe fini d'ordre n, alors $x^n = e$ pour tout $x \in G$.*

Démonstration. Soit $x \in G$. En vertu du théorème de Lagrange, $ordre(x)$ divise $|G| = n$. Alors il existe $k \in \mathbb{N}$ tel que $n = k\, ordre(x)$. D'où

$$x^n = x^{k\, ordre(n)} = (x^{ordre(n)})^k = e^k = e.$$

□

Corollaire 3.8. *Soit G un groupe d'ordre p premier, alors G est cyclique.*

Démonstration. Exercice. □

3.1.2 Application à l'arithmétique modulaire

Le petit théorème de Fermat généralisé

Voici la généralisation du petit théorème de Fermat [2] par Gauss [3] .

Théorème 3.9 (Fermat-Euler)**.** *Soit $n \in \mathbb{N}^*$ et a un entier premier avec n alors*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

où φ est l'indicatrice d'Euler [4]*.*

Démonstration. Comme a est premier avec n, $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ qui est un groupe multiplicatif d'ordre $\varphi(n)$. En vertu du corollaire du théorème de Lagrange ci-dessus, $\overline{a}^{\,\varphi(n)} = \overline{1}$. □

2. Pierre Fermat, 1601-1665.
3. Carl Friedrich Gauss, 1777-1855.
4. Leonhard Euler, 1707-1783.

Le cryptage RSA

La plupart des cryptages informatiques actuels (SSH, SSL) font appel à l'algorithme de cryptage RSA [5].

Pourquoi ça marche ? Le cryptage RSA est très efficace car il est basé sur deux principes : la puissance modulaire, qui n'est pas une fonction réversible, et le fait que la difficulté à factoriser les grands nombres en nombres premiers excède la capacité de calcul des ordinateurs actuels.

Clef publique et privée : On se donne une *clef publique* (n, e) où $n, e \in \mathbb{N}^*$ sont tels que :

1. $n = pq$ où p, q sont deux nombres premiers très grands (c'est ce qu'on appelle un grand nombre).

   Lemme 3.10. *Si $n = pq$ avec $p \neq q$ nombres premiers, alors $\varphi(n) = (p-1)(q-1)$.*

   Démonstration. En effet, $k \leq n$ n'est pas premier avec pq si et seulement si p ou q est diviseur de k. Donc $k \leq n$ est premier avec n si et seulement si p et q ne sont pas diviseurs de k. Donc $k \in \{ab \,|\, 1 \leq a < p, 1 \leq b < q\}$ de cardinal $(p-1)(q-1)$ est l'ensemble des nombres plus petits que n et premiers avec n, d'où le résultat. □

2. e est premier avec $\varphi(n) = (p-1)(q-1)$, donc inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$.

La clef publique est détenue par tout le monde, i.e., le programme de cryptage générique.

On se donne aussi une *clef privée* (n, d) où d est tel que : $\overline{d}$ est l'inverse de $\overline{e}$ dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$. Il est très difficile de calculer $\overline{d}$, même si l'on connaît e.

Chiffrement d'un message : On se donne un message M (un nombre plus petit que n). Le programme connaît la clef publique (n, e). On rappelle que n est un grand nombre. Alors le chiffrement est : $C \equiv M^e \pmod{n}$.

Déchiffrement du message : Pour déchiffrer C, on procède comme suit. Le receveur connaît la clef privée (n, d), donc il ne lui reste qu'à calculer C^d modulo n. Le résultat sera le message M.

Remarque 23. *Pour calculer d à l'aide de la clef publique (n, e), il faut résoudre l'équation diophantienne de $+\varphi(n)k = 1$, ce qui revient à connaître la décomposition $n = pq$ dont la complexité de calcul excède la capacité de nos ordinateurs.*

Exemple 3.11. *On prend un petit exemple pour illustrer le processus. Dans la pratique on prend des très grands nombres. On prend $p = 7$ et $q = 5$ et $n = 5 \cdot 7 = 35$. Donc $\varphi(n) = (5-1)(7-1) = 24$.*

- *La clef publique est $(n = 35, e = 5)$.*
- *La clef privée est $(n = 35, d = 5)$. En effet $5 \cdot 5 = 1 + 1 \cdot 24 \equiv 1 \pmod{\varphi(n)}$.*

5. Rivest, Shamir et Adleman (1977).

– *Le message est* $M = 8$.

Le message crypté est $C = M^e = 8^5 = 32768$.

Essayons de retrouver le message. Calculons modulo 35 *:*

$$(32768)^d \equiv (32768)^5 \equiv 4768^5 \equiv 218^5 \equiv 8^5 \equiv 64 \cdot 64 \cdot 8 \equiv -6 \cdot (-6) \cdot 8 \equiv 36 \cdot 8 \equiv 8 \pmod{35}.$$

On retrouve bien $M = 8$.

Démonstration. En effet,

$$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M \cdot M^{\varphi(n)k} = M \cdot (M^{\varphi(n)})^k \pmod{n}$$

car $ed \equiv 1 \pmod{\varphi(n)}$ ($\overline{e} = \overline{d}^{\,-1}$). Donc si M est premier avec n, on obtient en vertu du petit théorème de Fermat généralisé par Euler que

$$C^d \equiv M \pmod{n}.$$

Si M n'est pas premier avec n, puisque $M < n$, alors $p|M$ ou $q|M$. Si $p|M$ alors

$$M^{ed} \equiv 0 \equiv M \pmod{p}.$$

Si p ne divise pas M alors en vertu du petit théorème de Fermat on a

$$M^{p-1} \equiv 1 \pmod{p} \Longrightarrow M^{ed} \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \pmod{p}.$$

En procédant de même avec q, on en déduit que p et q divisent $M^{ed} - M$ donc n aussi divise $M^{ed} - M$. D'où

$$C^d \equiv M^{ed} \equiv M \pmod{n}.$$

Puisque $M < n$, le résultat de ce calcul est M ! □

3.2 Groupes quotients

L'ensemble quotient G/H admet-il une structure de groupe héritée de G, tel $\mathbb{Z}/n\mathbb{Z}$ a sa structure héritée de $\mathbb{Z}$?

3.2.1 Sous-groupes normaux

Définition 3.12. *Soit G un groupe et $H \leq G$, on dit que H est un sous-groupe* normal dans G *ou* distingué dans G *si $xH = Hx$ pour tout $x \in G$.*

Notation 5. *Si H est un sous-groupe normal de G, on note $H \lhd G$.*

Proposition 3.13. *Soit G un groupe et $H \leq G$, montrer que les propositions suivantes sont équivalentes.*

1. $H \lhd G$;
2. $xHx^{-1} = H$, *pour tout* $x \in G$;
3. $x^{-1}Hx = H$, *pour tout* $x \in G$;
4. $xhx^{-1} \in H$, *pour tout* $x \in G$, *pour tout* $h \in H$;
5. $x^{-1}hx \in H$, *pour tout* $x \in G$, *pour tout* $h \in H$.

Démonstration. Exercice. □

Exemples 6.

1. *Le centre du groupe $Z(G)$ est normal dans G. En effet, si $x \in G$, alors $xg = gx$ pour tout $g \in Z(G)$. Donc $xZ(G) = Z(G)x$.*
2. *$Int(G) \lhd Aut(G)$.*
3. *Si G est un groupe abélien, tout sous-groupe est normal dans G.*
4. *L'intersection de sous-groupes normaux dans G est un sous-groupe normal dans G.*

Remarque 24. *Soit G un groupe et $K \leq H \leq G$.*

1. **$\lhd$ n'est pas une relation transitive** *: si $K \lhd H$ et $H \lhd G$,* **il n'est pas vrai** *que $H \lhd G$. On trouve un contre-exemple dans S_4 (exercice).*
2. *si $K \lhd G \Longrightarrow K \lhd H$: en effet, $xK = Kx$ pour tout $x \in G$ donc aussi pour tout $x \in H$.*
3. *Si $H \lhd G$ et $K \leq G$ contenant H alors $H \lhd K$ (exercice).*

3.2.2 Groupe quotient

Théorème 3.14. *Soit G un groupe et H un sous-groupe normal de G, alors la fonction*

$$\begin{array}{rcl} G/H \times G/H & \longrightarrow & G/H \\ (xH, yH) & \mapsto & xH \cdot yH = xyH \end{array}$$

munit G/H d'une structure de groupe. On l'appelle le groupe quotient de G par H. *De plus*

(i) $e_{G/H} = H \quad et \quad (xH)^{-1} = x^{-1}H$;

(ii) la fonction $\pi : G \to G/H$ définie par $\pi(x) = xH$ est un morphisme de groupe surjectif appelé épimorphisme canonique ;

(iii) $\ker(\pi) = H$.

Remarque 25. *En notation additive, on obtient commme loi de composition interne :* $(x+H)+(y+H)=(x+y)+H$*, ce qui correspond bien à notre addition sur* $\mathbb{Z}/n\mathbb{Z}$ *!*

Démonstration du théorème 3.14. La preuve est entièremen similaire à la démonstration du fait que $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe (on remplace l'addition par la multiplication, $\mathbb{Z}$ par G et $\mathbb{Z}$ par H ; seule la commutativité manque, mais le fait que H est un sous-groupe normal de G nous donne les hypothèses suffisantes pour prouver le résultat).

La difficulté de la preuve de ce théorème n'est pas de vérifier les axiomes de groupes, mais plutôt de montrer que le produit est *bien défini*. Soit $xH, x'H, x'H, y'H$ tel que $xH = x'H$ et $yH = y'H$, il faut montrer que $xyH = x'y'H$. Puisque $H \lhd G$, on obtient

$$x'y'H = x'Hy' = (x'H)y' = (xH)y' = xy'H = x(y'H) = xyH.$$

Montrons maintenant que les axiomes de groupes sont satisfaits : Soit $xH, yH, zH \in G/H$, alors

- *associativité :* $(xH \cdot yH) \cdot zH = (xyH) \cdot zH = (xy)zH = x(yz)H = xH \cdot (yH \cdot zH)$ car la loi de G est associative ;
- *élément neutre :* $xH \cdot H = xH = H \cdot xH$ car $H = eH$. Donc $e_{G/H} = eH = H$;
- *inverse :* $xH \cdot X^{-1}H = xx^{-1}H = H = x^{-1}H \cdot XH$ donc xH est inversible d'inverse $x^{-1}H$.

Enfin, on constate que $\pi(xy) = xyH = xH \cdot yH = \pi(x) \cdot \pi(y)$ donc π est un morphisme de groupe clairement surjectf ; de plus : $\ker(\pi) = \pi^{-1}(e_{G/H}) = \pi^{-1}(H) = \{x \in G \,|\, xH = H\} = H$. □

Théorème 3.15. *Soit G un groupe et $H \leq G$, alors $H \lhd G$ si et seulement si il existe un morphisme de groupes $f : G \to G'$ tel que $H = \ker(f)$.*
En particulier, $\ker(f) \lhd G$*, pour tout morphisme de groupes $f : G \to G'$.*

Démonstration. Si $H \lhd G$, il suffit de prendre $f = \pi : G \to G/H$. Réciproquement, il suffit de montrer que $\ker(f) \lhd G$: soit $x \in G$ et $g \in \ker(f)$, alors $f(xgx^{-1}) = f(x)f(g)f(x)^{-1}f(x)e_{G'}f(x)^{-1} = e_{G'}$ car $g \in \ker(f)$ et f est un morphisme de groupes. Ainsi $xgx^{-1} \in \ker(f)$, le noyau est donc normal dans G en vertu de la proposition 3.13. □

Il est utile de considérer les groupes quotients pour faire des arguments par récurrence dans les groupes finis. Nous allons donner un exemple. Rappelons que, dans un groupe, l'ordre d'un élément x est le plus entier naturel n (s'il existe) tel que $x^n = e$, où e désigne l'élément neutre de G.

Proposition 3.16. *Soit G un groupe abélien fini tel que tout élément de G est d'ordre une puissance de 3. Alors le cardinal de G est une puissance de 3.*

Démonstration. On procède par récurrence sur le cardinal de G, noté $|G|$. Supposons G tel que pour tout $g \in G$, $ordre(g)$ est une puissance de 3. À VOIR : $|G|$ est une puissance de 3.

Soit $g \in G$, $g \neq e$, disons $ordre(g) = 3^{n_0}$.

1) Cas de base. Si $G = \{e, g, \ldots, g^{3^{n_0}-1}\}$, c'est-à-dire g est le groupe cyclique engendré par g, alors on a fini.

2) Récurrence. Autrement, posons $H = \{e, g, \ldots, g^{3^{n_0}-1}\}$. On a $H \subset G$, $|H| < |G|$. L'hypothèse de récurrence est que le résultat est vrai pour tous les groupes abéliens finis dont le cardinal est plus petit que $|G|$.
Considérons G/H. Comme G est abélien, H est un sous-groupe normal et G/H est un groupe. C'est un groupe abélien fini dont le cardinal est $|G/H| = \frac{|G|}{|H|}$ qui est plus petit que $|G|$. Pour utiliser l'hypothèse de récurrence il faut aussi vérifier que l'ordre de tout élément de G/H est une puissance de 3. Considérons l'homomorphisme naturel

$$G \to G/H$$

$$g \mapsto gH$$

Disons $g^{3^n} = e$, alors $(gH)^{3^n} = g^{3^n}H = eH = e_{G/H}$. Donc, 3^n est un multiple de $ordre(gH)$. D'où $ordre(gH)$ est une puissance de 3. On peut donc appliquer l'hypothèse de récurrence à G/H et on obtient que $|G/H|$ est une puissance de 3. Disons $|G/H| = 3^{n_1}$. On obtient

$$|G/H| = \frac{|G|}{|H|} = \frac{|G|}{3^{n_0}} = 3^{n_1}$$

$$|G| = 3^{n_0+n_1}$$

et donc $|G|$ est bien une puissance de 3.

Cela complète la récurrence. □

3.2.3 Premier théorème d'isomorphisme

On va maintenant pouvoir énoncer un théorème de première importance en algèbre, appelé *propriété universelle des groupes quotients, ou premier théorème d'isomorphisme.*

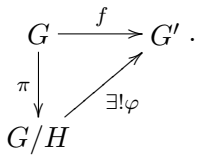
Théorème 3.17 (Premier théorème d'isomorphisme)**.** *Soit G un groupe, $H \lhd G$ et $\pi : G \to G/H$ la surjection canonique. Soit $f : G \to G'$ un morphisme de groupes tel que $H \subseteq \ker(f)$, alors il existe un unique morphisme $\varphi : G/H \to G'$ tel que $f = \varphi \circ \pi$. De plus*

(i) si $H = \ker(f)$ alors φ est injective ;

(ii) si f est surjective, alors φ est surjective.

Plus spécifiquement, si f est surjective et $H = \ker(f)$ alors φ est un isomorphisme.

Remarque 26. *On peut mémoriser ce résultat en le résumant dans le diagramme suivant*[6] *:*



6. On dit que le diagramme est *commutatif*, puisque $f = \varphi \circ \pi$.

Exemples 7.

1. *Si $f : G \to G'$ est un morphisme de groupes, alors $G/\ker(f) \simeq Im(f)$ (exercice).*
2. *En outre, en vertu du théorème de Lagrange, le groupe alterné $A_n = \ker(\epsilon)$ est d'ordre $|A_n| = n!/2$.*
3. *$(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$. En effet, $\mathbb{R} \lhd \mathbb{C}$ car $(\mathbb{C}, +)$ est abélien. De plus, le morphisme de groupes $f : \mathbb{C} \to \mathbb{R}$, défini par $f(a + ib) = b$, est surjectif. Son noyau est $\ker(f) = \mathbb{R}$, donc en vertu du théorème d'isomorphisme, il existe un isomorphisme $\varphi : \mathbb{C}/\mathbb{R} \to \mathbb{R}$. D'où $\mathbb{C}/\mathbb{R} \simeq \mathbb{R}$.*

Démonstration du théorème 3.17.

Unicité : Soit φ et φ' tel que $f = \varphi \circ \pi = \varphi' \circ \pi$. Soit $x \in G$ alors $f(x) = \varphi \circ \pi(x) = \varphi' \circ \pi(x)$, donc $\varphi(\pi(x)) = \varphi'(\pi(x))$. Donc pour tout $xH \in G/H$ on a $\varphi(xH) = \varphi'(xH)$. D'où $\varphi = \varphi'$ car deux fonctions sont égales si et seulement si leurs valeurs sur tous les éléments de l'ensemble de départ sont égales.

Existence : Commençons par montrer que la fonction $\varphi : G/H \to G'$ définie par $\varphi(xH) = f(x)$, $x \in G$, est bien définie. Pour cela, il faut montrer que si $xH = yH$ alors $f(x) = f(y)$. Ainsi, soit $x, y \in G$ tel que $xH = yH$. Donc $x^{-1}yH = H$ et donc $x^{-1}y \in H \subseteq \ker(f)$. D'où $f(x^{-1}y) = e_{G'}$. Comme f est un morphisme de groupes, on obtient que $f(x)f(y)^{-1} = e_{G'}$ et donc que $f(x) = f(y)$. La fonction φ est bien définie.
Il reste à montrer que φ est un morphisme de groupes, que si $\ker(f) = H$ alors φ est injective et que si f est surjective, alors φ l'est aussi.

- φ est un morphisme de groupe car : si $xH, x'H \in G/H$ alors puisque f est un morphisme de groupes on obtient

$$\varphi(xH \cdot x'H) = \varphi(xx'H) = \varphi \circ \pi(xx') = f(xx') = f(x)f(x') = \varphi \circ \pi(x)\varphi \circ \pi(x') = \varphi(xH)\varphi(x'H).$$

- φ est surjective si f l'est : soit $y \in G'$, alors il existe $x \in G$ tel que $f(x) = y$. D'où

$$\varphi(xH) = \varphi \circ \pi(x) = f(x) = y.$$

- φ est injective si $H = \ker(f)$: soit $xH, x'H \in G/H$ tel que $\varphi(xH) = \varphi(x'H)$, alors $f(x) = f(x')$. Autrement dit, et en utilisant le fait que f est un morphisme de groupes, on a $f(x^{-1}x') = e_{G'}$. Donc $x^{-1}x' \in \ker(f) = H$. On en déduit que $x^{-1}x'H = H$ et donc que $x'H = xH$. En d'autres termes, φ est bien injective. □

3.2.4 Sous-groupes d'un groupe quotient

On a vu que les sous-groupes du groupe quotient $(\mathbb{Z}/n\mathbb{Z}, +)$ correspondent aux sous-groupes de $(\mathbb{Z}, +)$ contenant $n\mathbb{Z}$. On montre ici que ce phénomène est vrai en général.

Théorème 3.18. *Soit G un groupe, $H \lhd G$ et $\pi : G \to G/H$ l'épimorphisme canonique. Alors la fonction $K \mapsto \pi(K)$ est une bijection de l'ensemble des sous-groupes de G contenant H sur l'ensemble des sous-groupes de G/H.*

Remarque 27.

1. *Autrement dit, L est un sous-groupe de G/H si et seulement si il existe $K \leq G$ tel que $H \subseteq K$ et $\pi(K) = L$.*
2. *Si $K = \langle S \rangle$ alors $\pi(K) = \langle \pi(S) \rangle$ (exercice).*
3. *Si K est fini, alors en vertu du théorème de Lagrange $|\pi(K)| = |K|/|H|$ (exercice).*
4. *Si K est un sous-groupe de G contenant H alors $H \lhd K$ et donc le groupe quotient K/H existe. D'autre part, grâce au théorème ci-dessus on sait que $\pi(K) \leq G/H$. Ainsi, en vertu du théorème d'isomorphimme que $\pi(K) \simeq K/H$ (exercice).*

Exemple 3.19. *On retrouve ainsi le résultat connu suivant : soit $n \in \mathbb{N}$ alors les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $\pi(k\mathbb{Z}) = \langle \overline{k} \rangle$ tel que $k|n$ et sont d'ordre n/k. Mais grâce à la remarque ci-dessus, on a aussi que $\pi(k\mathbb{Z}) \simeq k\mathbb{Z}/n\mathbb{Z}$. On verra dans la section suivante qu'en fait $\pi(k\mathbb{Z}) \simeq \mathbb{Z}/(n/k)\mathbb{Z}$ car c'est un groupe cyclique d'ordre n/k.*

Démonstration du théorème. À nouveau, les arguments de la preuve sont les même que dans le cas des groupes $\mathbb{Z}/n\mathbb{Z}$. Soit $K \leq G$ qui contient H. Montrons que $\overline{K} = \pi(K)$ est un sous-groupe de G/H. On a $H = e_{G/H} \in \overline{K}$ car $H \subseteq K$ implique que $\pi(H) = H \subseteq \pi(K) = \overline{K}$. Soit $xH, yH \in \overline{K}$, $x, y \in K$, alors $xH(yH)^{-1} = xy^{-1}H = \pi(xy^{-1}) \in \pi(K) = \overline{K}$ car $K \leq G$. Donc $\overline{K} \leq G/H$.

Donc la fonction $K \to \pi(K)$ est bien définie de l'ensemble des sous-groupes de G contenant H dans l'ensemble des sous-groupes de G/H. Il reste à montrer qu'elle est bijective.
Surjective : Soit $L \leq G/H$, posons $K = \pi^*(L) = \{g \in G \,|\, \pi(g) \in L\}$. Alors $e \in K$ car $\pi(e) = e_{G/H} \in L$. Si $x, y \in K$ alors puisque π est un morphisme de groupes on a $\pi(xy^{-1}) = \pi(x)\pi(y)^{-1} \in L$ car $L \leq G/H$, donc $xy^{-1} \in K$. Donc $K \leq G$. L'application est surjective.
Injective : Soit K, K' deux sous-groupes de G contenant H tel que $\pi(K) = \pi(K')$. Par symétrie, il suffit de montrer que $K \subseteq K'$ pour montrer que $K = K'$ et donc son injectivité. Soit $x \in K$ alors $\pi(x) \in \pi(K) = \pi(K')$. Donc $xH = yH$ avec $y \in K'$. Ce qui implique qu'il existe $h \in H$ tel que $x = yh$. Puisque $H \subseteq K'$, $y, h \in K'$. En outre, puisque $x = yh$ et $K' \leq G$, on obtient que $x \in K'$. □

3.3 Applications

3.3.1 Groupes monogènes et cycliques

Nous allons voir que l'étude des groupes monogène et cycliques se réduit à l'étude du groupe monogène $\mathbb{Z}$ et des groupes cycliques $\mathbb{Z}/n\mathbb{Z}$.

Théorème 3.20. *Soit $G = \langle x \rangle$ un groupe monogène, alors*

1. *Si G est infini, alors $G \simeq (Z, +)$.*
2. *Si G est fini d'ordre n, alors $G \simeq (Z/n\mathbb{Z}, +)$.*

Démonstration. On considère $f : \mathbb{Z} \to G$ définie par $f(n) = x^n$. Alors f est un morphisme de groupes : $f(n+m) = x^{n+m} = x^n x^m = f(n)f(m)$ (on notera que $\mathbb{Z}$ est un groupe noté additivement tandis que G est noté multiplicativement). Il est clair que f est surjective. Si $\ker(f) = \{0\}$ alors $G \simeq \mathbb{Z}$.

Si $\ker(f)$ n'est pas 0 alors il existe $k \in \mathbb{Z}$ tel que $\ker(f) = k\mathbb{Z}$ car $\ker(f)$ est un sous-groupe de $\mathbb{Z}$ et les seuls sous-groupes de $\mathbb{Z}$ sont les ensembles de multiples. Donc en vertu du théorème d'isomorphismes, $G \simeq \mathbb{Z}/k\mathbb{Z}$. Puisque $n = |G| = |\mathbb{Z}/k\mathbb{Z}| = k$, on en déduit le théorème. □

Corollaire 3.21. *Tout sous-groupe d'un groupe cyclique est cyclique.*

Démonstration. Soit G un groupe cyclique, alors $G \simeq (\mathbb{Z}, +)$ ou $G \simeq (\mathbb{Z}/n\mathbb{Z}, +)$. Les sous-groupes de G sont donc isomorphes à des sous-groupes de $(\mathbb{Z}, +)$ ou de $(\mathbb{Z}/n\mathbb{Z}, +)$ qui sont tous cycliques. Donc par isomorphisme inverse, les sous-groupes de G sont cycliques (s'en convaincre en faisant l'exercice). □

Exemples 8.

1. *Soit* $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$. *On a* $\mathbb{U} \leq (\mathbb{C}^*, \cdot)$ *et* $\mathbb{U} \simeq (\mathbb{R}, +)/ < 2\pi >$.
2. *(Racines nième de l'unité) Soit* $n \in \mathbb{N}$, *on dit que* $z \in \mathbb{C}$ *est une* racine $n$ième de l'unité *si* $z^n = 1$. *On note* $\mathbb{U}(n)$ *l'ensemble des racines nième de l'unité. Soit* $n \in \mathbb{N}$, *alors* $\mathbb{U}(n)$ *est un sous-groupe cyclique fini de* $\mathbb{U}$ *isomorphe à* $\mathbb{Z}/n\mathbb{Z}$. *Il est engendré par* $e^{2i\pi/n}$.

Chapitre 4

Les produits directs de groupes

On peut construire de nouveaux groupes à partir de groupes qu'on a déjà à l'aide de la construction du *produit direct*. À l'inverse, on peut reconnaître qu'un groupe est isomorphe à un produit direct, ce qui nous donne en quelque sorte une idée de sa structure. Nous allons étudier cette construction et cette décomposition.
Dans les chapitres suivants, nous allons désigner les ensembles $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}_n$ pour alléger la notation.

4.1 Le produit direct externe

Soient G, H deux groupes et considérons le produit cartésien

$$G \times H = \{(g, h) : g \in G, h \in H\}.$$

On définit sur $G \times H$ une structure de groupe à l'aide des relations suivantes

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

$$e_{G\times H} = (e_G, e_H)$$
$$(g, h)^{-1} = (g^{-1}, h^{-1})$$

En effet, on a

$$(g, h) \cdot (e_G, e_H) = (g e_G, h e_h) = (g, h)$$
$$(e_G, e_H)(g, h) = (e_G g, e_H h) = (g, h)$$
$$(g, h) \cdot (g^{-1}, h^{-1}) = (g g^{-1}, h h^{-1}) = (e_G, e_H)$$
$$(g^{-1}, h^{-1}) \cdot (g, h) = (g^{-1} g, h^{-1} h) = (e_G, e_H)$$
$$((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) = (g_1 g_2, h_1, h_2) \cdot (g_3, h_3) = ((g_1 g_2) g_3, (h_1 h_2) h_3)$$

$$(g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)) = (g_1, h_1) \cdot (g_2 g_3, h_2 h_3) = (g_1(g_2 g_3), h_1(h_2 h_3))$$

Cela montre bien que l'opération que nous avons définie est associative avec élément neutre (e_G, e_H) et que l'inverse que nous avons défini marche. Ces données font bien de $G \times H$ un groupe.

Définition 4.1. *Soient G, H des groupes. Le groupe que nous venons de définir avec le produit cartésien de G avec H est appelé* le produit direct *,ou* produit direct externe*, de G avec H. Il est noté $G \times H$.*

Exercice 4.2. *Soient G, H des groupes abéliens. Alors $G \times H$ est aussi un groupe abélien.*

Exemple 4.3. *On a $\mathbb{Z} \times \mathbb{Z}$.*

Exemple 4.4. *On a $\mathbb{Z}_2 \times \mathbb{Z}_3$, qui donne un groupe d'ordre 6.*

Exemple 4.5. *On a $\mathbb{Z}_2 \times \mathbb{Z}_2$, qui donne un groupe d'ordre 4, mais qui n'est pas isomorphe à $\mathbb{Z}_4$. En effet, dans $\mathbb{Z}_2 \times \mathbb{Z}_2$ on a pour tous g, $g + g = e$, ce qui n'est pas le cas dans $\mathbb{Z}_4$.*

Exemple 4.6. *On a $\mathbb{Z}_2 \times \mathbb{Z}_4$, qui donne un groupe d'ordre 8, mais qui n'est pas isomorphe à $\mathbb{Z}_8$. En effet, dans $\mathbb{Z}_2 \times \mathbb{Z}_4$ on a pour tous g, $g + g + g + g = e$, ce qui n'est pas le cas dans $\mathbb{Z}_8$.*

Exercice 4.7. *Soient G, H des groupes. Selon l'ordre choisi pour faire le produit cartésien, on obtient deux groupes, $G \times H$ et $H \times G$. Vérifiez que l'application $f : G \times H \to H \times G$ définie par $f(g, h) = (h, g)$ est un isomorphisme.*

La construction du produit direct de groupes se fait avec plus de deux facteurs. Soient $G_1, \ldots, G_n$ des groupes. Considérons le produit cartésien

$$G_1 \times \ldots \times G_n = \{(g_1, \ldots, g_n) : g_1 \in G_1, \ldots, G_n \in G_n\}$$

On définit sur $G_1 \times \ldots \times G_n$ une structure de groupe à l'aide des relations suivantes

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$$

$$e_{G_1 \times \ldots \times G_n} = (e_{G_1}, \ldots, e_{G_n})$$
$$(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$$

En effet, on a

$$(g_1, \ldots, g_n) \cdot (e_{G_1}, \ldots, e_{G_n}) = (g_1 e_{G_1}, \ldots, g_n e_{G_n}) = (g_1, \ldots, g_n)$$
$$(e_{G_1}, \ldots, e_{G_n}) \cdot (g_1, \ldots, g_n) = (e_{G_1} g_1, \ldots, e_{G_n} g_n) = (g_1, \ldots, g_n)$$
$$(g_1, \ldots, g_n) \cdot (g_1^{-1}, \ldots, g_n^{-1}) = (g_1 g_1^{-1}, \ldots, g_n g_n^{-1}) = (e_{G_1}, \ldots, e_{G_n})$$
$$(g_1^{-1}, \ldots, g_n^{-1}) \cdot (g_1, \ldots, g_n) = (g_1^{-1} g_1, \ldots, g_n^{-1} g_n) = (e_{G_1}, \ldots, e_{G_n})$$

Exercice 4.8. *Vérifiez que l'opération que nous avons définie sur $G_1 \times \ldots \times G_n$ est associative.*

Cela montre que l'opération que nous avons définie est associative avec élément neutre $(e_{G_1}, \ldots, e_{G_n})$ et que l'inverse que nous avons défini marche. Ces données font bien de $G_1 \times \ldots \times G_n$ un groupe.

Définition 4.9. *Soient $G_1, \ldots, G_n$ des groupes. Le groupe que nous venons de définir avec le produit cartésien de $G_1, \ldots, G_n$ est appelé* le produit direct *,ou* produit direct externe*, des G_i. Il est noté $G_1 \times \ldots \times G_n$, ou quelquefois $\Pi_{i=1}^n G_i$.*

Exemple 4.10. *On a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, qui donne un groupe d'ordre 8. Il n'est pas isomorphe à $\mathbb{Z}_8$ ni à $\mathbb{Z}_2 \times \mathbb{Z}_4$. Pouvez-vous en donner une raison ?*

Exercice 4.11. *Montrez que le produit direct de groupes abéliens donne un groupe abélien.*

4.2 Quelques isomorphismes

Exemple 4.12. *On montre que $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$.*

Proposition 4.13. *Soient $f : A \to C$ et $g : B \to D$ des isomorphismes de groupes. Alors*

$$\varphi : A \times B \to C \times D$$

définie par

$$\varphi(a, b) = (f(a), g(b))$$

est un isomorphisme de groupes.

Démonstration. Exercice. □

Soient H, K des parties d'un groupe, rappelons que HK désigne la partie de G suivante :

$$\{xy : x \in H \text{ et } y \in K\}.$$

Proposition 4.14. *Soient A, B des groupes. Posons $G = A \times B$, $H = A \times \{e_B\}$, $K = \{e_A\} \times B$. Alors $H \lhd G, K \lhd G$, $H \cap K = \{e\}$ et $G = HK$.*

Proposition 4.15. *Soient G un groupe. Supposons A, B des sous-groupes de G tels que*

i) $A \lhd G, B \lhd G$.

ii) $A \cap B = \{e\}$.

iii) $G = AB$.

Alors $G \simeq A \times B$.

Démonstration. Considérons l'application

$$\varphi : A \times B \to G$$

$$\varphi(a, b) = ab$$

La condition (iii) dit précisément que cette fonction est surjective. C'est aussi un homomorphisme puisqu'on a

$$\varphi((a_1, b_1) \cdot (a_2, b_2)) = \varphi(a_1 a_2, b_1 b_2) = a_1 a_2 b_1 b_2$$

$$\varphi(a_1, b_1) \cdot \varphi(a_2, b_2) = (a_1 b_1) \cdot (a_2 b_2) = a_1 b_1 a_2 b_2$$

mais notons que $a_2 b_1 = b_1 a_2$, ou autrement dit $a_2 b_1 a_2^{-1} b_1^{-1} = e$. En effet, $a_2 b_1 a_2^{-1} \in B$ car $B \lhd G$, et donc $a_2 b_1 a_2^{-1} b_1^{-1} \in B$; aussi $b_1 a_2^{-1} b_1^{-1} \in A$ car $A \lhd G$ et donc $a_2 b_1 a_2^{-1} b_1^{-1} \in A$; donc $a_2 b_1 a_2^{-1} b_1^{-1} \in A \cap B$, d'où le résultat. L'homomorphisme φ est injectif, car si $\varphi(a, b) = e$, c'est-à-dire $ab = e$, alors $a = b^{-1} \in A \cap B$; d'où $a = e$, $b^{-1} = e$, et $b = e$, et ainsi $(a, b) = (e, e) = e_{A \times B}$. □

4.3 Le produit direct interne

La proposition précédente motive la définition suivante.

Définition 4.16. *Soient G un groupe et H, K des sous-groupes de G tels que*

i) $H \lhd G, K \lhd G$.

ii) $H \cap K = \{e\}$.

iii) $G = HK$.

On dit alors que G est produit direct interne *ou produit direct de ses sous-groupes H et K.*

Si G est produit direct interne de H et K, on dit que G se décompose dans le produit direct de H et K, et que H et K sont *les facteurs* de cette décomposition.

Soient X une partie d'un groupe G, on utilisera la notation $\langle X \rangle$ pour désigner le sous-groupe de G engendré par X, c.-à-d. le plus petit sous-groupe de G qui contienne X. Si $X = \{x\}$, on utilise aussi la notation $\langle x \rangle$, qui désigne le sous-groupe engendré par x.

Exemple 4.17. *Ainsi $\mathbb{Z}_6$ est produit direct interne de ses sous-groupes $\langle \bar{3} \rangle$ et $\langle \bar{2} \rangle$.*

La notion de produit directe interne se généralise à plus de deux facteurs.

Définition 4.18. *Soient G un groupe et $H_1 \ldots, H_n$ des sous-groupes de G tels que*

i) $H_i \lhd G$, *pour chaque i.*

ii) $H_i \cap \langle H_1 \cup \ldots \cup \widehat{H_i} \cup \ldots \cup H_n \rangle = \{e\}$.

iii) $G = H_1H_2 \dots H_n$.

où, par exemple, $H_1 \cup \widehat{H_2} \cup \dots \cup H_n = H_1 \cup H_3 \cup H_4 \cup \dots \cup H_n$. *On dit alors que* G *est* produit direct interne *ou produit direct des sous-groupes* H_i.

Exemple 4.19. *Considérons* $\mathbb{Z}_{30}$. *Il est produit direct interne de ses sous-groupes* $\langle\overline{15}\rangle$, $\langle\overline{10}\rangle$ *et* $\langle\bar{6}\rangle$.

Proposition 4.20. *Supposons* G *un groupe et* $H_1, \dots, H_n$ *des sous-groupes de* G *tels que* G *soit produit direct interne des* H_i. *Alors* $G \simeq H_1 \times \dots \times H_n$.

Démonstration. Considérons l'application

$$\varphi : H_1 \times \dots H_n \to G$$

$$(x_1, x_2, \dots, x_n) \mapsto x_1x_2 \dots x_n$$

La condition (iii) assure précisément que cette application est surjective. C'est aussi un homomorphisme puisqu'on a

$$\varphi((x_1, \dots, x_n) \cdot (y_1, \dots, y_n)) = \varphi(x_1y_1, x_2y_2, \dots x_ny_n) = x_1y_1x_2y_2 \dots x_ny_n$$

$$\varphi(x_1, \dots, x_n) \cdot \varphi(y_1, \dots, y_n) = (x_1x_2 \dots x_n) \cdot (y_1y_2 \dots y_n) = x_1x_2 \dots x_ny_1y_2 \dots y_n$$

mais que de façon semblable au cas de deux facteurs, des éléments de deux facteurs différents commutent entre eux, c'est-à-dire que si $h_i \in H_i, h_j \in H_j, i \neq j$, alors $h_ih_j = h_jh_i$, de sorte que de proche en proche on obtient

$$\begin{aligned} x_1y_1x_2y_2 \dots x_ny_n &= x_1x_2y_1y_2x_3y_3 \dots x_ny_n \\ &= x_1x_2x_3y_1y_2y_3x_4y_4 \dots x_ny_n \\ &\vdots \\ &= x_1x_2 \dots x_ny_1y_2 \dots y_n \end{aligned}$$

L'homomorphisme φ est aussi injectif car si $\varphi(x_1, x_2, \dots, x_n) = x_1x_2 \dots x_n = e$, alors $x_1x_2 \dots x_{n-1} = x_n^{-1} \in \langle H_1 \cup \dots H_{n-1}\rangle \cap H_n = \{e\}$, de sorte que $x_n = e$ et $x_1x_2 \dots x_{n-1} = e$. De proche en proche, de façon semblable, on obtient $x_n = e, x_{n-1} = e, \dots, x_1 = e$, d'où $(x_1, \dots, x_n) = (e, \dots, e) = e_{H_1 \times \dots \times H_n}$. □

Si G est produit direct interne des H_i, on dit que G se décompose dans le produit direct des H_i, et que les H_i sont *les facteurs* de cette décomposition.

Chapitre 5

La structure des groupes abéliens finis

Un groupe cyclique est abélien et un produit direct de groupes finis cycliques sera donc abélien. En fait, les groupes abéliens finis s'obtiennent tous de cette façon. Dans ce chapitre nous allons montrer le théorème suivant.

Théorème 5.1. *Tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques.*

On représentera chaque groupe abélien fini comme un produit direct de certains de ses sous-groupes. Puisqu'on est dans les groupes abéliens on n'aura pas à se préoccuper de la normalité des sous-groupes, qui est automatique. On pourra être plus précis dans la représentation en produit direct par une certaine *unicité*. Dans les groupes abéliens on utilise plus souvent la notation additive, et on parle alors de *somme directe* et on utilise la notation $G \oplus H$, $H_1 \oplus H_2 \oplus \ldots \oplus H_n$.

Rappelons la notation $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

5.1 Les groupes cycliques

Définition 5.2. *Un groupe G est dit cyclique si il peut être engendré par un seul élément, c'est-à-dire s'il existe au moins un $g \in G$ tel que $G = \langle g \rangle$.*

Exemple 5.3. *Le groupe additif des entiers $(\mathbb{Z}, +)$ peut être engendré par 1, mais il n'est pas fini.*

Exemple 5.4. *Le groupe additif $(\mathbb{Z}_n, +)$ est cyclique puisqu'il peut être engendré par $\bar{1}$.*

Exemple 5.5. *Le groupe multiplicatif $\{1, -1\}$ est cyclique puisqu'il est engendré par -1.*

Exemple 5.6. *Soit μ_n le groupe multiplicatif des racines complexes n^e de 1*

$$\mu_n = \{e^{2k\pi i/n} : k = 0, 1, \ldots, n-1\}$$

C'est un groupe cyclique puisqu'il peut être engendré par $e^{2\pi i/n}$.

Soit G un groupe et $a \in G$. Considérons le sous-groupe de G engendré par a, noté $\langle a \rangle$. On a

$$\langle a \rangle = \{e, a, a^{-1}, a^2, a^{-2}, \ldots\}$$

On a deux cas. Si toutes les puissances de a sont distinctes alors $\langle a \rangle$ est isomorphe à $\mathbb{Z}$ par l'isomorphisme $\mathbb{Z} \to \langle a \rangle$ défini par $k \mapsto a^k$. Si deux au moins des puissances de a sont égales, disons $a^i = a^j$,avec $i < j$,alors on a $a^{j-i} = e$ où $j - i > 0$, et $\langle a \rangle$ est isomorphe à $(\mathbb{Z}_n, +)$, où n est le plus entier positif tel que $a^n = e$, par l'isomorphisme $\mathbb{Z}_n \to \langle a \rangle$ défini par $k \mapsto a^k$. Cet entier n est appelé l'ordre de a, noté $ordre(a)$, et est alors le cardinal de $\langle a \rangle$.

Proposition 5.7. *Soient G un groupe et $a \in G$.*

1) Si $a^m = e$, alors m est un multiple de $ordre(a)$.

2) $ordre(a^{-1}) = ordre(a)$.

Démonstration. (1) Disons $ordre(a) = t$, et supposons $a^m = e$. On peut supposer que $m \geq 0$, car $a^{-m} = (a^m)^{-1}$. Faisons la division euclidienne $m = qt + r$, $q, t \in \mathbb{N}, 0 \leq r < t$. On obtient $e = a^m = a^{qt+r} = a^{qt}a^r = (a^t)^q a^r = ea^r = a^r$. Ainsi on ne peut avoir $r > 0$ car cela contredirait la minimalité de t. Donc $r = 0$ et m est un multiple de t.
(2) En effet, on a la relation $(x^{-1})^n = x^{-1} \ldots x^{-1} = (x \ldots x)^{-1} = (x^n)^{-1}$. Donc $x^n = e \iff x^{-n} = e$. □

.

5.2 Les groupes abéliens primaires

Définition 5.8. *Soient G un groupe abélien et p un nombre premier qui divise $|G|$.* La composante p-primaire *de G, notée $G(p)$, est définie par*

$$G(p) = \{x \in G : \exists n \in \mathbb{N}, ordre(x) = p^n\}$$

Par convention on pose $G(p) = \{e\}$ si p ne divise pas $|G|$.

Proposition 5.9. *Soit p un nombre premier et G un groupe abélien. Alors $G(p)$ est un sous-groupe de G.*

Démonstration. On a $e \in G(p)$ puisque $ordre(e) = 1 = p^0$. D'autre part, si $x \in G(p)$, alors $x^{-1} \in G(p)$ car $ordre(x^{-1}) = ordre(x)$. Finalement supposons $x, y \in G(p)$ et montrons que $xy \in G(p)$. En effet, disons $ordre(x) = p^{n_1}, ordre(y) = p^{n_2}$ et posons $n = n_1 + n_2$. On obtient $(xy)^{p^n} = xy \cdot xy \cdot \ldots \cdot xy = xx \ldots x \cdot yy \ldots y = x^{p^n} y^{p^n}$, car G est abélien. Donc $(xy)^{p^n} = x^{p^n} y^{p^n} = x^{p^{n_1+n_2}} y^{p^{n_1+n_2}} = (x^{p^{n_1}})^{p^{n_2}} (y^{p^{n_2}})^{p^{n_1}} = ee = e$. D'où p^n est un multiple de $ordre(xy)$, de sorte que $ordre(xy)$ doit être une puissance de p. □

Exemple 5.10. *Considérons* $G = \mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. *On a* $ordre(\bar{1}) = 6$, $ordre(\bar{2}) = 3$, $ordre(\bar{3}) = 2$, $ordre(\bar{4}) = 3$, $ordre(\bar{5}) = 6$, $|G| = 2 \cdot 3$. *On obtient* $G(2) = \{\bar{0}, \bar{3}\}$, $G(3) = \{\bar{0}, \bar{2}\}$.

Exemple 5.11. *Considérons* $G = \mathbb{Z}_{24} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{24}\}$. *On a* $|G| = 2^3 \cdot 3$. *On obtient* $G(2) = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}\}$, $G(3) = \{\bar{0}, \bar{8}, \overline{16}\}$.

Par définition même, $G(p)$ consiste de tous les éléments de G qui sont d'ordre une puissance de p.

Proposition 5.12. *Soit p un nombre premier et G un groupe abélien fini dont tous les éléments sont d'ordre une puissance de p. Alors le cardinal de G est une puissance de p.*

Démonstration. On a déjà fait le cas où $p = 3$. Le cas général est identique en remplaçant partout 3 par p. □

Notons que, réciproquement, si $|G| = p^n$ alors tous les éléments de G sont d'ordre une puissance de p.

Définition 5.13. *Soit p un nombre premier. Un groupe fini est appelé un* p-groupe *si son cardinal est une puissance de p.*

On dit aussi que les p-groupes, indépendamment du p, sont des *groupes primaires.*

Exemple 5.14. *Le groupe $\mathbb{Z}_9$ est un 3-groupe.*

Exemple 5.15. *Le groupe $\mathbb{Z}_3 \times \mathbb{Z}_3$ est un 3-groupe.*

Exemple 5.16. *Le groupe $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \ldots \times \mathbb{Z}_3$ est un 3-groupe.*

Exemple 5.17. *Le groupe $\mathbb{Z}_3 \times \mathbb{Z}_{27}$ est un 3-groupe.*

5.3 La décomposition primaire

Nous allons montrer que tout groupe abélien fini est produit direct interne de ses composantes primaires.

Théorème 5.18. *Soit G un groupe abélien fini et $|G| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ où les p_i sont premiers. Alors G est produit direct interne de ses composantes primaires $G(p_i)$, en particulier $G \simeq G(p_1) \times \ldots \times G(p_k)$.*

Illustrons d'abord le théorème par un exemple.

Exemple 5.19. *Considérons* $G = \mathbb{Z}_{30}$. *On a* $30 = 2 \cdot 3 \cdot 5$, $\mathbb{Z}_{30}(2) = \{\bar{0}, \overline{15}\}$, $\mathbb{Z}_{30}(3) = \{\bar{0}, \overline{10}, \overline{20}\}$, $\mathbb{Z}_{30}(5) = \{\bar{0}, \bar{6}, \overline{12}, \overline{18}, \overline{24}\}$. *On a déjà vu que $\mathbb{Z}_{30}$ est produit direct interne de ces sous-groupes.*

On a besoin de résultats préliminaires.

Lemme 5.20. *Soit G un groupe abélien fini, $y_1, \ldots, y_n \in G$, $ordre(y_i) = m_i$ tels que les m_i sont premiers deux à deux. Alors $ordre(y_1 \ldots y_n) = m_1 \ldots m_n$.*

Démonstration. Nous n'allons faire que le cas $n = 2$; le cas général peut se faire par récurrence. Donc disons y_1, y_2 avec $ordre(y_1) = m_1$ et $ordre(y_2) = m_2$. À voir : $ordre(y_1 y_2) = m_1 m_2$. Il suffit de voir que si $(y_1 y_2)^m = e$ alors m est un multiple de $m_1 m_2$. Notons que $\langle y_1 \rangle \cap \langle y_2 \rangle = \{e\}$; en effet posons $H = \langle y_1 \rangle \cap \langle y_2 \rangle$, alors H est un sous-groupe de $\langle y_1 \rangle$ et $\langle y_2 \rangle$, donc $|H|$ divise m_1 et m_2, d'où $|H| = 1$ car m_1 et m_2 sont premiers entre eux. Supposons $(y_1 y_2)^m = e$. On a $(y_1 y_2)^m = y_1^m y_2^m$ car G est abélien. On obtient $y_1^m = y_2^{-m} \in H$, donc $y_1^m = e$ et $y_2^{-m} = e = y_2^m$. Il s'ensuit que m est un multiple de m_1 et m_2, donc un mutliple de $m_1 m_2$, car m_2 et m_2 sont premiers entre eux. □

Lemme 5.21. *Soient G un groupe abélien et $H_1, \ldots, H_n$ des sous-groupes de G. Alors $\langle H_1 \cup \ldots \cup H_n \rangle = H_1 H_2 \ldots H_n$.*

Démonstration. On a

$$H_1 H_2 \ldots H_n = \{g \in G : \exists h_i \in H_i, g = h_1 h_2 \ldots h_n\}$$

Il est immédiat que chaque élément $h_1 h_2 \ldots h_n$, $h_i \in H_i$, appartient à tout sous-groupe de G qui contient $H_1 \cup \ldots \cup H_n$. Il suffit donc de voir que $H_1 H_2 \ldots H_n$ forme un sous-groupe de G qui contient $H_1 \cup \ldots \cup H_n$. Or si $h_i \in H_i$, alors $h_i = e \ldots e h_i e \ldots e \in H_1 H_2 \ldots H_n$. Donc on a bien $H_1 \cup \ldots \cup H_n \subseteq H_1 H_2 \ldots H_n$. Puisque $e \in H_i$, on a $e = e \ldots e \in H_1 H_2 \ldots H_n$. Par ailleurs, si $x \in H_1 H_2 \ldots H_n$, disons $x = h_1 \ldots h_n$, $h_i \in H_i$, alors $x^{-1} = h_n^{-1} \ldots h_1^{-1} = h_1^{-1} \ldots h_n^{-1}$, car G est abélien, et comme $h_i^{-1} \in H_i$ on a bien $x^{-1} \in H_1 H_2 \ldots H_n$. Finalement, si $x, y \in H_1 H_2 \ldots H_n$, disons $x = a_1 \ldots a_n$, $a_i \in H_i$, $y = b_1 \ldots b_n$, $b_i \in H_i$, alors $xy = a_1 \ldots a_n b_1 \ldots b_n = a_1 b_1 \ldots a_i b_i \ldots a_n b_n$, car G est abélien, et $a_i b_i \in H_i$, de sorte que $xy \in H_1 H_2 \ldots H_n$. □

Démonstration. (du théorème) On sait déjà que les $G(p_i)$ sont des sous-groupes normaux, et que par le lemme précédent

$$\langle G(p_1) \cup \ldots \cup \widehat{G(p_i)} \ldots \cup G(p_k) \rangle = G(p_1) G(p_2) \ldots \widehat{G(p_i)} \ldots G(p_k)$$

donc il reste à voir

1) $G(p_i) \cap G(p_1) G(p_2) \ldots \widehat{G(p_i)} \ldots G(p_k) = \{e\}$.
2) $G = G(p_1) \ldots G(p_k)$.

1) Soit $x \in G(p_i) \cap G(p_1) G(p_2) \ldots \widehat{G(p_i)} \ldots G(p_k)$, disons $ordre(x) = p_i^{t_i}, t_i \leq \alpha_i$, et

$$x = x_1 \ldots \widehat{x_i} \ldots x_k$$

$x_j \in G(p_j)$, $ordre(x_j) = p^{t_j}, t_j \leq \alpha_j$. Par un des lemmes ci-dessus on a

$$ordre(x_1 \ldots \widehat{x_i} \ldots x_k) = p_1^{t_1} \ldots \widehat{p_i^{t_i}} \ldots p_k^{t_k}$$

La seule possibilité est $t_i = 0$ et $n_j = 0$, pour tout j, d'où $x = e$.
2) Soit $x \in G$. On a $ordre(x) \mid p_1^{\alpha_1} \dots p_k^{\alpha_k}$, disons

$$ordre(x) = n = p_1^{t_1} \dots p_k^{t_k} \quad , \quad t_i \leq \alpha_i$$

Posons

$$n_i = \frac{n}{p_i^{t_i}} = p_1^{t_1} \dots \widehat{p_i^{t_i}} \dots p_k^{t_k}$$

Alors $p.g.c.d.(n_1, \dots, n_k) = 1$ et il existe des $\lambda_i \in \mathbb{Z}$ tels que

$$\lambda_1 n_1 + \dots + \lambda_k n_k = 1$$

Ainsi on a

$$x = x^{\lambda_1 n_1 + \dots + \lambda_k n_k} = x^{\lambda_1 n_1} x^{\lambda_2 n_2} \dots x^{\lambda_k n_k}$$

et comme

$$(x^{\lambda_i n_i})^{p_i^{t_i}} = x^{\lambda_i n_i t_i} = x^{\lambda_i n} = e$$

on a $x^{\lambda_i n_i} \in G(p_i)$. □

Corollaire 5.22. *Soit G comme ci-dessus, $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Alors $|G(p_i)| = p_i^{\alpha_i}$.*

Démonstration. On a $|G(p_i)| = p_i^{\lambda_i}$, où $\lambda_i \leq \alpha_i$, mais comme $|G| = p_1^{\lambda_1} \dots p_k^{\lambda_k}$, la seule possibilité est $\lambda_i = \alpha_i$, pour tout i. □

Le théorème précédent nous ramène à étudier les groupes abéliens finis primaires. Il suffira de montrer que tout groupe abélien fini primaire est produit direct de groupes cycliques.

5.4 La décomposition des groupes primaires

Théorème 5.23. *Tout p-groupe abélien fini est produit direct interne de groupes cycliques.*

Démonstration. Soit p premier. On procède par récurrence sur l'ordre des p-groupes abéliens finis. Soit G un p-groupe abélien fini, disons $|G| = p^n$.
Cas de base. C'est le cas où $|G| = p$; mais alors $G \simeq \mathbb{Z}_p$ et on a fini.
Récurrence. On a $|G| = p^n$, $n \geq 2$. Notons que $G = G(p)$. Soit $a \in G$ dont l'ordre est maximum, disons $ordre(a) = p^m$, $m \geq 1$. Notons que pour tout $g \in G$, $ordre(g) = p^\alpha$ où $\alpha \leq m$, de sorte que $g^{p^m} = e$. Si $ordre(a) = p^n$, alors $G = \langle a \rangle$ et on a fini. Sinon, on a $\langle a \rangle \subset G$. Considérons $G/\langle a \rangle$. C'est un groupe abélien fini et

$$|G/\langle a \rangle| = \frac{|G|}{|\langle a \rangle|} = p^{n-m}$$

Donc $G/\langle a\rangle$ est un p-groupe abélien fini d'ordre plus petit que G. Posons $\overline{G} = G/\langle a\rangle$ et $H = \langle a\rangle$. Par récurrence, $\overline{G}$ est produit direct interne de sous-groupes cycliques, disons les $\overline{G_i} \leq \overline{G}$, $\overline{G_i} = \langle \beta_i\rangle$, $\beta_i = b_i H$, $i = 1, \ldots, r$, et $|\overline{G_i}| = ordre(\beta_i) = p^{m_i}$. Notons que pour $b \in G$, si on pose $\beta = bH$, on a

$$\beta = \beta_1^{k_1} \ldots \beta_r^{k_r} \quad , \quad \text{où } k_i \in \mathbb{N}$$

$$bH = b_1^{k_1} \ldots b_r^{k_r} H$$

En particulier,

$$b = b_1^{k_1} \ldots b_r^{k_r} a^k \quad , \quad \text{où } k \in \mathbb{N}$$

Ainsi si on pose $K_i = \langle b_i\rangle$, on a

$$G = K_1 K_2 \ldots K_r H$$

mais rien n'assure qu'on ait un produit direct interne. Cependant on peut remarquer que n'importe quels b_i tels que $\beta_i = b_i H$ donnent la même relation. Puisque $b_i a^{n_i} H = b_i H$, nous allons trouver des ajustements $a^{n_1}, \ldots, a^{n_r}$ de façon à obtenir un produit direct interne. Notons que $\beta_i^{p^{m_i}} = e_{G/H}$, ou autrement dit $b_i^{p^{m_i}} H = H$, de sorte que $b_i^{p^{m_i}} \in H$, disons $b_i^{p^{m_i}} = a^{s_i}$, et donc $b_i^{p^{m_i}} \in K_i \cap H$, ce qui empêche possiblement d'avoir un produit direct interne. Considérons

$$(b_i^{p^{m_i}})^{p^{m-m_i}} = (a^{s_i})^{p^{m-m_i}}$$

$$b_i^{p^m} = (a^{p^{m-m_i}})^{s_i}$$

$$e = (a^{p^{m-m_i}})^{s_i}$$

Mais

$$ordre(a^{p^{m-m_i}}) = p^{m_i}$$

car $ordre(a) = p^m$, donc s_i est un multiple de p^{m_i}, disons

$$s_i = t_i p^{m_i}$$

Alors

$$(b_i a^{-t_i})^{p^{m_i}} = b_i^{p^{m_i}} a^{-t_i p^{m_i}} = a^{s_i} a^{-s_i} = e$$

Posons

$$b_i' = b_i a^{-t_i}$$

$$H_i = \langle b_i'\rangle$$

Alors

$$b_i' H = \beta_i$$

d'où, comme auparavant,

$$G = H_1 \ldots H_r H$$

Je dis que G est produit direct interne de $H_1, \ldots, H_r, H$. Posons $H_{r+1} = H$, il s'agit de vérifier que

$$H_i \cap H_1 H_2 \ldots \widehat{H_i} \ldots H_{r+1} = \{e\} \quad , \quad i = 1, \ldots, r+1$$

Soit $x \in H_i \cap H_1 H_2 \ldots \widehat{H_i} \ldots H_{r+1}$. À voir : $x = e$. Disons $x = x_1 \ldots \widehat{x_i} \ldots x_{r+1}$, $x \in H_i$, $x_j \in H_j, j \neq i$. Posons

$$\gamma = xH$$

$$\gamma_j = x_j H$$

On a

$$\gamma = \gamma_1 \ldots \widehat{\gamma_j} \ldots \gamma_{r+1}$$

dans $\overline{G}$, où $\gamma \in \overline{G_i}$, $\gamma_j \in \overline{G_j}, i \neq j$, $\gamma_{r+1} = e_{\overline{G}}$. Donc on a

$$\gamma = \gamma_1 \ldots \widehat{\gamma_j} \ldots \gamma_r$$

D'où $\gamma = e_{\overline{G}}$, $\gamma_j = e_{\overline{G}}$, car on a un produit direct interne de $\overline{G}$. Autrement dit

$$x \in H \quad , \quad x_j \in H$$

Il suffit donc de voir que $H \cap H_i = \{e\}$, pour tout $i = 1, \ldots, r$. Or, notons que $\beta_i^{ordre(b_i')} = b_i' H^{ordre(b_i')} = b_i'^{ordre(b_i')} H = eH = e_{\overline{G}}$, de sorte que $ordre(b_i')$ est un multiple de $ordre(\beta_i) = p^{m_i}$. Mais $(b_i')^{p^{m_i}} = e$, donc p^{m_i} est un multiple de $ordre(b_i')$. D'où l'égalité $ordre(b_i') = p^{m_i} = ordre(\beta_i)$ [1]. Considérons $x \in H \cap H_i$, disons $x = b_i'^k$, $k < p^{m_i}$.On a

$$xH = e_{\overline{G}}$$

$$xH = b_i'^k H = (b_i' H)^k = \beta_i^k$$

La seule possibilité est $k = 0$, car $p^{m_i} = ordre(\beta_i)$. D'où $x = e$, tel que voulu. □

5.5 Le théorème principal

Théorème 5.24. *Tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques. Plus précisément, il est produit direct interne de sous-groupes cycliques.*

Démonstration. Découle des deux théorèmes précédents. □

1. C'était le but de l'ajustement.

Notons qu'on n'a pas une unicité directe : par exemple le groupe cyclique $\mathbb{Z}_6$ est aussi isomorphe au produit direct $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Par contre, on peut noter que la décomposition d'un groupe abélien en produit direct interne de ses composantes primaires est unique puisque les composantes primaires sont complètement déterminées.

D'autre part on a le résulat suivant.

Théorème 5.25. *La décomposition d'un p-groupe abélien fini en produit direct de groupes cycliques est unique au sens suivant. Soit G un p-groupe abélien fini et G_i, H_i des p-groupes cycliques tels que*

$$G \simeq G_1 \times \ldots \times G_r$$

et

$$G \simeq H_1 \times \ldots \times H_s$$

Alors $r = s$ et, à un réarrangement près, $|G_i| = |H_i|$ (donc $G_i \simeq H_i$).

Démonstration. Voir Kostrikin, p. 312, théorème 12. □

Ce résultat et la remarque précédente sur les composantes primaires permettent d'introduire une certaine unicité dans le théorème principal.

Théorème 5.26. *Tout groupe abélien fini possède une décomposition en produit direct interne de sous-groupes cycliques primaires, et cette décomposition est unique au sens où deux telles décomposition comportent le même nombre de facteurs de chaque ordre.*

Exemple 5.27. *Soit $G = \mathbb{Z}_n$, et $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. On note que chaque composante primaire $\mathbb{Z}_n(p_i)$ est cyclique. Ainsi, la décomposition primaire donne la décomposition dont il est question dans le théorème précédent :*

$$\mathbb{Z}_n = \mathbb{Z}_n(p_1) \times \ldots \times \mathbb{Z}_n(p_r)$$

Une conséquence de l'unicité dans le théorème précédent est que tout p-groupe abélien fini qui est cyclique est *indécomposable*, c'est-à-dire qu'il ne peut pas être représenté comme produit direct de groupes plus petits.

Une autre conséquence est qu'on peut faire la liste exacte à isomorphisme près de tous les groupes abéliens finis d'un cardinal donné. En effet, il suffit d'énumérer toutes les combinaisons possibles par produit direct des groupes cycliques primaires qui permettent d'obtenir la cardinalité voulue.

Exemple 5.28. *On peut faire la liste à isomorphisme près de tous les groupes abéliens finis d'ordre 8. En effet, dans la décomposition on ne peut avoir que des 2-groupes et les seules possibilités sont*

$$\mathbb{Z}_8$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Exemple 5.29. *On peut faire la liste à isomorphisme près de tous les groupes abéliens finis d'ordre* 180. *En effet,* $180 = 2^2 \cdot 3^2 \cdot 5$. *Donc dans la décomposition on ne peut avoir que des* 2*-groupes de cardinal* 2 *ou* 4*, des* 3*-groupes de cardinal* 3 *ou* 9*, et des* 5*-groupes de cardinal* 5. *On peut lister toutes les possibilités :*

$$\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$

$$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

Plus ou moins étonnamment, il n'y en a que 4.

Sauriez-vous dire combien il y a, à isomorphisme près, de groupes abéliens finis d'un cardinal donné n ?

Chapitre 6

Les actions de groupes

Dans ce chapitre nous allons étudier les actions de groupes. Les théorèmes de Sylow [1] permettront de prédire l'existence de certains sous-groupes dans un groupe fini, seulement à partir du cardinal du groupe.

6.1 Les groupes qui opèrent sur les ensembles

Définition 6.1. *Soient G un groupe et E un ensemble non vide. On dit que G* opère à gauche sur *E si on a une fonction*

$$f : G \times E \to E$$

notée habituellement $f(g, x) = g.x$ ou encore gx, et telle que pour tous $x \in E$, et $g_1, g_2 \in G$ on ait

1) $e.x = x$. (où e est le neutre de G)

2) $(g_1 g_2).x = g_1.(g_2.x)$.

On appelle aussi f une action de G sur E, *et on dit que G* agit sur E par f.

Remarque 28. *Il peut y avoir plusieurs actions possibles d'un groupe sur le même ensemble.*

Définition 6.2. *Soit G un groupe agissant sur un ensemble E. Soit $x \in E$.*

*1) L'*orbite *de x, notée $Orb(x)$, est définie par,*

$$Orb(x) = \{y \in E : \text{ il existe au moins un } g \in G \text{ tel que } y = g.x\}$$

2) Le stabilisateur *de x, noté $Stab(x)$, est défini par*

$$Stab(x) = \{g \in G : g.x = x\}$$

1. Ludwig Sylow, 1832-1918.

L'orbite de x consiste de tous les points de E de la forme $g.x$ quand g parcourt G. C'est l'ensemble de tous les points obtenus de x à partir de l'action de G. Il y a deux cas extrêmes. Le premier est le cas où il y a une seule orbite, on dit alors que l'action est *transitive*. Le deuxième cas est celui où chaque orbite ne contient qu'un seul élément, on dit alors que c'est l'action triviale.

Théorème 6.3. *Soit G un groupe agissant sur un ensemble E, et $x \in E$.*

1) $Stab(x)$ est un sous-groupe de G.

2) La relation

$$\text{« l'élément } x \text{ est dans l'orbite de l'élément } y \text{ »}$$

est une relation d'équivalence sur E.

3) L'ensemble E est la réunion disjointes des orbites.

Exemple 6.4. *Soient $G = (\mathbb{R}, +)$, $E = \mathbb{C}$ et l'action*

$$\mathbb{R} \times \mathbb{C} \to \mathbb{C}$$

$$(r, z) \mapsto r + z$$

On a pour $z \in \mathbb{C}$ que $Orb(z)$ correspond dans le plan complexe à la droite horizontale qui passe par z, et que $Stab(z) = \{0\}$. Aussi, $\mathbb{C}$ vu comme réunion des orbites correspond à voir le plan complexe comme réunion de toutes les droites horizontales.

Exemple 6.5. *Soient $G = (\mathbb{R}^*, \cdot)$, $E = \mathbb{C}$ et l'action*

$$\mathbb{R}^* \times \mathbb{C} \to \mathbb{C}$$

$$(r, z) \mapsto rz$$

On a pour $z \in \mathbb{C}$, $z \neq 0$, que $Orb(z)$ correspond dans le plan complexe à la droite de direction z mais à laquelle on enlève l'origine, et que $Stab(z) = \{1\}$. D'autre part $Orb(0) = \{0\}$ et $Stab(0) = \mathbb{R}^*$. Aussi, $\mathbb{C}$ vu comme réunion des orbites correspond à voir le plan complexe comme réunion de l'origine avec toutes les droites qui passent par l'origine, mais auxquelles on l'a enlevé.

Proposition 6.6. *Soit G qui opère sur E. Pour $g \in G$, posons*

$$\gamma_g : E \to E$$

$$\gamma_g(x) = g.x$$

Alors γ_g est une bijection de E sur lui-même.

Démonstration. Montrons que γ_g est surjectif et injectif. Surjectif : soit $x \in E$, on a $x = e.x = (gg^{-1}).x = g.(g^{-1}.x) = \gamma_g(g^{-1}.x)$; donc chaque $x \in E$ possède bien au moins un antécédent par γ_g. Injectif : supposons $\gamma_g(x) = \gamma_g(y)$, alors on a

$$\begin{aligned} g.x &= g.y \\ g^{-1}.(g.x) &= g^{-1}.(g.y) \\ (g^{-1}g).x &= (g^{-1}g).y \\ e.x &= e.y \\ x &= y \end{aligned}$$

Donc chaque $z \in E$ possède bien au plus un antécédent par γ_g. □

Remarque 29. *Cette proposition donne une application $\gamma : G \to S_E$, définie par $\gamma(g) = \gamma_g$. On peut vérifier que γ est un homomorphisme. Et en fait, réciproquement, tout homomorphisme $G \to S_E$ donne une action de G sur E (exercice), voir l'exercice* **??**.

Exemple 6.7. *Soit $E = \mathbb{R}^2$ et G le groupe des matrices de rotation du plan et l'action naturelle*

$$G \times \mathbb{R}^2 \to \mathbb{R}^2$$

$$M_\theta.X = M_\theta X$$

où on écrit les éléments de $\mathbb{R}^2$ en matrices colonnes, et M_θ est la matrice de rotation d'angle θ, $0 \leq \theta \leq 2\pi$:

$$M_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

On a $e = M_0$, donc $e.X = X$. D'autre part le produit matriciel assure que $(M_{\theta_1}M_{\theta_2}).X = (M_{\theta_1}M_{\theta_2})X = M_{\theta_1}(M_{\theta_2}X) = M_{\theta_1}.(M_{\theta_2}.X)$. Pour $X \in \mathbb{R}^2$, $Orb(X)$ correspond au cercle centré à l'origine qui passe par X, et $Stab(X) = \{e\}$.

Exemple 6.8. *Soit $E = S^2$, la surface de la sphère de rayon 1 centrée à l'origine, et $G = (\{1, -1\}, \cdot)$ et l'action*

$$\{1, -1\} \times S^2 \to S^2$$

$$1.P = P$$

$$-1.P = -P$$

où $-P$ désigne le point antipode de P, si disons $P = (x, y, z)$ alors $-P = (-x, -y, -z)$. On vérifie directement les relations requises :

$$(1 \cdot -1).P = -P$$

$$1.(-1.P) = -P$$

$$(-1 \cdot -1).P = 1.P = P$$
$$-1.(-1.P) = -(-P) = P$$

On a $Orb(P) = \{P, -P\}$ *et* $Stab(P) = \{1\}$.

Exemple 6.9. *Soit E un ensemble non vide et $G = S_E$, le groupe des permutations de E c'est-à-dire le groupe des bijections de E sur lui-même dont l'opération est la composition des fonctions et l'élément neutre est la fonction identité. On a l'action naturelle*

$$S_E \times E \to E$$
$$g.x = g(x)$$

Pour $x \in E$, on a $Orb(x) = E$. Il n'y a pas grand chose de particulier qu'on puisse dire de $Stab(x)$ à part le fait qu'il s'identifie avec $S_{E\setminus\{x\}}$.

Exemple 6.10. *Soit G un groupe et prenons $E = G$. On a l'action de G sur lui-même*

$$G \times G \to G$$
$$g.h = gh$$

appelé action de G sur lui-même par translation. *On a bien $e.h = eh = h$ et $(g_1g_2).h = (g_1g_2)h = g_1(g_2h) = g_1.(g_2.h)$, puisque c'est l'associativité de l'opération de G. On a $Orb(h) = G$ et $Stab(h) = \{e\}$.*

Exemple 6.11. *Soit G un groupe et prenons $E = G$. On a l'action de G sur lui-même*

$$G \times G \to G$$
$$g.h = ghg^{-1}$$

appelé action de G sur lui-même par conjugaison. *On a bien $e.h = ehe^{-1} = ehe = h$ et $(g_1g_2).h = (g_1g_2)h(g_1g_2)^{-1} = g_1g_2hg_2^{-1}g_1^{-1} = g_1(g_2.h)g^{-1} = g_1.(g_2.h)$. On appelle $Orb(h)$* la classe de conjugaison de h *et ses éléments* les conjugués de h. *On a $Stab(h) = \{g \in G : ghg^{-1} = h\} = \{g \in G : gh = hg\}$, qu'on appelle* le centralisateur de h, *aussi noté $C(h)$.*

Exemple 6.12. *Soit G un groupe et prenons $E = \mathcal{P}(G)$ c'est-à-dire l'ensemble des parties de G. On a l'action de*

$$G \times \mathcal{P}(G) \to \mathcal{P}(G)$$
$$g.X = gX = \{gx : x \in X\}$$

Si $X = H$ est un sous-groupe de G, alors $Orb(H)$ consiste en les translatés à gauche de H et $Stab(H) = \{g \in G : gH = H\} = H$. L'indice de H dans G, *noté $[G : H]$, coïncide avec le cardinal de $Orb(H)$, ou autrement dit le nombre de translatés à gauche de H.*

Exemple 6.13. *Soit G un groupe et prenons $E = \mathcal{P}(G)$. On a l'action de*

$$G \times \mathcal{P}(G) \to \mathcal{P}(G)$$

$$g.X = gXg^{-1} = \{gxg^{-1} : x \in X\}$$

Si $X = H$ est un sous-groupe de G, alors $Orb(H)$ consiste en les conjugués de H et $Stab(H) = \{g \in G : gHg^{-1} = H\}$ est appelé le normalisateur de H, *aussi noté $N(H)$. Notons que $H \triangleleft Stab(H)$ et $H \triangleleft G \iff Stab(H) = G$.*

6.2 Orbites vs stabilisateurs

Proposition 6.14. *Soit G opérant sur E et $x \in E$.*

1) *Il y a une bijection entre $Orb(x)$ et les translatés à gauche de $Stab(x)$. En particulier, si $Orb(x)$ est fini, alors $Stab(x)$ est d'indice fini et $|Orb(x)| = [G : Stab(x)]$.*
2) *Si $Orb(x) = Orb(y)$, alors $Stab(x)$ et $Stab(y)$ sont conjugués.*

Démonstration. (1) Considérons $Orb(x)$ et $\{gStab(x) : g \in G\}$. Notons que

$$\begin{aligned} g.x = g'.x &\iff g'^{-1}.(g.x) = g'^{-1}.(g'.x) \\ &\iff (g'^{-1}g).x = (g'^{-1}g').x \\ &\iff (g'^{-1}g).x = e.x \\ &\iff (g'^{-1}g).x = x \\ &\iff g'^{-1}g \in Stab(x) \\ &\iff gStab(x) = g'Stab(x) \end{aligned}$$

On peut donc définir la fonction

$$Orb(x) \to \{gStab(x) : g \in G\}$$

$$g.x \mapsto gStab(x)$$

qui donne une bijection.
(2) Supposons $y = g.x$. Alors $g^{-1}.y = (g^{-1}g).x = x$. Montrons que $Stab(y) \subseteq gStab(x)g^{-1}$ et $gStab(x)g^{-1} \subseteq Stab(y)$. Soit $h \in Stab(y)$, alors on a

$$h.(g.x) = g.x$$

$$(hg).x = g.x$$

$$g^{-1}hg.x = x$$
$$g^{-1}hg \in Stab(x)$$

et on a $h = g(g^{-1}hg)g^{-1}$. Cela montre la première inclusion. Soit $k \in Stab(x)$. On a $gkg^{-1}.y = (gk).(g^{-1}y) = gk.x = g.(k.x) = g.x = y$. Cela montre la deuxième inclusion. □

Corollaire 6.15. *Soit G opérant sur E,* où G et E sont finis. Soit la partition de E en orbites pour cette action

$$E = Orb(x_1) \cup \ldots \cup Orb(x_n)$$

Alors $|E| = \sum_{i=1}^{n} [G : Stab(x_i)]$.

Ce corollaire est à la base de beaucoup d'applications aux groupes finis. Nous allons en donner une tout de suite.

Définition 6.16. *Soit G un groupe. Rappelons que* le centre de G, *noté $Z(G)$, est défini par*

$$\begin{aligned} Z(G) &= \{h \in G : gh = hg, \text{ pour tout } g \in G\} \\ &= \{h \in G : ghg^{-1} = h, \text{ pour tout } g \in G\} \end{aligned}$$

Considérons un groupe fini G qui opère sur lui-même par conjugaison, et soit $G = Orb(h_1) \cup \ldots \cup Orb(h_r)$ la partition de G en orbites, disons ordonnées en ordre croissant de cardinal. Notons que $h \in Z(G) \iff Orb(h) = \{h\}$. Alors on obtient

$$|G| = |Z(G)| + \sum_{h_i \notin Z(G)} [G : C(h_i)]$$

Rappelons qu'un p-groupe fini est un groupe fini qui possède p^n éléments pour un certain n, où p est un nombre premier.

Théorème 6.17. *Tout p-groupe fini possède un centre non trivial.*

Démonstration. Supposons $|G| = p^n$. Si $G = C(G)$, on a fini. Sinon, considérons

$$|G| = |C(G)| + \sum_{h_i \notin C(G)} [G : C(h_i)]$$

Notons que $g \in C(G) \iff C(g) = G$ et que $g \notin C(G) \iff C(g) \subset G \iff [G : C(G)] > 1$. Puisque $G \neq C(G)$, on obtient que $C(h_i) \subset G$ pour au moins un i et alors $[G : C(h_i)] > 1$ pour tous ces i. Par ailleurs on a $p|[G : C(h_i)]$ pour chaque i tel que $C(h_i) \neq G$. Ainsi on obtient

$$p^n = |C(G)| + pt$$

où $t \neq 0$. D'où $p|C(G)$, et en particulier $C(G) \neq \{e\}$, tel que voulu. □

6.3 Les théorèmes de Sylow

QUESTION : trouver tous les sous-groupes d'un groupe fini donné.

Les notions et résultats précédents permettent d'étudier cette question. On sait déjà qu'il y a une contrainte sur l'ordre des sous-groupes d'un groupe donné. L'ordre de chacun doit être un diviseur de l'ordre du groupe. Cela diminue considérablement les possibilités. Cependant, cette contrainte n'est pas suffisante en général [2]. Un contre-exemple est fourni par le groupe alterné A_4, qui est d'ordre $12 = 2 \cdot 6$, mais qui ne possède pas de sous-groupe d'ordre 6 (voir l'exercice 7.6.3). Nous allons nous concentrer sur la question suivante.

QUESTION : si $d \mid |G|$, quand peut-on dire que G possède un sous-groupe d'ordre d ?

Dans cette direction, on a les résultats remarquables du mathématicien norvégien Sylow (1832-1918) pour $d = p^n$, une puissance d'un nombre premier.

Définition 6.18. *Soit G un groupe fini, $|G| = p^n m$, où p est premier et $p \not| m$. Un sous-groupe de G qui est d'ordre p^n est appelé* un p-sous-groupe de Sylow de G.

Théorème 6.19 (Premier théorème de Sylow)**.** *Soit G un groupe fini, $|G| = p^n m$, où p est premier et $p \not| m$. Alors G possède un p-sous-groupe de Sylow pour chaque nombre premier qui divise son ordre. Plus précisément, G possède un sous-groupe d'ordre p^s, pour chaque $0 \leq s \leq n$.*

Théorème 6.20 (Deuxième théorème de Sylow)**.** *Soit G un groupe fini. Pour chaque diviseur premier p de $|G|$, les p-sous-groupes de Sylow sont conjugués.*

Théorème 6.21 (Troisième théorème de Sylow)**.** *Soit G un groupe fini, et p un diviseur premier de $|G|$. Soit N_p le nombre de p-sous-groupe de Sylow de G. Alors $N_p = [G : N(S)]$, où S est n'importe quel p-sous-groupe de Sylow, et $N_p \equiv 1 \ mod(p)$.*

Nous n'allons démontrer que les deux premiers théorèmes de Sylow. Pour le premier, on procède par récurrence sur l'ordre du groupe $|G| = p^n m$, et on utilise le cas particulier connu d'un sous-groupe d'ordre p pour les groupes abéliens. On suppose que $|G| > 1$. Considérons l'action de G sur lui-même par conjugaison, et soit $G = Orb(x_1) \cup \ldots \cup Orb(x_r)$ la partition de G en orbites, disons ordonnées en ordre croissant de cardinalité. Considérons la relation déjà vue

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : C(x_i)]$$

Nous allons distinguer deux cas.

1er cas. $p \not| \ |Z(G)|$. Alors $p \not| \ [G : C(x_i)]$ pour un certain i. D'où $p^s | \ |C(x_i)|$, puisque $|G| = [G : C(x_i)] \cdot |C(x_i)|$, et on a aussi $|C(x_i)| < |G|$, car $x_i \notin Z(G)$. Par récurrence, $C(x_i)$ possède un sous-groupe H d'ordre p^s, qui est en même temps un sous-groupe de G d'ordre p^s.

2. Bien qu'elle le soit pour les groupes abéliens. Voir l'exercice 7.5.2 .

2e cas $p \mid |Z(G)|$. Alors $Z(G)$ possède un élément d'ordre p, disons c. Soit H_0 le sous-groupe engendré par c. C'est un groupe cyclique d'ordre p, qui est un sous-groupe normal de G car $c \in Z(G)$. Alors G/H_0 est un groupe d'ordre $\frac{p^n m}{p} = p^{n-1}m$. Par récurrence, G/H_0 possède un sous-groupe d'ordre p^{s-1}, disons K. Soit $H = \pi^*(K)$, où π est l'homomorphisme naturel $G \to G/H_0$. C'est un sous-groupe de G tel que $H_0 \subset H$ et $H/H_0 \simeq K$. D'où $|H| = |H_0| \cdot |K| = p^s$. Ainsi H est un p-sous-groupe de G de l'ordre voulu, ce qui termine la preuve.

Pour le deuxième théorème de Sylow, fixons un p-sous-groupe de Sylow S et considérons un autre p-sous-groupe de Sylow S_1. Soit Γ_S l'ensemble des translatés de S. Le groupe G agit par translation sur Γ_S et de même S_1 agit aussi par translation sur Γ_S. On obtient donc

$$|\Gamma_S| = \sum_i [S_1 : Stab_{S_1}(T_i)]$$

où $T_1, T_2, \ldots$ désignent les translatés de S. Or, on note que tous les $[S_1 : Stab_{S_1}(T_i)]$ divise p^n alors que p ne divise pas $|\Gamma_S|$. Il doit donc y avoir au moins un $[S_1 : Stab_{S_1}(T_i)]$ qui soit égal à 1, disons pour $T_i = gS$. On a donc $S_1 \cdot gS = gS$. En particulier, $S_1 \subseteq gSg^{-1}$, et on doit avoir égalité puisque les deux ensembles ont le même nombre d'éléments. Ainsi S_1 et S sont conjugués, tel que voulu.

REMARQUES SUR LES THÉORÈMES DE SYLOW.

1) En particulier un groupe fini G possède au moins un élément d'ordre p, pour chaque nombre premier qui divise l'ordre de G.
2) Si p est un facteur premier de $|G|$, alors G possède au moins un p-sous-groupe de Sylow , $N_p \mid |G|$ et $N_p \equiv 1 \ mod(p)$.
3) Les p-sous-groupes de Sylow forment une orbite pour l'action de G sur $\mathcal{P}(G)$ par conjugaison et N_p est le cardinal de cette orbite qui est égal à $[G : N(S)]$.
4) Un groupe fini G possède un seul p-sous-groupe de Sylow si et seulement si il possède un p-sous-groupe de Sylow qui soit un sous-groupe normal.
5) Si $N_{p,s}$ désigne le nombre de sous-groupe d'ordre p^s, on peut montrer que $N_{p,s} \equiv 1 \bmod (p)$.

Exemple 6.22. *Supposons G un groupe d'ordre 30. On a $30 = 2 \cdot 3 \cdot 5$. Il y a au moins un 2-sous-groupe de Sylow, au moins un 3-sous-groupe de Sylow et au moins un 5-sous-groupe de Sylow. Les possibilités pour N_2 sont $1, 3, 5, 15$. Les possibilités pour N_3 sont $1, 10$. Les possibilités pour N_5 sont $1, 6$.*

Exemple 6.23. *Tout groupe d'ordre 20 possède au moins un sous-groupe normal propre. En effet, on a $20 = 2^2 \cdot 5$ et $N_5 | 20$, $N_5 \equiv 1 \ mod(5)$. Les possibilités pour N_5 sont $1, 6, 11, 16$. On voit que nécessairement $N_5 = 1$. Il n'y a donc qu'un seul 5-sous-groupe de Sylow et il doit être normal.*

Exemple 6.24. *Tout groupe d'ordre 2^n possède au moins un sous-groupe normal propre. En effet, il possède au moins un sous-groupe d'ordre 2^{n-1} qui est alors d'indice 2 et donc normal.*

Exemple 6.25. *Tout groupe d'ordre* 30 *possède au moins un sous-groupe normal propre. En effet, il suffit de voir qu'au moins un parmi* N_2, N_3, N_5 *vaut* 1. *On a déjà vu que* $N_2 = 1$ *ou* 3 *ou* 5 *ou* 15, $N_3 = 1$ *ou* 10, $N_5 = 1$ *ou* 6. *Montrons que* $N_3 = 1$ *ou* $N_5 = 1$. *Sinon, on aurait* $N_3 = 10$ *et* $N_5 = 6$. *Disons* $K_1, \ldots, K_{10}$ *les* 3*-sous-groupes de Sylow, d'ordre* 3, *et* $H_1, \ldots, H_6$ *les* 5*-sous-groupes de Sylow, d'ordre* 5. *Puisqu'une intersection* $H_i \cap H_j$ *est un sous-groupe de* H_i *et* H_j *et que son ordre est un facteur de* 5, *on a* $H_i \cap H_j = \{e\}$ *si* $i \neq j$. *De façon semblable* $K_i \cap K_j = \{e\}$ *si* $i \neq j$. *Les* H_i *fourniraient donc au moins* 24 *éléments différents de* e *et les* K_i *au moins* 20, *ce qui donneraient au moins* 44 *éléments différents dans* G, *ce qui est absurde. Donc on doit avoir* $N_3 = 1$ *ou* $N_5 = 1$, *tel que voulu.*

Proposition 6.26. *Soit* G *un groupe fini et* H, K *des sous-groupes de* G. *Alors on a la relation*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Démonstration. Déjà vu dans un exercice.

Exemple 6.27. *Tout groupe d'ordre* 48 *possède au moins un sous-groupe normal propre. En effet, on a* $48 = 2^4 \cdot 3$. *Considérons* N_2. *D'après les théorèmes de Sylow les possibilités sont* $N_2 = 1$ *ou* $N_2 = 3$. *Si* $N_2 = 1$, *alors il y a un seul* 2*-sous-groupe de Sylow et il est normal, on a fini. Si* $N_2 = 3$, *soient* H *et* K *deux* 2*-sous-groupes de Sylow distincts, ici d'ordre* 16. *Considérons* $|H \cap K|$. *Les possibilités sont* $|H \cap K| = 1, 2, 4, 8$. *Si* $|H \cap K| < 8$, *alors d'après la proposition précédente* $|HK| > 64$, *ce qui ne peut être le cas. Donc on doit avoir* $|H \cap K| = 8$. *Alors* $H \cap K$ *est un sous-groupe d'indice* 2 *à la fois dans* H *et dans* K, *donc normal dans* H *et dans* K. *Mais alors* H *et* K *sont tous deux inclus dans le normalisateur de* $H \cap K$ *dans* G, *et on a sûrement* $|N(H \cap K)| \geq |HK| = 32$. *Puisque* $|N(H \cap K)|$ *doit aussi être un facteur de* 48 *on doit avoir* $|N(H \cap K)| = 48$. *Donc* $N(H \cap K) = G$, *autrement dit* $H \cap K$ *est normal dans* G, *et on a trouvé un sous-groupe normal de* G.

6.4 Le groupe des isométries du cube

On considère un cube $\mathcal{C}$ comme une partie de $\mathbb{R}^3$. On considère l'action naturelle du groupe des isométries de $\mathbb{R}^3$, $\mathcal{ISO}_{\mathbb{R}^3}$, sur $\mathbb{R}^3$. On obtient aussi une action sur l'ensemble $P(\mathbb{R}^3)$ des parties de $\mathbb{R}^3$

$$\mathcal{ISO}_{\mathbb{R}^3} \times P(\mathbb{R}^3) \to P(\mathbb{R}^3)$$

On considère les isométries qui conservent le cube, c'est-à-dire le stabilisateur de $\mathcal{C}$ pour cette action, disons $G = Stab_{\mathcal{ISO}_{\mathbb{R}^3}}(\mathcal{C})$. Nous allons *déterminer ce groupe de la façon la plus précise posssible ; au moins à isomorphisme près.*

1) *notons que comme les distances sont conservées le groupe* G *va permuter entre eux les sommets. En effet, les extrémités des diagonales sont les points les plus éloignés l'un de l'autre sur le cube et comme la distance est conservée ils doivent être envoyés sur les extrémités d'une diagonale, donc sur deux autres sommets, et cela va déterminer complètement l'image des autres points.*

2) ceci permet de voir G comme un groupe de permutation des sommets à travers l'homomorphisme de restriction suivant, qui est injectif

$$\rho : G \to S_8$$

$$\rho(g) = g \mid_{\{sommets\}}$$

3) on a un premier élément de G en la rotation de 90 degrés autour d'un axe vertical qui passe par le centre de la face 1234 et le centre du cube. Notons-la α. En termes de permutation on a

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}$$

α est un élément d'ordre 4.

4) on a aussi la rotation de 90 degrés autour d'un axe horizontal qui passe par le centre de la face 1265 et le centre du cube. Notons-la β. En termes de permutation on a

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 7 & 3 & 1 & 5 & 8 & 4 \end{pmatrix}$$

β est un élément d'ordre 4.

5) considérons l'orbite du sommet 1 ; on a $\alpha(1) = 2, \alpha^2(1) = 3, \alpha^3(1) = 4, \beta(1) = 2, \beta^2(1) = 6, \beta^3(1) = 5, \alpha\beta^2(1) = 7, \alpha^2\beta^2(1) = 8$. Ainsi $Orb(1) = \{1, 2, 3, 4, 5, 6, 7, 8\}$ et il y a une seule orbite pour l'action de G.

6) puisque $|Orb(1)| = [G : Stab(1)] = \frac{|G|}{|Stab(1)|}$, il suffit de calculer $|Stab(1)|$ pour connaître l'ordre de G.

7) soit γ la rotation de 120 degrés autour de la diagonale 17. C'est un élément d'ordre 3. On a $\gamma(1) = 1, \gamma^2(1) = 1$, donc $e, \gamma, \gamma^2 \in Stab(1)$. Soit δ la symétrie par rapport au plan 1357. C'est un élément d'ordre 2. On a $\delta(1) = 1$, donc $\delta \in Stab(1)$. En combinant γ et δ on a aussi $\gamma\delta$ et $\delta\gamma$ qui peuvent donner de nouveaux eléments de $Stab(1)$. On peut le vérifier en les exprimant tous sous forme de permutation

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 8 & 5 & 2 & 3 & 7 & 6 \end{pmatrix}$$

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 2 & 5 & 8 & 7 & 6 \end{pmatrix}$$

$$\gamma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 6 & 2 & 4 & 8 & 7 & 3 \end{pmatrix}$$

$$\delta\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 6 & 5 & 4 & 3 & 7 & 8 \end{pmatrix}$$

$$\gamma\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 8 & 4 & 2 & 6 & 7 & 3 \end{pmatrix}$$

Ainsi on a $|Stab(1)| \geq 6$, de sorte que $|G| \geq 48$.

8) d'autre part, on a déjà observé que les éléments de G échangent entre elles les diagonales du cube. On peut donc considérer l'appplication de restriction de G dans le groupe de permutation de l'ensemble Γ des quatre diagonales. C'est un homomorphisme

$$r : G \to S_\Gamma$$

$$g \mapsto g\,|_{\{diagonales\}}$$

On vérifie directement que c'est un homomorphisme. Soit σ l'application *antipode* par rapport au centre du cube. C'est un élément de G, mais qui laisse fixe globalement chaque diagonale de sorte que sa restriction à l'ensemble des quatre diagonales est l'application identité. On a donc $\sigma \in ker(r)$. Mais aussi, si $g \in ker(r), g \neq e$, disons $g(2) = 8$, alors parce que la distance est préservée on doit aussi avoir $g(1) = 7$, d'où $g(4) = 6$ et $g(5) = 3$; donc $g = \sigma$. On a donc $ker(r) = \{e, \sigma\}$.

9) par le théorème des homomorphismes, on obtient

$$|G/ker(r)| \leq |S_\Gamma|$$

$$\frac{|G|}{|ker(r)|} \leq |S_\Gamma|$$

$$\frac{|G|}{2} \leq 24$$

$$|G| \leq 48$$

D'où $|G| = 48$.

10) peut-on obtenir de l'information plus fine sur la structure de G ? Par commodité, considérons le cube centré à l'origine. Les rotations de l'espace qui fixent l'origine forme un groupe. Désignons-le par $RO_{\mathbb{R}^3}$ (c'est un sous-groupe de $GL_3(\mathbb{R})$). Soit

$$H = G \cap RO_{\mathbb{R}^3}$$

Le groupe H est un sous-groupe de G et $\sigma \notin H$, à cause de *l'orientation* qui est préservée par toute rotation. On peut donc conclure que le noyau de l'homomorphisme de restriction

$$r\,|_H \colon H \to S_\Gamma$$

est $\{e\}$ et que c'est donc un homomorphisme injectif, de sorte que $|H| \mid 24$. Mais notons que $e, \alpha, \alpha^2, \alpha^3, \beta, \beta^2, \beta^3, \alpha\beta, \alpha\beta^2, \alpha^2\beta, \alpha^3\beta, \alpha^2\beta^2, \alpha^3\beta^2 \in H$ sont tous distincts, ce qui force $|H| > 12$ et $|H| = 24$. Ainsi H est d'indice 2 dans G, donc c'est un sous-groupe normal. Par ailleurs, soit $K = \{e, \sigma\} = ker(r)$. C'est aussi un sous-groupe normal et $H \cap K = \{e\}$. De plus on vérifie que $G = HK$. Ainsi G est produit direct interne de H et K.

Chapitre 7

Exercices

Certains exercices sont cotés A,B ou C, selon le degré de difficulté croissant ($A \nearrow B \nearrow C$) et l'ordre de priorité décroissant ($1 \searrow 2 \searrow 3$)

7.1 Structure de groupes

7.1.1

Soit la loi de composition interne $\star : (a, b) \mapsto ab + a + b$ sur $\mathbb{R}$. Est-ce que $\star$ est associative ? commutative ?

7.1.2

Soit la loi de composition interne $\star : (A, B) \mapsto AB + I$ sur $\mathcal{M}_n(\mathbb{R})$ l'ensemble des matrices carrées $n \times n$. Est-ce que $\star$ est associative ? commutative ?

7.1.3

(Différence symétrique) Soit E un ensemble. Soit la loi de composition interne

$$\Delta : (A, B) \mapsto (A \cup B) \setminus (A \cap B)$$

sur $\mathcal{P}(E)$. Montrer que $(\mathcal{P}(E), \Delta)$ est associative. Est-elle commutative ?

7.1.4

Soit $n \in \mathbb{N}^*$.

1. Montrer que dans $\mathbb{Z}/n\mathbb{Z}$, $+$ est associative et commutative.
2. Montrer que dans $\mathbb{Z}/n\mathbb{Z}$, $\cdot$ est associative et commutative.

3. Montrer que $\cdot$ est une loi de composition interne associative et commutative dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Qu'en est-il de $+$?
4. Soit la loi de composition interne $\star : (a, b) \mapsto ab + a + b$ dans $\mathbb{Z}/n\mathbb{Z}$. Est-ce que $\star$ est associative, commutative ?

7.1.5

Soit E un ensemble muni d'une multiplication et d'une addition. On considère dans E la loi de composition interne $\star : (a, b) \mapsto ab + a + b$.

1. Posons $E = \mathbb{R}$. Est-ce que $(\mathbb{R}, \star)$ possède un élément neutre ? (justifier). Lesquels des sous-ensembles $A \subseteq \mathbb{R}$ suivants sont stables pour $\star$:
   (a) $A = \mathbb{N}$; (b) $A = \mathbb{Q}^-$; (c) $A = \mathbb{Q}^{+*}$ (d) $A = \mathbb{R}$; (e) $A = n\mathbb{Z}$.
2. Mêmes questions avec $E = \mathcal{M}_n(\mathbb{R})$ et $A = \mathrm{GL}_n(\mathbb{R})$.

7.1.6

On considère les ensembles $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{Z}^*$, $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{Q}^+$, $\mathbb{Q}^{+*}$, $\mathbb{R}^*$, $\mathbb{R}^+$, $\mathbb{R}^{+*}$, $\mathbb{Z}^-$, $\mathbb{Q}^-$ et $\mathbb{R}^-$. Parmis ces ensembles, lesquels sont des groupes ou des monoïdes pour : (a) l'addition sur $\mathbb{R}$; (b) la multiplication sur $\mathbb{R}$. Justifier et préciser l'ensemble de leurs éléments inversibles.

7.1.7

Soit G un ensemble munit d'une loi de composition interne $*$. Montrer que $(G, *)$ est un groupe si et seulement si

(i) $*$ est associative ;

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

(iii) $\forall\, x \in G,\ \exists\, y \in G$ tel que $x * y = e$. (*élément inversible à droite*).

7.1.8

Soit E un ensemble.

1. Montrer que $(\mathcal{P}(E), \cup)$ et $(\mathcal{P}(E), \cap)$ sont des monoïdes. Sont-ils des groupes ?
2. On considère dans $\mathcal{P}(E)$ la loi de composition interne

$$\Delta : (A, B) \mapsto A\Delta B = (A \cup B) \setminus (A \cap B) \quad (\textit{Différence symétrique}).$$

   Montrer que $(\mathcal{P}(E), \Delta)$ est un groupe. Quel est son élément neutre ? Quel est l'inverse de A ? Est-ce un groupe abélien ?

7.1.9

Soit $n \in \mathbb{N}^*$.

1. Montrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien de cardinal n.
2. Montrer que $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ est un monoïde commutatif. Est-ce un groupe ? (Justifier.)
3. Montrer que $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe abélien de cardinal $\varphi(n)$.
4. Soit la loi de composition interne $\star : (a, b) \mapsto ab + a + b$ dans $\mathbb{Z}/n\mathbb{Z}$. Est-ce que $\star$ possède un élément neutre ? (Justifier.) Est-ce que $(\mathbb{Z}/n\mathbb{Z})^\times$ est stable pour $\star$?

7.1.10

Soit G un groupe. On suppose que pour tout $x \in G$ on a $x^2 = e$. Montrer que G est abélien.

7.1.11

Soit G un groupe et soit $a, b \in G$ tel que $a^5 = e$ et $a^3 b = ba^3$.
(1) Montrer que $a^6 b = ba^6$; (2) en déduire que $ab = ba$.

7.1.12

(*Groupe orthogonal*) Soit $n \in \mathbb{N}^*$.
(a) Montrer que l'ensemble

$$O(n) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^tMM = I_n\}$$

est un groupe. (Indication : on pourra montrer que c'est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.)
(b) Montrer que l'ensemble

$$SO(n) = \{M \in O(n) \mid \det(M) = 1\}$$

est un sous-groupe de $O(n)$; et montrer que c'est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

7.1.13

Soit G un groupe et $A \subseteq G$. Pour $g \in G$ on note $gAg^{-1} = \{gxg^{-1} \mid x \in A\}$.
(a) Montrer que $Z(A) = \{g \in G \mid gx = xg,\ \forall x \in A\}$ est un sous-groupe de G.
(b) Montrer que gAg^{-1} et A sont en bijection.
(c) Montrer que $N(A) = \{g \in G \mid gAg^{-1} = A\}$ est un sous-groupe de G.
(d) Montrer que $Z(A) \leq N(A)$.

7.1.14

(a) Quel est le centre du groupe S_n, où $n \in \mathbb{N}^*$?
(b) Montrer que G est un groupe abélien si et seulement si G est égal à son centre.

7.1.15

Montrer que les seuls sous-groupes de $(\mathbb{Z}, +)$ sont les $(n\mathbb{Z}, +)$, pour $n \in \mathbb{N}$.

7.1.16

Soit G un groupe. Montrer que

1. Soit $H \subseteq G$, alors H est un sous-groupe de G si et seulement si $e \in H$ et $\forall x, y \in H$, $xy^{-1} \in H$.
2. Si $H \leq G$ et $K \leq H$ alors $K \leq G$ (la relation $\leq$ est transitive).
3. L'intersection non vide d'une famille de sous-groupes de G est un sous-groupe de G.

7.1.17

Soit G un groupe et H, H' deux sous-groupes de G. Montrer que $H \cup H'$ est un sous-groupe de G si et seulement si $H \subseteq H'$ ou $H' \subseteq H$.

7.1.18

Soit G un groupe. On dit que x et y *sont conjugués dans* G si il existe $g \in G$ tel que $x = gyg^{-1}$. On notera $x \sim y$.

1. Montrer que $\sim$ est une relation d'équivalence sur G.
   La classe d'équivalence de $x \in G$ est appelée *classe de conjugaison de* x.
2. Soit $x \in G$, montrer que l'ensemble $G_x = \{g \in G \,|\, gxg^{-1} = x\}$ est un sous-groupe de G, appelé sous-groupe stabilisateur de $x \in G$.

7.1.19

Soit $G = \langle s \rangle$ un groupe monogène. Montrer que
(a) G est un groupe abélien.
(b) $G = \{s^n \,|\, n \in \mathbb{Z}\}$.
(c) La fonction $f : \mathbb{Z} \to \langle x \rangle$, définie par $f(k) = x^k$, est surjective et que $f(k + l) = f(k)f(l)$.
Si G est noté additivement, montrer que $G = \{ns \,|\, n \in \mathbb{Z}\}$.

7.1.20

(Un peu de topologie, difficile) On dit que $A \subseteq \mathbb{R}$ est *dense dans* $\mathbb{R}$ si :

$$\forall x \in \mathbb{R},\ \forall \varepsilon > 0, \quad A \cap]x - \varepsilon, x + \varepsilon[\neq \emptyset.$$

1. Montrer que tout sous-groupe de $(\mathbb{R}, +)$ est ou bien dense dans $\mathbb{R}$, ou bien il existe $n \in R^+$ tel que $H = n\mathbb{Z}$. (Indication : considérer une borne inférieur n de l'ensemble $H^+ = \mathbb{R}^+ \cap H$.)
2. Montrer que tout sous-groupe de $(\mathbb{R}, +)$ est soit dense dans $\mathbb{R}$, soit monogène.

7.1.21

Soit G un groupe et $g \in G$. Montrer que

1. Si $ordre(g) = \infty$ alors $ordre(g^k) = \infty$ pour tout $k \in \mathbb{N}^*$.
2. Si $ordre(g) = n$ est fini et $k \in \mathbb{N}^*$, alors $ordre(g^k) = n/\text{pgcd}(n, k)$.
3. $ordre(g^{-1}) = ordre(g)$.

7.1.22

Soit le groupe $G = \mathbb{Z}/12\mathbb{Z}$.

1. Déterminer le sous-groupe H de G engendré par $\overline{6}$ et $\overline{8}$. Déterminer son ordre.
2. Caractériser les générateurs de G.
3. Quel est l'ordre de l'élément $\overline{9}$?

7.1.23

On considère dans cette exercice le groupe symétrique S_4. On note

$$s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = 2134 \quad s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = 1324 \quad s_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = 1243.$$

1. Écrire tous les éléments de S_4 comme un produit de transpositions adjacentes ;
2. Calculer les ordres et les longueurs des éléments de S_4.
3. On considère les sous-groupes de S_4 suivants :

$$H = \langle s_1, s_2 \rangle ; \quad K = \langle s_2, s_3 \rangle \quad \text{et} \quad L = \langle s_1, s_3 \rangle .$$

   (a) Quels sont les ordres de H, K et L ?
   (b) Écrire la table de multiplication de ces sous-groupes. Sont-ils abéliens ?
   (c) Que remarquez-vous ?

7.1.24

Soit $n \in \mathbb{N}^*$, montrer que

1. La fonction $k\mathbb{Z} \mapsto \langle k \rangle$ est une bijection entre l'ensemble des sous-groupes $k\mathbb{Z}$ de $\mathbb{Z}$ tel que $k|n$ et l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.
2. $\mathbb{Z}/n\mathbb{Z} = \langle x \rangle$ si et seulement si $\text{pgcd}(x, n) = 1$.
3. $(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$.

7.1.25

(*Relations de tresse*) Dans S_n, montrer que pour tout $1 \leq i, j \leq n$: $\tau_i \tau_j = \tau_j \tau_i$ si $|i-j| > 1$ et que $\tau_i \tau_j \tau_i = \tau_j \tau_i \tau_j$ si $|i-j| = 1$.

7.1.26

On considère la fonction

$$\begin{array}{rcl} \gamma : S_n & \to & \mathbb{Z}/2\mathbb{Z} \\ \sigma & \mapsto & \overline{\ell(\sigma)} = \ell(\sigma) + 2\mathbb{Z}. \end{array}$$

1. Montrer que $\gamma(e) = 2\mathbb{Z}$ et que $\gamma(\tau_i) = 1 + 2\mathbb{Z}$ pour tout $1 \leq i < n$.
2. Soit $\sigma\tau \in S_n$. Par récurrence sur $\ell(\sigma)$, montrer que $\ell(\sigma\tau) \equiv \ell(\sigma) + \ell(\tau) \pmod 2$.
3. Montrer que $\gamma(\sigma\tau) = \gamma(\sigma)\gamma(\tau)$, $\forall \sigma, \tau \in S_n$.

7.1.27

(a) Décomposer en cycles disjoints les permutations dans S_3 et dans S_4.

Exercice 8 Soit $\sigma = (a_1, \ldots, a_p) \in S_n$ un p-cycle, alors

1. $\sigma^{-1} = (a_1, a_p, a_{p-1}, \ldots a_2)$ est un p-cycle ;
2. $ordre(\sigma) = p$.

7.1.28

Considérons les deux permutations suivantes de S_9 : $\sigma = 492517683$ et $\tau = 719238465$.

1. Écrire σ et τ comme produits de cycles disjoints.
2. Trouver l'ordre de σ et de τ.
3. Écrire σ et τ comme produits de transpositions adjacentes.

7.1.29

(*Décomposition en cycles*) Soit $\sigma \in S_n$, montrer que σ s'écrit de manière unique comme produit de cycles disjoints (à l'ordre des facteurs près).

7.1.30

(*Classe de conjugaison de S_n*) (a) Soit $\sigma \in S_n$ et $\alpha = (a_1, \ldots, a_k)$ un k-cycle. Montrer que $\sigma\alpha\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))$ est un k-cycle.

(b) Montrer que $\alpha, \beta \in S_n$ sont conjugués si et seulement si pour tout k, α et β ont le même nombre de k-cycles dans leur décomposition en cycles disjoints. (On rappelle que si G est un groupe, on dit que x et y *sont conjugués dans* G si il existe $g \in G$ tel que $x = gyg^{-1}$.)

7.1.31

Soit une permutation $\sigma \in S_n$ et $\sigma = c_1 \ldots c_k$ la décomposition de σ en cycles disjoints, alors on a que $ordre(\sigma) = \text{ppcm}(ordre(c_1), ordre(c_2), ordre(c_3), \ldots, ordre(c_k))$.

7.1.32

Écrire la table du groupe diédral D_3. Comparer avec la table du groupe S_3 : que remarquez-vous ?

7.1.33

Soit $D_m = \langle s, r \rangle$ le groupe diédral d'ordre $2m$ engendré par la rotation r et la symétrie s usuelle. Soit $t = sr$, montrer que t est une involution et que $D_m = \langle s, t \rangle$.

7.2 Morphismes de groupes

7.2.1

On utilisera la notation $[k]_6$ pour désigner la classe de l'entier k modulo 6, et la notation $[k]_3$ pour désigner la classe de l'entier k modulo 3. On considère les groupes $(\mathbb{Z}/6\mathbb{Z}, +)$ et $(\mathbb{Z}/3\mathbb{Z}, +)$ et la fonction

$$f : (\mathbb{Z}/6\mathbb{Z}, +) \to (\mathbb{Z}/3\mathbb{Z}, +)$$

$$f([k]_6) = [k]_3$$

1) Montrer que f est bien définie, à savoir qu'on a toujours que si $[k]_6 = [m]_6$ alors $[k]_3 = [m]_3$.
2) Montrer que f est un homomorphisme surjectif.
3) Déterminer le noyau de f.

7.2.2

Soit $f \in \text{Hom}\,(G, G')$ et $H' \leq G'$. Montrer que $f^*(H') \leq G'$.

7.2.3

Soit G, G' et G'' trois groupes, montrer que
(i) $G \simeq G$; (ii) $G \simeq G' \iff G' \simeq G$; (iii) si $G \simeq G'$ et $G' \simeq G''$ alors $G \simeq G''$.

7.2.4

(1) Soit $f : G \to G'$ un morphisme de groupes injectif. Montrer que

1. $G \simeq f(G) = \mathrm{Im}(f)$;
2. $ordre(f(x)) = ordre(x)$ pour tout $x \in G$.

(2) Soit $G \simeq G'$ et $q \in \mathbb{N}^*$. Montrer que le nombre d'éléments de G d'ordre q est égal au nombre d'éléments de G' d'ordre q.

7.2.5

Soit $G = \langle x \rangle$ un groupe monogène. On considère la fonction

$$\begin{array}{rcl} f : \mathbb{Z} & \to & G \\ k & \mapsto & x^k. \end{array}$$

1. Montrer que f est un morphisme de groupes surjectif.
2. Montrer qu'il existe $n \in \mathbb{N}$ tel que $\ker(f) = n\mathbb{Z}$.
3. Si G est infini, montrer que $G \simeq \mathbb{Z}$.
4. $*$ Si G est fini d'ordre n, montrer que $G \simeq \mathbb{Z}/n\mathbb{Z}$.

7.2.6

(Translation à gauche) Soit G un groupe. Pour $g \in G$, on considère la fonction

$$\begin{array}{rcl} f_g : G & \to & G \\ x & \mapsto & gx. \end{array}$$

(a) Montrer que $f_g \in S_G$ et que $(f_g)^{-1} = f_{g^{-1}}$.
(b) Est-ce que f_g est un morphisme de groupes ?
(c) Montrer que $f_g \circ f_h = f_{gh}$ pour tout $g, h \in G$.

7.2.7

Soit G un groupe.

1. Montrer que l'ensemble $\mathrm{Int}\,(G)$ des morphismes intérieurs du groupe G est un sous-groupe de $\mathrm{Aut}\,(G)$.
2. Soit $g, g' \in G$, montrer que $\varphi_g = \varphi_{g'}$ si et seulement si $g^{-1}g' \in Z(G)$ le centre du groupe G.
3. Montrer que si G est fini, alors $|\mathrm{Int}\,(G)| \leq |G|$.
4. Calculer $\mathrm{Int}\,(S_3)$ et $\mathrm{Int}\,(\mathbb{Z}/n\mathbb{Z})$.

7.2.8

Montrer que
(a) le groupe diédral D_m est isomorphe à un sous-groupe de S_m.
(b) $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à un sous-groupe de S_n.

7.3 Classe modulo un sous-groupe et groupes quotients

7.3.1

Soit G un groupe et $H \leq G$, montrer que

1. si $x \in G$ alors $xH = H$ si et seulement si $x \in H$;
2. si $x, y \in G$ alors $xH = yH \iff x^{-1}yH = H \iff y^{-1}xH = H \iff x^{-1}y \in H$;
3. si G est abélien, alors $xH = Hx$ pour tout $x \in G$;
4. si $x, y \in G$, alors $y \in xH \iff y^{-1} \in Hx^{-1}$;
5. si $x \in H$, alors la fonction $h \mapsto xh$ est une bijection de H sur xH.
6. En déduire que xH, H et Hx ont même cardinal.

7.3.2

On considère $G = S_3$.

1. Donner tous les sous-groupes de S_3 ;
2. pour tout sous-groupe H de S_3, donner G/H et $H\backslash G$.

7.3.3

Soit G un groupe d'ordre p premier, montrer que G est cyclique.

7.3.4

Soit G un groupe et H, K deux sous-groupes finis de G.

1. Montrer que si $|H|$ et $|K|$ sont premiers entre eux, alors $H \cap K = \{e\}$.
2. On pose $n = [H \,:\, H \cap K]$. Soit $\{x_i \,|\, 1 \leq i \leq n\}$ un système de représentants des classes de $H/H \cap K$.
   (a) Montrer que $\{x_i K \,|\, 1 \leq i \leq n\}$ est une partition de HK.
   (b) Montrer que
   $$|HK| = |KH| = \frac{|H||K|}{|H \cap K|}.$$

7.3.5

Soit G un groupe abélien d'ordre $|G| = nm$ où n et m sont premiers entre eux. Soit H et K deux sous-groupes de G tel que $|H| = n$ et $|K| = m$. Montrer que $G \simeq H \times K$.

7.3.6

Soit G un groupe et $H_1, \ldots, H_n$ des sous-groupes de G *d'indice fini*. Montrer par récurrence sur $n \in \mathbb{N}^*$ que l'indice du sous-groupe $\bigcap_{i=1}^{n} H_i$ est fini.

7.3.7

Soit G un groupe et $x, y \in G$ d'ordre fini tel que $xy = yx$. Montrer que :
(a) xy est d'ordre fini ; (b) si $ordre(x) = n$ et $ordre(y) = m$ sont premiers entre eux, alors $ordre(xy) = nm$.

7.3.8

(Formule de l'indice) Soit H un sous-groupe d'indice fini d'un groupe G et $K \leq H$. Le but de ce problème est de montrer que K est d'indice fini dans G si et seulement si il est d'indice fini dans H, ainsi que la formule suivante :
$$[G \,:\, K] = [G \,:\, H][H \,:\, K].$$

1. Si $K \subseteq H$, notons $I \subseteq G$ un système de représentant des classes à gauche modulo H et $J \subseteq H$ un système de représentant des classes à gauche H/K modulo K.
   Montrer que
   (a) $\Lambda = IJ$ est un système de représentant des classes G/K ;
   (b) Λ est en bijection avec $I \times J$.
2. Montrer que $[G \,:\, K] = [G \,:\, H][H \,:\, K]$.
3. En déduire que K est d'indice fini dans G si et seulement si il est d'indice fini dans H.

7.3.9

(La preuve « savante » du théorème de Wilson [1]) Cet exercice a pour but de proposer une preuve du théorème de Wilson qui exploite les notions de ce chapitre.

Théorème 7.1 (Wilson). *Soit $n \in \mathbb{N}$, $n \geq 2$, alors n est premier si et seulement si* $(n-1)! \equiv -1 \pmod{n}$.

1. Montrer que $x = \overline{(p-1)!}$ est est le produit de tous les éléments du groupe abélien $(\mathbb{Z}/p\mathbb{Z})^\times$.
2. Soit G un groupe abélien fini et x le produit des éléments de G.
   (a) Si $|G|$ est impair, montrer que $x = e$;
   (b) si $|G|$ est pair et G ne contient qu'une involution alors montrer que x est cette unique involution ;
   (c) si $|G|$ est pair et G contient plus d'une involution, montrer que $x = e$ (difficile).
3. En déduire la preuve du théorème de Wilson.

7.3.10

Soit G un groupe et $H \leq G$, montrer que les propositions suivantes sont équivalentes.

1. $H \lhd G$;
2. $xHx^{-1} = H$, $\forall x \in G$;
3. $x^{-1}Hx = H$, $\forall x \in G$;
4. $xhx^{-1} \in H$, $\forall x \in G$, $\forall h \in H$;
5. $x^{-1}hx \in H$, $\forall x \in G$, $\forall h \in H$.

7.3.11

Soit G un groupe et $H \leq G$ d'indice 2, montrer que H est normal dans G.

7.3.12

Soit G un groupe, montrer que $\mathrm{Int}\,(G) \lhd \mathrm{Aut}\,(G)$.

7.3.13

Soit G un groupe et $S \subseteq G$. Posons $H = \langle S \rangle$.
(a) Montrer que si $xSx^{-1} \subseteq H$ pour tout $x \in G$, alors $H \lhd G$.
(b) Si $f : G \to G'$ est un isomorphisme, montrer que $f(H) = \langle f(S) \rangle$.

1. John Wilson, 1741-1793.

7.3.14

Dans le groupe symétrique S_4, on considère

$$H = \langle (1,2)(3,4) \rangle \quad \text{et} \quad K = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

(a) Vérifier que $K = \langle (1,2)(3,4), (1,3)(2,4) \rangle$.
(b) Montrer que $H \lhd K$ et $K \lhd S_4$, mais que H n'est pas normal dans S_4.

7.3.15

Soit G un groupe et $H, K \leq G$, montrer que

1. si $H \lhd G$ et $K \leq G$ contenant H alors $H \lhd K$;
2. $H \lhd G \Longrightarrow H \cap K \lhd G$;
3. En déduire que l'intersection de sous-groupes normaux de G est un sous-groupe normal de G.

7.3.16

Soit G un groupe et $H, K \leq G$.

1. Montrer que $HK \leq G \iff HK = KH$.
2. Montrer que si $HK \leq G$ alors $HK = \langle H \cup K \rangle$. Est-ce que dans ce cas HK est abélien ?
3. Montrer que si $H \lhd G$ alors $HK \leq G$ et $H \lhd HK$.

7.3.17

Soit $f : G \to G'$ un morphisme de groupes, montrer que

1. si $H \lhd G$ alors $f(H) \lhd f(G)$, et que si f est surjective alors $f(H) \lhd G$. Est-ce vrai dans le cas où f n'est pas surjective ?
2. Si $H' \lhd G'$ alors $f^*(H') \lhd G$.

7.3.18

Si $f : G \to G'$ est un morphisme de groupes, montrer que $G/\ker(f) \simeq \mathrm{Im}(f)$.

7.3.19

Soit $n \in \mathbb{N}$ et $d|n$.

1. Montrer qu'il existe un morphisme de groupes injectif $\iota : (\mathbb{Z}/d\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$.
2. Montrer qu'il existe un morphisme de groupes surjectif $\varphi : (\mathbb{Z}/n\mathbb{Z}, +) \to (\mathbb{Z}/d\mathbb{Z}, +)$.

7.3.20

Soit G un groupe, $H \lhd G$ et K est un sous-groupe de G contenant H. On note $\pi : G \to G/H$ le morphisme surjectif canonique. Montrer que

1. $\pi(K) \simeq K/H$;
2. si $K = \langle S \rangle$ alors $\pi(K) = \langle \pi(S) \rangle$;
3. si K est fini, alors $|\pi(K)| = |K|/|H|$.

7.3.21

Donner tous les sous-groupes de $(\mathbb{Z}/20\mathbb{Z}, +)$.

7.3.22

(*Deuxième et troisième théorèmes d'isomorphisme*)
Soit G un groupe et $H \lhd G$ et $K \leq G$.

1. Montrer que $H \cap K \lhd G$ et $K/(K \cap H) \simeq HK/H$.
2. Si de plus $K \lhd G$ et $K \subseteq H$, montrer que $H/K \lhd G/K$ et $(G/K)/(H/K) \simeq G/H$.

Indice : Se servir du premier théorème d'isomorphisme.

7.3.23

Soit G un groupe, montrer que si $G/Z(G)$ est un groupe monogène, alors G est abélien.

7.3.24

Justifier les isomorphismes suivants :

1. $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$;
2. $(\mathbb{R}/\mathbb{Z}, +) \simeq (\mathbb{U}, \cdot)$;
3. $(\mathbb{C}^*/\mathbb{R}^{+*}, \cdot) \simeq (\mathbb{U}, \cdot)$;
4. $(\mathbb{C}^*/\mathbb{R}^*, \cdot) \simeq (\mathbb{U}, \cdot)$;
5. $(\mathbb{U}/\mathbb{U}(n), \cdot) \simeq (\mathbb{U}, \cdot)$;
6. $(\mathbb{C}^*/\mathbb{U}(n), \cdot) \simeq (\mathbb{C}^*, \cdot)$.

7.3.25

Soit G un sous-groupe d'indice fini dans $(\mathbb{C}^*, \cdot)$, montrer que $G = (\mathbb{C}^*, \cdot)$.

7.4 Les produits directs de groupes

7.4.1

(B1) Soit $G_1, \ldots, G_n$ des groupes et $\sigma \in S_n$,c'est-à-dire une permutation de $1, 2, \ldots, n$. Vérifiez que l'application

$$\varphi_\sigma : G_1 \times \ldots \times G_n \to G_{\sigma(1)} \times \ldots \times G_{\sigma(n)}$$

définie par

$$\varphi_\sigma(g_1, \ldots, g_n) = (g_{\sigma(1)}, \ldots, g_{\sigma(n)})$$

est un isomorphisme. Cela montre que l'ordre des facteurs d'un produit direct n'est pas essentiel.

7.4.2

(A1) Soit A_1, A_2, B_1, B_2 des groupes et $f : A_1 \to A_2$, $g : B_1 \to B_2$ des isomorphismes. Vérifiez que $h : A_1 \times B_1 \to A_2 \times B_2$ défini par $h(a, b) = (f(a), g(b))$ est un isomorphisme.

7.4.3

(B1) Soit H, K des groupes et $G = H \times K, A = \{e_H\} \times K$ et $B = H \times \{e_K\}$. Vérifiez que que $A \triangleleft G, B \triangleleft G$, et que G/A est isomorphe à H et G/B isomorphe à K.

7.4.4

(B1) Soit G un groupe et $H_i \trianglelefteq G$ [2],$i = 1, \ldots, n$ tels que $G = H_1 H_2 \ldots H_n$. Vérifiez que les énoncés suivants sont équivalents :

(1) Pour tout i, $H_i \cap \langle \bigcup_{j \neq i} H_j \rangle = \{e\}$.

(2) Tout élément $g \in G$ s'exprime de façon unique comme un produit d'éléments des H_i : $g = h_1 h_2 \ldots h_n, h_i \in H_i$.

7.4.5

(A1) Soient $A_1, \ldots, A_n$, $B_1, \ldots, B_n$ des groupes, $f_i : A_i \to B_i$, un isomorphisme, $i = 1, \ldots, n$. Soit la fonction

$$f : A_1 \times \ldots \times A_n \to B_1 \times \ldots \times B_n$$

définie par $f(a_1, \ldots, a_n) = (f_1(a_1), \ldots, f_n(a_n))$, où $a_i \in A_i$, $i = 1, \ldots, n$. Montrez que f est un isomorphisme.

2. C'est-à-dire : H_i est un sous-groupe normal de G.

7.4.6

(B1) Soit A un groupe abélien, B un sous-groupe de A et $f : A \to B$ un homomorphisme tel que $f(x) = x$ si $x \in B$ (N.B. Ceci n'entraîne pas que f est une bijection.)

(a) Montrez que si pour $a \in A$ on pose $a_1 = f(a^{-1})$, alors $aa_1 \in ker(f)$.

(b) Montrez que A est produit direct interne de $ker(f)$ et B.

7.5 La structure des groupes abéliens finis

7.5.1

(A2) Désignons par $ordre(z)$ l'ordre de l'élément z dans un groupe donné. Donnez un contre-exemple pour vérifier que la relation $ordre(xy) = p.p.c.m.(ordre(x), ordre(y))$ n'est pas valide en général.

7.5.2

(B1) Montrez que dans un groupe abélien fini A, il existe pour tout diviseur d de $|A|$, un sous-groupe d'ordre d. (N.B. C'est en quelque sorte une réciproque du théorème de Lagrange pour les groupes abéliens.)

7.5.3

(B1) Soit $n > 1$ un entier qui n'est pas divisible par le carré d'un autre entier plus grand que 1. Montrez alors que tout groupe abélien fini d'ordre n est cyclique.

7.5.4

(B1) Énumérez tous les groupes abéliens d'ordre 72, à isomorphisme près.

7.5.5

(C1) Les groupes $\mathbb{Z}_{12} \times \mathbb{Z}_{72}$ et $\mathbb{Z}_{18} \times \mathbb{Z}_{48}$ sont-ils isomorphes ?

7.5.6

(B1) Soit G un groupe abélien, $H_1, \ldots, H_n$ des sous-groupes, et $H = H_1 H_2 \cdots H_n$.

(a) Montrez que $H \leq G$.

(b) Montrez que H est le plus petit sous-groupe de G qui contienne $H_1 \cup \cdots \cup H_n$.

7.5.7

(A1) Faites la liste de tous les groupes abéliens finis d'ordre 252, à isomorphisme près. Justifiez.

7.6 Les actions de groupes

7.6.1

(A1) Soit G un groupe opérant sur un ensemble Ω. On dira qu'un sous-ensemble Γ de Ω est *invariant par rapport à* G ou G*-invariant*, si $g.x \in \Gamma$ pour tout $g \in G$ et tout $x \in \Gamma$. Montrez que tout sous-ensemble invariant de Ω est une réunion d'orbites et que la G-orbite de tout élément $x \in \Omega$ n'est autre chose que le sous-ensemble invariant le plus petit contenant x.

7.6.2

(B1) Soit G un groupe et E un ensemble. Vérifiez qu'une action de G sur E correspond à un homomorphisme de G dans le groupe S_E des permutations de E, de la manière suivante.

(a) Soit $\alpha : G \times E \to E$ une action de G sur E. Vérifiez que l'application $\tilde{\alpha} : G \to S_E$, définie par $\tilde{\alpha}(g) = \alpha_g$, est un homomorphisme, où $\alpha_g(x) = g.x$.

(b) Soit $\varphi : G \to S_E$ un homomorphisme. Vérifiez que l'application $\overline{\varphi} : G \times E \to E$, définie par $\overline{\varphi}(g, x) = (\varphi(g))(x)$ donne une action de G sur E.

(c) Vérifiez que les correspondances $\alpha \mapsto \tilde{\alpha}$ et $\varphi \mapsto \overline{\varphi}$ établies en (a) et (b) sont inverses l'une de l'autre.

7.6.3

(A1) Montrez que le groupe A_4 ne possède pas de sous-groupe d'ordre 6 (même si 6 est un diviseur de 12 qui est l'ordre de A_4).

7.6.4

(C2) Dans cet exercice nous allons établir des propriétés de base du groupe symétrique S_n.

(a) Considérons l'action naturelle du groupe symétrique S_n sur l'ensemble $\{1, 2, \ldots, n\}$ et soit $s \in S_n$. En considérant l'action induite du sous-groupe $H = \langle s \rangle$ engendré par s et les orbites de cette action, montrez que s se décompose en un produit de permutations cycliques disjointes ou cycles disjoints, c.-à-d. $(i_1, \ldots, i_s) \ldots (j_1, \ldots, j_t)$ tel que $\{i_1, \ldots, i_s\} \cap \{j_1, \ldots, j_t\} = \emptyset$. Vérifiez que des cycles disjoints commutent entre eux et que la décomposition ci-dessus est unique à l'ordre des facteurs près.

(b) Soit n un entier naturel. Mettons-le sous la forme d'une somme

$$n = n_1 + n_2 + \ldots + n_m$$

avec

$$n_1 \geq n_2 \geq \ldots \geq n_m \geq 1$$

Une telle décomposition est appelée une partition de n ou un partage de n. Si on désigne le nombre de toutes ces partitions par $p(n)$, alors, par exemple, $p(3) = 3, p(4) = 5$, etc. La décomposition $s = s_1 \ldots s_m$ d'une permutation $s \in S_n$ en un produit de cycles disjoints, détermine une partition du nombre n. Montrez que les classes de conjugaison du groupe S_n sont en correspondance biunivoque avec les partitions du nombre n. (Aide : si $s = s_1 \ldots s_m$, où les s_i sont des cycles disjoints, alors $rsr^{-1} = rs_1r^{-1}rs_2r{-}1 \ldots rs_mr^{-1}$; on a aussi pour tout cycle $(i_1, \ldots, i_k)$ de longueur k , $r(i_1, i_2, \ldots, i_k)r^{-1} = (r(i_1), r(i_2), \ldots, r(i_k))$.

7.6.5

(B1)

(a) Soit $g : \mathbb{C} \to \mathbb{C}$ un automorphisme d'anneaux de $\mathbb{C}$, c.-à-d. un automorphisme du groupe additif $(\mathbb{C}, +)$ mais qui a aussi la propriété que $g(xy) = g(x)g(y)$ pour tous $x, y \in \mathbb{C}$. Vérifiez que pour tout $x \in \mathbb{Q}$, on a $g(x) = x$. (Aide : vérifiez d'abord que $g(1) = 1$.)

(b) Soit $f \in \mathbb{Q}[X]$ un polynôme à coefficients dans $\mathbb{Q}$, et soit

$$E = \{z \in \mathbb{C} : f(z) = 0\}$$

l'ensemble des racines de f. Soit G le groupe des automorphismes d'anneaux de $\mathbb{C}$. Vérifiez que pour tout $z \in E$ et tout $g \in G$ on a $g(z) \in E$, et que l'opération de $G \times E$ dans E définie par $g.z = g(z)$ donne une action de G sur E. (Rappel : l'opération dans le groupe G est la composition des fonctions.)

7.6.6

(C1) Soit $f \in \mathbb{Q}[X]$ et G le groupe des automorphismes d'anneau de $\mathbb{C}$. On sait que G agit de façon naturelle sur l'ensemble $L = \{z \in C : f(z) = 0\}$ des racines de f.

(a) Montrez que deux racines de f qui appartiennent à la même orbite doivent être racines d'un même facteur irréductible de f dans $\mathbb{Q}[X]$.

(b) Déduire de (a) que si f n'a pas de racine multiple et que l'action de G sur L n'a qu'une seule orbite, alors f est irréductible dans $\mathbb{Q}[X]$.

7.6.7

(B1) En s'appuyant sur le fait que tout p-groupe possède un centre qui ne se réduit pas à l'élément identité, démontrez que tout groupe d'ordre p^2 est abélien. (Aide : passez à un groupe quotient.)

7.6.8

(A1) Soit un groupe G opérant sur un ensemble E et soit $Y \subseteq E$. Montrez que $\{g \in G : g.y = y, \text{ pour tout } y \in Y\}$ est un sous-groupe de G.

7.6.9

Soit

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} ; a, b, c \in \mathbb{R} \text{ et } ac \neq 0 \right\}$$

(a) Vérifiez que G est un sous-groupe de $GL_2(\mathbb{R})$ et que G agit sur $\mathbb{R}$ par l'opération

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} .x = \frac{ax + b}{c}$$

(b) Déterminez l'orbite de 0 et le stabilisateur de 0 pour cette action.

7.6.10

(A1) Une bijection $f : \mathbb{R}^3 \to \mathbb{R}^3$ est appelée une *isométrie* si elle conserve la distance entre les points, c'est-à-dire, si pour tous points $P, Q \in \mathbb{R}^3$ on a $distance(f(P), f(Q)) = distance(P, Q)$. Par exemple, une rotation est une isométrie, une symétrie par rapport à un plan fixé (*image miroir*) est aussi une isométrie (N.B. Il y en a d'autres). Montrez que les isométries forment un sous-groupe du groupe $S_{\mathbb{R}^3}$ de toutes les permutations de $\mathbb{R}^3$. Soit $\mathcal{ISO}_{\mathbb{R}^3}$ le groupe des isométries de $\mathbb{R}^3$, vérifiez que $\mathcal{ISO}_{\mathbb{R}^3}$ agit sur $\mathbb{R}^3$ par l'action naturelle $\mathcal{ISO}_{\mathbb{R}^3} \times \mathbb{R}^3 \to \mathbb{R}^3$, définie par $f.P = f(P)$.

7.6.11

(A1) Soit p un nombre premier et G l'ensemble suivant de matrices à coefficients dans le corps $\mathbb{Z}_p$ des entiers modulo p

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$$

(a) Vérifiez que G est un sous-groupe de $GL_3(\mathbb{Z}_p)$, qu'il a p^3 éléments, et qu'il n'est pas abélien.

(b) Vérifiez que le centre de G est formé des matrices suivantes

$$C(G) = \left\{ \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : t \in \mathbb{Z}_p \right\}$$

7.6.12

(B1) Montrez que tout groupe d'ordre 96 possède au moins un sous-groupe normal propre.

7.6.13

(A1) Soient A et B deux sous-groupes d'un groupe G. On considère l'action de B sur $\mathcal{P}(G)$ par translation à gauche. Montrez que $Stab_B(A) = A \cap B$.

7.6.14

(B1) Soit G un groupe fini opérant sur un ensemble E. Montrez que si G n'est pas isomorphe au groupe additif $\mathbb{Z}_2$ et que E possède un élément dont l'orbite possède exactement deux éléments, alors G possède au moins un sous-groupe normal propre.

7.6.15

(A1) Si un groupe d'ordre 104 ne contient pas de sous-groupe normal d'ordre 8, combien a-t-il de sous-groupes d'ordre 8 ?

7.6.16

(B1) Soit G un groupe fini et $T \lhd G$. Soit p un nombre premier et supposons que p ne divise pas $[G : T]$. Montrez que T contient tous les p-sous-groupes de Sylow de G.

7.6.17

(B1) Soit G un groupe fini, et soit p le plus petit diviseur premier de $|G|$. Supposons que G possède un sous-groupe H tel que $[G : H] = p$. Le but de cet exercice est de montrer qu'on a alors $H \lhd G$. Soit $E = \{H, x_1H, \ldots, x_{p-1}H\}$ l'ensemble des translatés de H. Comme on l'a vu, G opère sur E par translation à gauche. Cela donne un homomorphisme $\varphi : G \to S_E$ de G dans le groupe des permutations de E.

(a) Rappelez la définition de φ.

(b) Montrez que $ker(\varphi) \subseteq H$.

(c) Soit $K = \{f \in S_E : f(H) = H\}$. Montrez que K est un sous-groupe de S_E et que $|K| = (p-1)!$.

(d) Soit $L = \{\varphi(h) : h \in H\}$ l'image de H par φ. Vérifiez que $L \leq K$ et déduisez-en que $|L|$ divise $(p-1)!$.

(e) Montrez que $|L|$ divise $|H|$. (Aide : considérez la restriction $\varphi|_H : H \to L$ et utilisez le théorème des homomorphismes.)

(f) Montrez que $|L| = 1$ en utilisant l'hypothèse faite sur p. Déduisez-en que $H = ker(\varphi)$, de sorte que $H \lhd G$!

N.B. Ce résultat généralise le cas particulier déjà vu où $p = 2$.

7.6.18

(A1) Soit p un nombre premier.

(a) Montrez que dans un groupe d'ordre $4p$, un p-sous-groupe de Sylow est toujours normal si $p \geq 5$.

(b) Est-ce vrai pour $p = 3$? Justifiez.

7.6.19

(C1) Montrez que tous les groupes d'ordre plus petit que 60 possède au moins un sous-groupe normal propre, sauf les groupes dont l'ordre est un nombre premier.

7.6.20

(B1)

(a) Montrez que tout groupe d'ordre 20 possède au moins un sous-groupe normal propre.

(b) Vérifiez que l'opération de $\mathbb{R}^* \times \mathbb{C}$ dans $\mathbb{C}$ définie par $r.z = rz$ constitue une action du groupe multiplicatif $\mathbb{R}^*$ sur l'ensemble des nombres complexes $\mathbb{C}$, et pour chaque $z \in \mathbb{C}$ calculez $Stab(z)$ et décrivez géométriquement $Orb(z)$ dans le plan complexe.

(c) Considérons G le groupe des isométries de l'icosaèdre. Vérifiez que G possède un sous-groupe d'ordre 2 qui est normal.

7.7 Exercices supplémentaires

7.7.1

(A1) Vérifiez que chacune des structures suivantes forme un anneau.

(a) On fixe X un ensemble non vide, et soit

$$\mathbb{R}^X = \{f : f \text{ est une fonction de } X \text{ dans } \mathbb{R}\}$$

On considère $(\mathbb{R}^X, +, -, \cdot, 0, 1)$, où $0, 1$ désigne les fonctions constantes de valeur 0 et 1 respectivement et où pour $f, g \in \mathbb{R}^X$, $f + g$, $f \cdot g$, $-f$ sont définis comme suit : $(f + g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x)g(x)$, $(-f)(x) = -f(x)$.

(b) $(C(\mathbb{R}), +, -, \cdot, 0, 1)$, où

$$C(\mathbb{R}) = \{f : f\text{est une fonction continue de } \mathbb{R} \text{ dans } \mathbb{R}\}$$

et les opérations $+, -, \cdot$ et les éléments distingués $0, 1$ sont définis comme en a).

(c) Soit A un anneau unitaire, $n \geq 1$. Considérons $(M_n(A), +, -, \cdot, O_n, I_n)$, où $M_n(A)$ désigne l'ensemble des matrices carrées d'ordre n à coefficients dans A, et $+, -, \cdot$ les opérations habituelles sur les matrices. O_n est la matrice nulle et I_n la matrice identité, toutes deux construites avec les éléments adéquats de A.

(d) Soit A un anneau unitaire commutatif, $n \geq 1$, $X_1, \ldots, X_n$ des indéterminées. On considère $(A[X_1, \ldots, X_n], +, -, \cdot, 0, 1)$, où $A[X_1, \ldots, X_n]$ désigne l'ensemble des polynômes en $X_1, \ldots, X_n$ à coefficients dans $A, 0$ et 1 sont les polynômes constants correspondant aux éléments adéquats de A, et $+, -, \cdot$ désignent les opérations habituelles sur les polynômes.

7.7.2

(A1) Montrez que les règles de calcul suivantes sont valables dans tout anneau, disons A.

(a) Pour tout $a \in A, a \cdot 0 = 0 = 0 \cdot a$.

(b) Pour tous $a, b \in A, (-a)b = a(-b) = -(ab)$ et $(-a)(-b) = ab$ et $-a = (-1)a$.

(c) Pour tous $a_1, \ldots, a_n, b_1, \ldots, b_m \in A, (a_1 + \ldots + a_n)(b_1 + \ldots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$.

(c) Pour tous $a, b \in A$ et $k \in \mathbb{Z}, k(ab) = (ka)b = a(kb)$.

7.7.3

(B2) Soit A un anneau commutatif. Montrez que les éléments inversibles de $M_n(A)$ sont les matrices dont le déterminant donne un élément inversible dans A. (N.B. Le déterminant est défini de la même façon que pour les matrices réelles.)

7.7.4

(C1) Soit $\mathbb{G} = \{a + bi : a, b \in \mathbb{Z}\}$, les *entiers de Gauss*, et pour $z \in \mathbb{G}$ soit $N(z) = |z|^2$. Vérifiez que $\mathbb{G}$ est un sous-anneau de $\mathbb{C}$ et que la fonction $N : \mathbb{G} \to \mathbb{N}$ a la propriété $N(xy) = N(x)N(y)$. Montrez que pour tous $x, y \in G, y \neq 0$, il existe $q, r \in \mathbb{G}$ tel que $x = qy + r$ et $N(r) < N(y)$. (N.B. : (1) représentez $\mathbb{G}$ dans le plan complexe (2) $N(x) < N(y) \iff |x| < |y|$).

7.7.5

(A1) *(Les quaternions de Hamilton*[3]*)* Soit $\mathbb{R}^4$ muni de l'addition et de la multiplication suivantes :

$$(a_1, b_1, c_1, d_1) + (a_2, b_2, c_2, d_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2, d_1 + d_2)$$

3. William Rowan Hamilton, 1805-1865.

$$\begin{aligned}(a_1, b_1, c_1, d_1) \cdot (a_2, b_2, c_2, d_2) &= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2, a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2, \\ &\quad a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2, a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\end{aligned}$$

(a) Vérifiez que $(1, 0, 0, 0)$ est un élément neutre pour cette multiplication.

(b) Vérifiez que $\mathbb{R}^4$ muni de cette addition et de cette multiplication forme un anneau. On appelle cet anneau l'anneau des quaternions et on le désigne par $\mathbb{H}$.

7.7.6

(A1) Pour les valeurs $p = 3, 5, 7, 11, 13$, trouvez le plus petit entier qui donne un générateur pour le groupe multiplicatif du corps $\mathbb{F}_p$ des entiers modulo p.

7.7.7

(B1) Soit K un corps fini de caractéristique p et ζ un générateur du groupe cyclique K^*. Montrez que ζ^p est aussi un générateur de K^*.

Chapitre 8

Solutions

8.4 Les produits directs de groupes

8.4.5

On a $A_1, \ldots, A_n, B_1, \ldots, B_n$ des groupes
$f_i : A_i \to B_i,$ des isomorphismes
$f : A_1 \times \ldots \times A_n \to B_1 \times \ldots \times B_n$
$f(a_1, \ldots, a_n) = (f_1(a_1), \ldots, f_n(a_n))$

À voir : f est un isomorphisme de groupes.

(i) f est un homomorphisme : soient $\vec{a} = (a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n$
$\vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \in A_1 \times \ldots \times A_n$

À voir : $f(\vec{a}\vec{\alpha}) = f(\vec{a})f(\vec{\alpha})$.

On a

$$\begin{aligned} f(\vec{a}\vec{\alpha}) &= f((a_1, \ldots, a_n)(\alpha_1, \ldots, \alpha_n)) \\ &= f(a_1\alpha_1, \ldots, a_n\alpha_n) \\ &= (f_1(a_1\alpha_1), \ldots, f_n(a_n\alpha_n)) \\ &= (f_1(a_1)f_1(\alpha_1), \ldots, f_n(a_n)f_n(\alpha_n)) \\ &= (f_1(a_1), \ldots, f_n(a_n))(f_1(\alpha_1), \ldots, f_n(\alpha_n)) \\ &= f(\vec{a})f(\vec{\alpha}) \end{aligned}$$

tel que voulu.

(ii) f est une bijection :
f est injectif, c.- à-d., $\ker f = \{e\}$: supposons $\vec{a} = (a_1, \ldots, a_n)$ tel que $f(\vec{a}) = e$ alors on a $f(\vec{a}) = (f_1(a_1), \ldots, f_n(a_n)) = (e_1, \ldots, e_n)$, où e_i est l'élément neutre de B_i. D'où $f_i(a_i) = e_i$ et

alors $a_i = e_{A_i}$ puisque f est un isomorphisme. Ainsi $\vec{a} = (e_{A_1}, \ldots, e_{A_n}) = e_{A_1 \times \ldots \times A_n}$ tel que voulu.
f est surjectif : soit $\vec{b} = (b_1, \ldots, b_n) \in B_1 \times \ldots \times B_n$. Puisque f_i est un isomorphisme, il existe $a_i \in A_i$ tel que $f_i(a_i) = b_i$. En posant $\vec{a} = (a_1, \ldots, a_n)$ on obtient $f(\vec{a}) = \vec{b}$, tel que voulu.

8.5 La structure des groupes abéliens finis

8.5.2

On a un groupe abélien fini A et d un diviseur de $|A|$.

À voir : A possède un sous-groupe d'ordre d. (Réciproque du théorème de Lagrange pour les groupes abéliens).
Soit $|A| \simeq p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ la décomposition de $|A|$ en facteurs premiers distincts alors $d = p_1^{k_1} \ldots p_n^{k_n}$ où $k_i \leq \alpha_i$.
On a $A \simeq A(p_1) \times \cdots \times A(p_n)$, la *décomposition* en produit direct des composantes primaires.
Il suffit de montrer que $A(p_i)$ possède un sous-groupe d'ordre p^{k_i}
En effet, supposons qu'on ait $H_i < A(p_i)$ tel que $|H_i| = p^{k_i}$.
Alors

$$H_1 \times \cdots \times H_n < A(p_i) \times \cdots \times A(p_n)$$

et

$$|H_1 \times \cdots \times H_n| = |H_1| \cdot \cdots \cdot |H_n| = p_1^{k_1} \ldots p_n^{k_n} = d.$$

Donc $A(p_1) \times \cdots \times A(p_n)$ posséderait un sous-groupe d'ordre d d'où A, qui lui est isomorphe, posséderait aussi un sous-groupe d'ordre d.
On se ramène donc à considérer le cas des p-groupes.
Soit donc

$$G \text{ un } p-\text{groupe, disons } |G| = p^\alpha$$
$$d \text{ un diviseur de } |G|, \text{ disons } d = p^k$$

À voir : G possède un sous-groupe d'ordre p^k.
Considérons la *décomposition* de G en sous-groupes cycliques.

$$G \simeq G_1 \times \cdots \times G_r, \ |G_i| = p^{\alpha_i}, \text{ disons } \alpha_1 \leq \cdots \leq \alpha_r$$

Si $k = \alpha_i$ pour un certain i alors le sous-groupe G_i fait l'affaire.
Si $k = \alpha_{i_1} + \cdots + \alpha_{i_s}$ pour certains $\alpha_{i_1} \leq \cdots \leq \alpha_{i_s}$ alors

$$\{e\} \times \cdots \times \{e\} \times G_{\alpha_{i_1}} \times \{e\} \times \cdots \times G_{\alpha_{i_2}} \times \{e\} \times \cdots \times G_{\alpha_{i_s}} \times \{e\} \times \cdots \times \{e\}$$

est un sous-groupe de $G_1 \times \cdots \times G_r$ qui est d'ordre d, d'où G qui est isomorphe à $G_1 \times \cdots \times G_r$ possède aussi un sous-groupe d'ordre d.

Sinon soit i_0 l'indice maximum tel que

$$\alpha_1 + \cdots + \alpha_{i_0} < k.$$

Alors on a

$$\alpha_1 + \cdots + \alpha_{i_0} < k < \alpha_1 + \cdots + \alpha_{i_0} + \alpha_{i_0+1}$$

$$k - (\alpha_1 + \cdots + \alpha_{i_0}) < \alpha_{i_0+1}$$

Comme $G_{\alpha_{i_0}+1}$ est cyclique d'ordre $p^{\alpha_{i_0+1}}$, il possède un sous-groupe d'ordre $p^{k-(\alpha_1+\cdots+\alpha_{i_0})}$, disons H_{i_0}. (N.B. $G_{\alpha_{i_0+1}} \simeq \mathbb{Z}_{p^{\alpha_{i_0+1}}}$ et $\langle p^{\alpha_1+\cdots+\alpha_{i_0+1}-k} \rangle$ est un sous-groupe d'ordre $p^{k-(\alpha_1+\cdots+\alpha_{i_0})}$ de $\mathbb{Z}_{p^{\alpha_{i_0+1}}}$)
Alors $G_{\alpha_1} \times \cdots \times G_{\alpha_{i_0}} \times H_{i_0} \times \{e\} \times \{e\} \times \cdots \times \{e\}$ est un sous-groupe de $G_1 \times \cdots \times G_r$ d'ordre $p^{\alpha_1} p^{\alpha_2} \cdots p^{\alpha_{i_0}} \cdot p^{k-(\alpha_1+\cdots+\alpha_{i_0})} = p^k = d$.
Donc G, qui est isomorphe à $G_1 \times \cdots \times G_r$, possède aussi un sous-groupe d'ordre d.

8.5.3

On a un groupe abélien fini G tel que $|G| = n$ n'est pas divisible par le carré d'un entier plus grand que 1.

À voir : G est cyclique.
L'hypothèse assure que $|G| = p_1 \dots p_k$, où les p_i sont des nombres premiers distincts.
On a la *décomposition* de G en produit direct de ses composantes primaires

$$G \simeq G(p_1) \times \ldots \times G(p_k)$$

On sait que $|G(p_i)| = p_i$.
Donc

$$G(p_i) \simeq \mathbb{Z}_{p_i}$$

et

$$G \simeq \mathbb{Z}_{p_i} \times \ldots \times \mathbb{Z}_{p_n}.$$

Par ailleurs on sait que

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_i} \times \ldots \times \mathbb{Z}_{p_n}.$$

D'où $G \simeq \mathbb{Z}_n$ et donc G est cyclique.

8.5.4

À voir : Énumérez tous les groupes abéliens non isomorphes d'ordre 72 (à isomorphisme près).
On a $72 = 8 \cdot 9 = 2^3 \cdot 3^2$.
Soit G un groupe abélien d'ordre 72.
On a

$$G \simeq G(2) \times G(3), \quad |G(2)| = 2^3, \ |G(3)| = 3^2$$

et en considérant les possbilités pour $G(2)$ et $G(3)$ on obtient la liste suivante (par le théorème d'unicité pour la décomposition en p-groupes cycliques).

1) $\mathbb{Z}_8 \times \mathbb{Z}_9$
2) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$
3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$
4) $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
5) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
6) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

8.6 Les actions de groupes

8.6.1

On a G qui opère sur un ensemble Ω et $\Gamma \subseteq \Omega$ tel que Γ est G-invariant.
À voir :

(1) Γ est une réunion d'orbites.

(2) L'orbite d'un élément $x \in \Omega$ est le plus petit sous-ensemble G-invariant auquel appartient x.

Notons

(i) Toute orbite est un ensemble G-invariant
En effet soit $y \in \mathrm{Orb}(x)$, disons $y = g_\circ.x$ alors pour tout $g \in G$, $g.y = g.(g_\circ.x) = (gg_\circ).x$ d'où $g.y \in \mathrm{Orb}(x)$.

(ii) Si $x \in \Gamma$ alors $\mathrm{Orb}(x) \subseteq \Gamma$
En effet si $x \in \Gamma$ alors pour tout $g \in G$ $g.x \in \Gamma$, c.-à-d. $\mathrm{Orb}(x) \subseteq \Gamma$.

Pour (1) : $\Gamma = U\{\mathrm{Orb}(x) : x \in \Gamma\}$:
$\subseteq$: puisque $x \in \mathrm{Orb}(x)$
$\supseteq$: par (ii) $\mathrm{Orb}(x) \subseteq \Gamma$ pour tout $x \in \Gamma$ d'où $U\{\mathrm{Orb}(x) : x \in \Gamma\} \subseteq \Gamma$.
Donc Γ est bien une réunion d'orbites.

Pour (2)
Par (i) Orb(x) est un ensemble G-invariant auquel appartient x.
Par (ii) Orb(x) est contenu dans tout ensembe G-invariant auquel appartient x. Donc Orb(x) est bien le plus petit sous-ensemble G-invariant auquel appartient x.

8.6.2

À voir :
Vérifiez qu'une action d'un groupe G sur un ensemble E correspond à un homomorphisme de G dans le groupe S_E des permutations de E.
Soit

$$G \text{ un groupe}$$
$$E \text{ un ensemble non vide}$$

La correspondance cherchée est la suivante :
A une action $\alpha : G \times E \to E$.
On fait correspondre l'homomorphisme $\tilde{\alpha} : G \to S_E$, défini par $\tilde{\alpha}(g) = \alpha_g$, où α_g est l'application $\alpha_g : E \to E, \alpha_g(x) = g.x$.
A un homomorphisme $\varphi : G \to S_E$
On fait correspondre l'action $\bar{\varphi} : G \times E \to E$, définie par $\bar{\varphi}(g, x) = \varphi(g)(x)$.
Nous allons vérifier que ces correspondances sont bien justifiées et inverses l'une de l'autre.

(1) Soit $\alpha : G \times E \to E$ une action de G sur E. Pour $g \in G$ on a déjà vérifié que l'application

$$\alpha_g : E \to E$$

défini par $\alpha_g(x) = g.x$ est une bijection dont l'inverse est $\alpha_{g^{-1}}$. Soit $\tilde{\alpha} : G \to S_E$ défini par $\tilde{\alpha}(g) = \alpha_g$.
$\tilde{\alpha}$ est un homomorphisme
En effet, pour $g, h \in G$ on a que pour tout $x \in E$,

$$\begin{aligned} \alpha_{gh}(x) &= (gh).x \\ &= g.(h.x) \\ &= \alpha_g(\alpha_h(x)) \\ &= (\alpha_g \circ \alpha_h)(x) \end{aligned}$$

D'où $\alpha_{gh} = \alpha_g \circ \alpha_h$ i.e. $\tilde{\alpha}(gh) = \tilde{\alpha}(g)\tilde{\alpha}(h)$. Ce qui montre que $\tilde{\alpha}$ est bien un homomorphisme.

(2) Soit $\varphi : G \to S_E$ un homomorphisme et $\bar{\varphi} : G \times E \to E$ l'application définie par $\bar{\varphi}(g, x) = \varphi(g)(x)$.
$\bar{\varphi}$ est une action de G sur E

(2.1) pour tout $x \in E, e.x = x$
En effet, pour $x \in E$,

$$\begin{aligned} e.x &= \varphi(e).(x) \\ &= \mathrm{id}(x), \text{ car } \varphi \text{ est un homomorphisme.} \end{aligned}$$

(2.2) pour tout $g, h \in G$ et $x \in E$, $g.(h.x) = (gh).x$
En effet soit $g, h \in G$ et $x \in E$, on a

$$\begin{aligned} g.(h.x) &= g.(\varphi(h)(x)) \\ &= \varphi(g)(\varphi(h)(x)) \\ &= (\varphi(g) \circ \varphi(h))(x) \\ &= \varphi(gh)(x), \text{ car } \varphi \text{ est un homomorphisme} \\ &= (gh).x \end{aligned}$$

(3) Les correspondances ci-dessus sont inverses l'une de l'autre

En effet soit α une action de G sur E et $\widetilde{\tilde{\alpha}}$ l'action associée à l'homomorphisme $\tilde{\alpha}$. Alors, on a pour $g \in G$ et $x \in E$, $\widetilde{\tilde{\alpha}}\ (g, x) = \tilde{\alpha}(g)(x) = \alpha_g(x) = g.x = \alpha(g.x)$.

Donc l'action $\widetilde{\tilde{\alpha}}$ coïncide avec l'action de départ α.

Réciproquement soit φ un homomorphisme de G dans S_E et $\widetilde{\bar{\varphi}}$ l'homomorphisme associé à l'action $\bar{\varphi}$.

Alors pour $g \in G$ et $x \in E$ on a

$$\widetilde{\bar{\varphi}}\ (g)(x) = \bar{\varphi}_g(x) = \varphi(g)(x)$$

Donc l'homomorphisme $\widetilde{\bar{\varphi}}$ coïncide avec l'homomorphisme de départ φ.

8.6.3

À voir : Le groupe A_4 n'a pas de sous-groupe d'ordre 6.

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}.$$

Les éléments de A_4 sont d'ordre 1,2 ou 3, et donnent les groupes cycliques suivants :

$$\begin{aligned} \{e\}, H_1 &= \{e, (12)(34)\}, H_2 = \{e, (13)(24)\}, H_3 = \{e, (14)(23)\} \\ K_1 &= \{e, (123), (132)\},\ K_2 = \{e, (124), (142)\}, \\ K_3 &= \{e, (134), (143)\},\ K_4 = \{e, (234)(243)\} \end{aligned}$$

Considérons la possibilité d'avoir un sous-groupe $H \leq A_4$ de cardinal 6. Il faudrait que ses éléments soient d'ordre $1, 2, 3$ ou 6. Or A_4 ne possède que des éléments d'ordre 2 ou 3 et il n'y a que 4 éléments d'ordre 2, donc H devrait posséder au moins un élément d'ordre 2 et un élément d'ordre 3.
Mais si par exemple $(12)(34) \in H$ et $(123) \in H$, alors on aurait aussi $(132) = (123)(123) \in H, (12)(34)(123) = (243) \in H, (12)(34)(132) = (143)$, $(123)(12)(34) = (134)$ ce qui ferait déjà 7 éléments (en comptant e), ce qui serait absurde. On vérifie de même pour les autres possibilités. Plus précisément, H doit contenir au moins un H_i et un K_j, mais on vérifie que $\langle H_i \cup K_j \rangle = A_4$.

8.6.4

Le groupe symétrique

On considère l'action naturelle du groupe symétrique S_n sur $\{1, 2, \ldots, n\}$.

(a) (Décomposition d'une permutation en cycles disjoints).
Soit $\sigma \in S_n$ et $H = \langle \sigma \rangle$. Posons $\Omega = \{1, 2, \ldots, n\}$. Considérons l'action de H sur Ω. Soit

$$\Omega = \Omega_1 \dot{\cup} \ldots \dot{\cup} \Omega_k$$

la décomposition de Ω en H-orbites. $\Omega_i = \{k_{i_1}, \ldots, k_{i_{l_i}}\}$ tel que $k_{i_1} = \min \Omega_i$.

Notons que $\Omega_i = \{k_{i_1}, \sigma(k_{i_1}), \sigma^2(k_{i_1}), \ldots, \sigma^{l_i^{-1}}(k_{i_1})\}$.
Posons σ_i le cycle de longueur $l_i, \sigma_i = (k_{i_1}\sigma(k_{i_1}) \ldots \sigma^{l_i-1}(k_{i_1}))$ de sorte que les cycles σ_i sont disjoints.
$\underline{\sigma = \sigma_1\sigma_2 \ldots \sigma_k}$: soit $j \in \Omega$

$$\text{si } j \notin \Omega_i, \text{ alors } \sigma_i(j) = j \qquad (*)$$

de sorte que $\sigma_1\sigma_2 \ldots \sigma_k(j) = \sigma_i(j)$, pour l'unique i tel que $j \in \Omega_i$. Mais alors $j = \sigma^{(r)}(k_{i_0})$, pour un certain $1 \leq r < l_i$ et $\sigma_i(j) = \sigma_i(\sigma^{(r)}(k_{i_0})) = \sigma(\sigma^{(r)}(k_{i_0})) = \sigma(j)$.
Ainsi $\sigma_1 \ldots \sigma_k(j) = \sigma(j)$, pour tout $j \in \Omega$.
Des cycles disjoints commutent entre eux
Soit $\mu = (k_1 \ldots k_l), \nu = (t_1 \ldots t_m)$ des cycles disjoints. Alors

$$\begin{array}{ll} \mu(t_i) = t_i & \text{pour tout } t_i, \quad \mu(k_i) \in \{k_1, \ldots, k_l\} \text{ et} \\ \nu(k_i) = k_i & \text{pour tout } k_i, \quad \nu(t_i) \in \{t_1, \ldots, t_m\} \end{array}$$

De sorte que pour $j \in \Omega$, on a

$$\mu\nu(j) = \begin{cases} j & \text{si } j \notin \{k_1, \ldots, k_l, t_1, \ldots, t_m\} \\ \nu(j) & \text{si } j \in \{t_1, \ldots, t_m\} \\ \mu(j) & \text{si } j \in \{k_1, \ldots, k_l\} \end{cases}$$

et de même

$$\nu\mu(j) = \begin{cases} j & \text{si } j \notin \{k_1, \ldots, k_l, t_1, \ldots, t_m\} \\ \nu(j) & \text{si } j \in \{t_1, \ldots, t_m\} \\ \mu(j) & \text{si } j \in \{k_1, \ldots, k_l\} \end{cases}$$

Donc on a bien $\mu\nu = \nu\mu$.

Unicité de la décomposition en cycles disjoints

Supposons $\sigma = \tau_1, \ldots \tau_m$ une décomposition de σ en cycles disjoints.

Soit

$$\tau_i = (t_{i_1} \ldots t_{in_i}), \quad t_{i_1} = \min_{1 \le j \le m_i} \{t_{ij}\}$$

et $E_i = \{t_{i_1}, \ldots, t_{i_{n_i}}\}$.

On note que soit $\sigma(j) = j$ soit $\sigma(j) = \tau_i(j)$ où $j \in E_i$, uniquement déterminé puisque les cycles τ_i sont disjoints.

Par ailleurs soit $j \in \Omega_{i_0}$, alors $\sigma(j) = \sigma_{i_0}(j)$ et on a

$$\begin{aligned} \tau_i &= (j\ \tau_i(j) \ldots \tau_i^{n_i^{-1}}(j)) \\ \sigma_{i_0} &= (j\ \sigma_{i_0}(j) \ldots \sigma_{i_0}^{l_{i_0}^{-1}}(j)) \text{ et} \\ \sigma_{i_0}^k(j) &= \sigma^k(j) = \tau_i^k(j), \text{ pour tout } k = 1, 2, \ldots \end{aligned}$$

D'où $n_i = l_{i_0}$ et $\tau_i = \sigma_{i_0}$.

On en déduit

$$\begin{aligned} \sigma\sigma_{i_0}^{-1} &= \sigma\tau_i^{-1} \\ \sigma_1 \ldots \hat{\sigma}_{i_0} \ldots \sigma_k &= \tau_1 \ldots \hat{\tau}_i \ldots \tau_m, \end{aligned}$$

puisque les cycles disjoints commutent. $*$

On a maintenant deux décompositions avec un cycle en moins et on peut conclure par récurrence.

$*$ N.B. $(t_1 \ldots t_5)^{-1} = (t_5 t_{5-1} \ldots t_2 t_1)$.

(b) **Les classes de conjugaison de S_n**

(b.1) Soit $\sigma \in S_n$ et

$$\sigma = \sigma_1 \ldots \sigma_m$$

la décomposition de σ en cycles disjoints de longueur $l(\sigma_i) = n_i$ avec $n_1 \ge n_2 \ge \ldots \ge n_m$. Posons $\Omega_i = \{k_{i_1}, \ldots, k_{i_{n_i}}\}$. Ce sont les H-orbites de Ω pour $H = \langle\sigma\rangle$, de sorte que $n = n_1 + n_2 + \cdots + n_m$ et on a une partition du nombre n.

(b.2) D'autre part soit

$$n = n_1 + n_2 + \cdots + n_m, \quad n_1 \ge n_2 \ge \cdots \ge n_m$$

une partition du nombre n, alors cette partition est associée à la permutation

$$\sigma = (1, 2 \dots n_1)(n_1 + 1, \dots, n_1 + n_2) \dots (n_1 + \cdots + n_{m-1}, \dots, n_1 + \cdots + n_m)$$

par le procédé vu en (b.1).

(b.3) Soit $\mathbb{P}(n)$ l'ensemble des partitions de n. $\Phi : S_n \to \mathbb{P}$ l'application définie par le procédé décrit en (b.1). Par (b.2) on sait que Φ est surjective. Pour montrer la correspondance biunivoque entre les classes de conjugaison de S_n et $\mathbb{P}_n$, il suffit de voir que pour $\sigma, \tau \in S_n$.
σ, τ sont conjugués ssi $\Phi(\sigma) = \Phi(\tau)$
Supposons σ, τ conjugués, disons $\tau = \rho\sigma\rho^{-1}$.
Soit $\sigma = \sigma_1\sigma_2 \dots \sigma_m$ la décomposition en cycles disjoints comme ci-dessus.
On a $\tau = \rho\sigma_1\rho^{-1}\rho\sigma_2\rho^{-1} \dots \rho\sigma_m\rho^{-1}$. D'autre part

$$\rho\sigma_i\rho^{-1} = \rho(k_{i_1}\sigma_i(k_{i_1}) \dots \sigma_i^{l_{i-1}}(k_{i_1}))\rho^{-1}.$$

Notons que

$$\begin{array}{l} \text{si } \rho^{-1}(j) \notin \Omega_i, \text{ alors } \rho\sigma_i\rho^{-1}(j) = j \\ \text{si } \rho^{-1}(j) \in \Omega_i, \text{ disons } \rho^{-1}(j) = \sigma_i^{(t)}(k_{i_1}) \end{array}$$

alors $\rho\sigma_i\rho^{-1}(j) = \rho(\sigma_i^{(t+1)}(k_{i_1}))$. Donc les seuls éléments non laissés fixes par $\rho\sigma_i\rho^{-1}$ sont les $\rho(k)$ pour $k \in \Omega_i$ et on a

$$\rho\sigma_i\rho^{-1} = (\rho(k_{i_1})\rho(\sigma_i(k_{i_1})) \dots \rho(\sigma_i^{l_i-1}(k_{i_1})))$$

Ainsi les $\rho\sigma_i\rho^{-1}$ sont des cycles disjoints : si $\rho(\sigma_i^{(t)}(k_{i_1})) = \rho(\sigma_j^{(k)}(k_{j_1}))$ pour $i \neq j$ alors $\sigma_i^{(t)}(k_{i_1}) = \sigma_j^{(k)}(k_{j_1})$ ce qui ne peut être le cas.
Comme $\rho\sigma_i\rho^{-1}$ est un cycle de même longueur que σ_i, on a bien $\Phi(\tau) = \Phi(\sigma)$.
Supposons $\Phi(\tau) = \Phi(\sigma)$, disons qui correspondent à la partition $n = n_1 + n_2 + \cdots + n_m$, $n_1 \geq n_2 \geq \cdots \geq n_m$. Il suffit de montrer que τ et σ sont tous deux conjugués à

$$\lambda = (1\, 2 \dots n_1)(n_1 + 1, \dots, n_1 + n_2) \dots (n_1 + \cdots + n_{m-1}, \dots, n_1 + \cdots + n_m)$$

Soit $\sigma = \sigma_1 \dots \sigma_m$ comme ci-dessus $\sigma_i = (k_{i_1}\sigma(k_{i_1}) \dots \tau^{n_{i-1}}(k_{i_1}))$.
Soit $\rho \in S_n$ défini par le tableau

$$\begin{array}{lccccccc} \Omega = & \{k_{11} & \sigma(k_{11}) & \dots & \sigma^{n_1^{-1}}(k_{11}) & k_{21} & \sigma(k_{21}) \\ \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow \\ \Omega : & 1 & 2 & & n_1 & n_1 + 1 & n_1 + 2 \end{array}$$

$$\begin{array}{lccccccc} \Omega = & \dots & \sigma^{n_2^{-1}}(k_{21}) & \dots & k_{m_1} & \dots & \sigma^{n_m}(k_{m_1})\} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \Omega : & & n_1 + n_2 & \dots & n_1 + \cdots + n_{m-1} + 1 & & n_1 + \cdots + n_m \end{array}$$

Alors, par un calcul déjà fait,

$$\begin{aligned}\rho\sigma\rho^{-1} &= (\rho(k_{11}),\dots,\rho(\sigma^{n_1-1}(k_{11})))(\rho(k_{21})\dots\rho(\sigma^{n_2^{-1}}(k_{21})))\dots \\ &\qquad (\rho(k_{m1})\dots\rho(\sigma^{n_m^{-1}}(k_{m1}))) \\ &= (1\dots n_1)(n_1+1\dots n_1+n_2)\dots(n_1+\dots+n_{m-1}+1,\dots,n_1+\dots+n_m) \\ &= \lambda\end{aligned}$$

De même τ est conjugué à λ.

8.6.6

Soit G un groupe et $C(G) = \{g \in G : \text{ pour tout } h \in G, gh = hg\}$ le centre de G. Notons que $e \in C(G)$.
À voir : $C(G) \leq G$.

(i) $g_1, g_2 \in C(G)$ entraîne $g_1g_2 \in C(G)$.
Supposons $g_1, g_2 \in C(G)$ et soit $h \in G$. On a

$$\begin{aligned}g_1g_2h &= g_1hg_2 \text{ , car } g_2 \in C(G) \\ &= hg_1g_2 \text{ , car } g_1 \in C(G)\end{aligned}$$

Donc $g_1g_2 \in C(G)$.
(ii) $g \in C(G)$ entraîne $g^{-1} \in C(G)$.
Supposons $g \in C(G)$ et soit $h \in G$. On a $hg = gh$, d'où $h = g^{-1}hg$ et $hg^{-1} = g^{-1}h$. Donc $g^{-1} \in C(G)$.

8.6.7

Supposons p un nombre premier et G un groupe d'ordre p^2.
À voir : G est abélien.

On sait que le centre de G est non trivial, disons $x \in C(G), x \neq e$.
Si $ordre(x) = p^2$, alors $G = \langle x\rangle$ est cyclique, donc abélien.
Si $ordre(x) = p$, alors $H = \langle x\rangle$ est un sous-groupe normal de G et G/H est un groupe d'ordre p. Donc G/H est cyclique, disons

$$G/H = \langle yH\rangle = \{H, yH, \dots, y^{p-1}H\}$$

Alors

$$G = H \cup yH \cup \dots \cup y^{p-1}H$$

$$G = \{e, x, x^2, \ldots, x^{p-1}, y, yx, yx^2, \ldots, yx^{p-1}, \ldots, y^{p-1}x, \ldots, y^{p-1}x^{p-1}\}$$

Donc tout $g \in G$ s'exprime sous la forme $g = y^i x^j$. Mais alors, disons $g_1 = y^i x^j$, $g_2 = y^k x^l$. On obtient

$$\begin{aligned} g_1 g_2 &= y^i x^j y^k x^l \\ &= y^i y^k x^j x^l \text{ , car } x \in C(G) \\ &= y^{i+k} x^{j+l} = y^{k+i} x^{l+j} \\ &= y^k y^i x^l x^j \\ &= y^k x^l y^i x^j \text{ , car } x \in C(G) \\ &= g_2 g_1 \text{ tel que voulu.} \end{aligned}$$

8.6.8

On a G qui opère sur E, on a $Y \subseteq E$, et $H = \{g \in H : g.y = y, \text{ pour tout } y \in Y\}$.

À voir : $H \leq G$.

Notons que $H = \{g \in G : g \in Stab(y), \text{ pour tout } y \in Y\}$. Ainsi

$$H = \bigcap_{y \in Y} Stab(y)$$

et on sait d'une part que $Stab(y)$ est un sous-groupe de G et d'autre part que l'intersection d'une famille de sous-groupes est aussi un sous-groupe. D'où $H \leq G$.

8.6.9

On a $G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R}, \ ac \neq 0 \right\}$.

(a) (a.1) $G \leq GL_2(\mathbb{R})$. [1]

(a.2) G agit sur $\mathbb{R}$ par l'opération $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \cdot x = \dfrac{ax+b}{c}$.

(a.1) $\underline{G \leq GL_2(\mathbb{R})}$

(a.1.1) On a $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$, $I = e_{GL_2(\mathbb{R})}$ l'élément neutre de $GL_2(\mathbb{R})$.

1. Rappelons que $GL_2(\mathbb{R})$ est le groupe des matrices réelles de format 2×2 qui sont inversibles. L'opération est le produit matriciel.

(a.1.2) $\underline{A, B \in G \Rightarrow AB \in G}$. Disons $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, B = \begin{bmatrix} e & f \\ 0 & g \end{bmatrix}$, $ac \neq 0, eg \neq 0$. Donc $a \neq 0, c \neq 0, e \neq 0, g \neq 0$.
On a $AB = \begin{bmatrix} ae & af+bg \\ 0 & cg \end{bmatrix}$ et $aecg = aceg \neq 0$.
Donc on a bien $AB \in G$, tel que voulu.

(a.1.3) $\underline{A \in G \Rightarrow A^{-1} \in G}$. Disons $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$. Alors $A^{-1} = \begin{bmatrix} a^{-1} & -ba^{-1}c^{-1} \\ 0 & c \end{bmatrix}$, et $a^{-1}c^{-1} \neq 0$.
Donc on a bien $A^{-1} \in G$, tel que voulu.

(a.2) (a.2.1) $I \cdot x = x$.
(a.2.2) $A_1 \cdot (A_2 \cdot x) = (A_1 A_2) \cdot x$.

(a.2.1) On a $I \cdot x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot x = \dfrac{1 \cdot x + 0}{1} = x$, tel que voulu.

(a.2.2) Disons $A_1 = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, A_2 = \begin{bmatrix} e & f \\ 0 & g \end{bmatrix}, ac \neq 0, eg \neq 0$.
On a

$$A_1 \cdot (A_2 \cdot x) = A_1 \cdot \left(\frac{ex+f}{g}\right) = \frac{a\left(\frac{ex+f}{g}\right) + b}{c} = \frac{aex + af + bg}{cg}$$

$$(A_1 A_2) \cdot x = \begin{bmatrix} ae & af+bg \\ 0 & cg \end{bmatrix} \cdot x = \frac{aex + af + bg}{cg}$$

Donc on a bien $A_1 \cdot (A_2 \cdot x) = (A_1 A_2) \cdot x$.

(b) (b.1) Orb(0).
(b.2) Stab(0).

(b.1) Notons que $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \cdot 0 = \dfrac{a \cdot 0 + b}{c} = \dfrac{b}{c}$, et avec des choix appropriés, $\dfrac{b}{c}$ prend toutes les valeurs réelles.
Donc Orb(0)=$\mathbb{R}$.

(b.2) On a $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \cdot 0 = 0$ exactement quand $b = 0$.
Donc Stab(0) $= \left\{ \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix} : \ a, c \in \mathbb{R}, a, c \neq 0 \right\}$.

8.6.10

Soit $ISO_{\mathbb{R}^3}$ l'ensemble des isométries de $\mathbb{R}^3$.
À voir :

(a) $ISO_{\mathbb{R}^3} \leq S_{\mathbb{R}^3}$

(b) $ISO_{\mathbb{R}^3}$ agit sur $\mathbb{R}^3$ par l'action naturelle $f.P = f(P)$

(a.1) $f, g \in ISO_{\mathbb{R}^3}$ entraîne $f \circ g \in ISO_{\mathbb{R}^3}$.
Supposons $f, g \in ISO_{\mathbb{R}^3}$ et considérons $P, Q \in \mathbb{R}^3$. On a

$$distance(f(g(P)), f(g(Q))) = distance(g(P), g(Q))$$

car $f \in ISO_{\mathbb{R}^3}$, et

$$distance(g(P), g(Q)) = distance(P, Q)$$

car $g \in ISO_{\mathbb{R}^3}$. D'où

$$distance(f(g(P)), f(g(Q))) = distance(P, Q)$$

tel que voulu.
(a.2) $f \in ISO_{\mathbb{R}^3}$ entraîne $f^{-1} \in ISO_{\mathbb{R}^3}$.
Supposons $f \in ISO_{\mathbb{R}^3}$. Considérons $P, Q \in \mathbb{R}^3$. On a

$$distance(f^{-1}(P), f^{-1}(Q)) = distancef((f^{-1}(P)), f(f^{-1}(Q)))$$

car $f \in ISO_{\mathbb{R}^3}$. D'où

$$distance(f^{-1}(P), f^{-1}(Q)) = distance(P, Q)$$

tel que voulu.

(b) On a l'action naturelle déjà vue

$$ISO_{\mathbb{R}^3} \times \mathbb{R}^3 \to \mathbb{R}^3$$

$$f.P = f(P)$$

L'action considérée est l'action induite par le sous-groupe $ISO_{\mathbb{R}^3}$.

8.6.11

On a p premier et

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{Z}_p \right\}.$$

a) $G \leq GL_3(\mathbb{Z}_p), |G| = p^3, G$ n'est pas abélien.

$\underline{G \leq GL_3(\mathbb{Z}_p)}$: $e_{GL_3(\mathbb{Z}_p)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ est bien dans G.

Soient $X, Y \in G$, disons $X = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, Y = \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix}$

on a

$$XY = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{bmatrix}$$

qui est bien dans G.

Notons que

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

donc $X^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$, et c'est bien dans G.

$\underline{|G| = p^3}$: on peut choisir a, b, c indépendamment dans $\mathbb{Z}_p$, ce qui fait $p \cdot p \cdot p = p^3$ choix.

L'exemple suivant montre que G n'est pas abélien

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

b) $C(G) = \left\{ \begin{bmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : t \in \mathbb{Z}_p \right\}$

Notons que

$$\begin{bmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & b+t \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & t+b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

donc $\begin{bmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in C(G)$. Il reste à voir qu'il n'y a pas d'autres éléments dans $C(G)$.

Notons que

$$\begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & d+a & b+dc+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{bmatrix}$$

de sorte que pour que $\begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} \in C(G)$ il faut que $dc = af$, pour tous $a, c \in \mathbb{Z}_p$.

En particulier il faut que $d = f$.

Mais alors si $d = f \neq 0$, il faudrait que

$$\begin{aligned} dc &= ad, && \text{pour tous } a, c \in \mathbb{Z}_p \\ d^{-1}dc &= add^{-1}, && \text{pour tous } a, c \in \mathbb{Z}_p. \\ c &= a, && \text{pour tous } a, c \in \mathbb{Z}_p. \end{aligned}$$

ce qui serait absurde.

Donc on doit avoir $d = 0, f = 0$, tel que voulu.

8.6.12

Soit G un groupe d'ordre 96. Nous allons utiliser les théorèmes de Sylow. On a $96 = 2^5 \cdot 3$. Considérons N_2 le nombre de 2-sous-groupes de Sylow. On a $N_2 \equiv 1$ modulo 2, et $N_2 | 96$. Les possibilités sont

$N_2 = 1$ et $N_2 = 3$. Si $N_2 = 1$, alors l'unique 2-sous-groupe de Sylow est normal, par le 2^e théorème de Sylow. Si $N_2 = 3$, soient H, K deux 2-sous-groupes de Sylow ; ils sont d'ordre 32. L'intersection $H \cap K$ est un sous-groupe d'ordre $2, 4, 8$ ou 16. Si $|H \cap K| \leq 8$, alors

$$\begin{aligned} |HK| &= \frac{|H| \cdot |K|}{|H \cap K|} \\ &\geq \frac{32 \cdot 32}{8} = 128 \end{aligned}$$

ce qui est trop dans un groupe d'ordre 96. Ainsi, on doit avoir $|H \cap K| = 16$. Alors

$$|HK| = \frac{32 \cdot 32}{16} = 64$$

Par ailleurs, $H \cap K$ est d'indice 2 dans H, et aussi dans K, d'où $H \cap K \lhd H$ et $H \cap K \lhd K$. Cela entraîne que $HK \subseteq N(H \cap K)$, le normalisateur de $H \cap K$. D'où $|N(H \cap K)| \geq 64$. Comme $|N(H \cap K)|$ doit aussi être un diviseur de 96, on doit avoir $|N(H \cap K)| = 96$, et donc $N(H \cap K) = G$, ce qui revient à dire que $H \cap K$ est un sous-groupe normal.

8.6.13

On a un groupe G et deux sous-groupes A et B, et on considère l'action de B sur les parties de G par translation à gauche.
À VOIR : $Stab_B(A) = A \cap B$.

(i) $A \cap B \subseteq Stab_B(A)$: soit $g \in A \cap B$, alors $gA = A$, puisque $g \in A$; donc on a bien $g \in Stab_B(A)$.

(ii) $Stab_B(A) \subseteq A \cap B$: soit $g \in Stab_B(A)$, alors $gA = A$ et en particulier $ge = g \in A$ (e désigne l'élément neutre), tel que voulu.

8.6.15

On a un groupe G d'ordre 104 et on considère les sous-groupes d'ordre 8. On suppose qu'aucun sous-groupe d'ordre 8 n'est normal. Notons que $104 = 2^3 \cdot 13$. Les sous-groupes d'ordre 8 sont donc les 2-sous-groupes de Sylow. Leur nombre, N_2, est impair et divise 104. Les possibilités sont $N_2 = 1$ ou $N_2 = 13$. Si $N_2 = 1$, alors l'unique 2-sous-groupe de Sylow serait normal par le 2^e théorème de Sylow, mais cela ne peut être le cas par hypothèse. La seule possibilité qui reste est $N_2 = 13$, et il y a donc 13 sous-groupes d'ordre 8.

8.6.17

On a G un groupe fini, p le plus petit diviseur premier de $|G|$, et $H \geq G$ tel que $[G : H] = p$. On a aussi l'ensemble des translatés à gauche de H, $E = \{H, x_1H, \ldots, x_{p-1}H\}$, et l'homomorphisme $\varphi : G \to S_E$ qui correspond à l'action de G sur E par translation à gauche. On a encore $K = \{f \in S_E : f(H) = H\}$ et $L = \{\varphi(h) : h \in H\}$.
À voir : $H \lhd G$.

(a) Pour $g \in G$ fixé, $\varphi(g)$ est la permutation de E donnée par la translation par l'élément g : $\varphi(g)(x_iH) = gx_iH$ et $\varphi(g)(H) = gH$.

(b) **À voir** : $ker(\varphi) \subseteq H$.
En effet, supposons $g \in ker(\varphi)$, c'est-à-dire que $\varphi(g)(x_iH) = x_iH$ et $\varphi(g)(H) = H$. En particulier, on a $gH = H$ et donc $g \cdot e = g \in H$, tel que voulu.

(c) **À voir** : $K \leq S_E$ et $|K| = (p-1)!$.
En effet, K est le stabilisateur de H pour l'action naturelle de S_E sur E. En fixant H, il reste $(p-1)$ éléments de E à permuter et tous les cas se réalisent, donc $|K| = |S_{p-1}| = (p-1)!$.

(d) **À voir** : $L \leq K$ et $|L| \mid (p-1)!$.
En effet, L est l'image de H par l'homomorphisme φ et c'est donc un sous-groupe de S_E. D'autre part, supposons $f \in L$, disons $f = \varphi(h)$, où $h \in H$, alors $f(H) = \varphi(h)(H) = hH = H$, puisque $h \in H$. Donc $L \subseteq K$ et ainsi $L \leq K$ et l'ordre de L divise $|K| = (p-1)!$, tel que voulu.

(e) **À voir** : $|L|$ divise $|H|$.
Considérons la restriction $\varphi\,|_H \colon H \to L$. Par le théorème des homomorphismes, $\varphi\,|_H$ se factorise par un isomorphisme de $H/ker(\varphi\,|_H)$ sur l'image de $\varphi\,|_H$ qui est L, d'où $|H| = |ker(\varphi\,|_H)| \cdot |L|$. D'où le résultat.

(f) **À voir** : $|L| = 1$ et $H = ker(\varphi)$.
En effet, par (d) et (e), $|L| < p$ et $|L|$ est un diviseur de $|H|$ et donc aussi un diviseur de $|G|$. Par l'hypothèse faite sur p, la seule possibilité est que $|L| = 1$. Mais alors φ envoie tous les éléments de H sur l'élément neutre de S_E, ou autrement dit $H \subseteq ker(\varphi)$. Par (b) on obtient $H = ker(\varphi)$.

8.7 Exercices supplémentaires

8.7.1

(a) On a $(\mathbb{R}^X, +, -, \cdot, 0, 1)$ où $0, 1$ désignent les fonctions constantes de valeur 0 et 1 respectivement et où les opérations $+, -, \cdot$ sont définies « point par point ».

(a.1) $(\mathbb{R}^X, +, -, 0)$ est un groupe abélien

Associativité : soit $f, g, h \in \mathbb{R}^X$.

À voir : $f + (g + h) = (f + g) + h$, c.-à-d. pour tout $x \in X$ $(f + (g + h))(x) = ((f + g) + h)(x)$.

Or on a pour $x \in X$.

$$\begin{aligned}(f + (g + h))(x) &= f(x) + (g + h)(x) \\ &= f(x) + (g(x) + h(x)) \\ &= (f(x) + g(x)) + h(x). \text{ (nous sommes maintenant dans } \mathbb{R}) \\ &= (f + g)(x) + h(x) \\ &= ((f + g) + h)(x)\end{aligned}$$

élément neutre : soit $f \in \mathbb{R}^X$.

À voir : $f + 0 = f$ et $0 + f = f$. Les deux sont semblables. Considérons $f + 0 = f$.

Il s'agit de voir que pour tout $x \in X, (f + 0)(x) = f(x)$. Or, pour $x \in X$ on a $(f + 0)(x) = f(x) + 0(x) = f(x) + 0 = f(x)$

Inverse : soit $f \in \mathbb{R}^X$.

À voir : $f + (-f) = 0$ et $(-f) + f = 0$. Les deux sont semblables. Considérons $f + (-f) = 0$.

Il s'agit de voir que pour tout $x \in X, (f + (-f))(x) = 0$.

Or, pour $x \in X$ on a

$$\begin{aligned}(f + (-f))(x) &= f(x) + (-f)(x) \\ &= f(x) + (-f(x)). \text{ (nous sommes maintenant dans } \mathbb{R}) \\ &= f(x) - f(x) \\ &= 0\end{aligned}$$

Commutativité : soit $f, g \in \mathbb{R}^X$.

À voir : $f + g = g + f$ c.-à-d. pour tout $x \in X$, $(f + g)(x) = (g + f)(x)$. On a bien pour $x \in X$,

$$\begin{aligned}(f + g)(x) &= f(x) + g(x) \\ &= g(x) + f(x). \text{ (nous sommes maintenant dans } \mathbb{R}) \\ &= (g + f)(x)\end{aligned}$$

Ainsi $(\mathbb{R}^X, +, -, 0)$ forme bien un groupe abélien.

N.B. : En vérifiant d'abord que l'opération + est commutative on évite d'avoir à considérer deux cas pour l'élément neutre et l'inverse.

(a.2) On note que dans les calculs précédents les propriétés voulues se vérifient directement du fait que la définition des opérations ("point par point") nous ramène aux propriétés analogues des nombres réels. De la même faǫn, l'associativité du produit, la distributivité du produit sur l'addition et le fait que la fonction constante 1 soit un élément neutre pour le produit se vérifient en se ramenant aux propriétés analogues des nombres réels.

(b) On a $(C(\mathbb{R}), +, -, \cdot, 0, 1)$, où $C(\mathbb{R}) = \{f \in \mathbb{R}^{\mathbb{R}} : f \text{ est continue}\}$ et les opérations sont définies comme en (a) avec $X = \mathbb{R}$.
Notons que par (a), $(\mathbb{R}^{\mathbb{R}}, +, -, \cdot, 0, 1)$ est un anneau unitaire. Or le sous-ensemble $C(\mathbb{R})$ de $\mathbb{R}^{\mathbb{R}}$ est fermé pour l'addition, l'inverse additif et le produit de $\mathbb{R}^{\mathbb{R}}$ puisque la somme et le produit de deux fonctions continues donne une fonction continue, et l'inverse additif d'une fonction continue est une fonction continue. Ainsi $(C(\mathbb{R}), +, -, \cdot, 0, 1)$ est un sous-anneau de $(\mathbb{R}^{\mathbb{R}}, +, -, \cdot, 0, 1)$, donc lui-même un anneau unitaire.

(c) On a $(M_n(A), +, -, \cdot, O_n, I_n)$, où A est un anneau unitaire, $M_n(A)$ est l'ensemble des matrices carrées d'ordre n à coefficients dans A et $+, -, \cdot$ les opérations habituelles sur les matrices.
Notons qu'on sait déjà que $M_n(A)$ forme un anneau dans le cas où A est un corps. Il s'agit de se rendre compte que les seules propriétés des corps en jeu ici sont celles d'anneau unitaire.
$(M_n(A), +, -, O_n)$ forme un groupe abélien
Comme pour le cas où A est un corps on se ramène directement au fait que la structure additive de l'anneau A forme un groupe abélien.
I_n est un élément neutre multiplicatif : vérification habituelle.
Associativité du produit soit $B, C, D \in M_n(A)$
À voir : $(BC)D = B(CD)$ disons $B = [b_{ij}], C = [c_{ij}], D = [d_{ij}], b_{ij}, c_{ij}, d_{ij} \in A$. Procédons en comparant directement les lignes de chaque côté.
Disons $D_i = i$-ème ligne de D.
On

$$\begin{aligned} \text{a la } i\text{-ème ligne de } (BC)D &= \sum_{j=1}^{n} \alpha_{ij} D_j, \text{ où } \alpha_{ij} = \sum_{k=1}^{n} b_{ik} c_{kj} \\ &= \sum_{j=1}^{n} \left(\sum_{k=1}^{n} b_{ik} c_{kj} \right) D_j \end{aligned}$$

D'autre part,

$$\begin{aligned} \text{la } i\text{-ème ligne de } B(CD) &= \sum_{k=1}^{n} b_{ik} \Lambda_k \\ &\quad \text{où } \Lambda_k \text{ est la } k\text{-ème ligne de } CD \\ &= \sum_{k=1}^{n} b_{ik} \left(\sum_{j=1}^{n} c_{kj} D_j \right) \end{aligned}$$

Or notons que $b_{ik}c_{kj}D_j = b_{ik}(c_{kj}D_j)$, en utilisant l'associativité de la multiplication dans A dans chaque composante.

D'où,

$$\begin{aligned} \text{la } i-\text{ème ligne de } B(CD) &= \sum_{k=1}^{n}\sum_{j=1}^{n} b_{ik}c_{kj}D_j \\ &= \text{la } i\text{-ème ligne de } (BC)D. \end{aligned}$$

Donc $(BC)D = B(CD)$.

Distributivité de $\cdot$ sur $+$ soit $B, C, D \in M_n(A)$

À voir : (1) $B(C+D) = BC + BD$.
(2) $(C+D)B = CB + DB$.

Disons $B = [b_{ij}], C = [c_{ij}], D = [d_{ij}], D_i =$ la i-ème ligne de $D, C_i =$ la i-ème ligne de $C, B_i =$ la i-ème ligne de B.

Procédons en comparant directement les lignes.

(1) La i-ème ligne de $B(C+D) = \sum_{j=1}^{n} b_{ij}(C_j + D_j)$.

D'autre part, la i-ème ligne de $BC + BD = \sum_{j=1}^{n} b_{ij}C_j + \sum_{j=1}^{n} b_{ij}D_j$.

Or notons que $b_{ij}(C_j + D_j) = b_{ij}C_j + b_{ij}D_j$, en utilisant la distributivité de la multiplication sur l'addition dans A dans chaque composante.

D'où :

$$\begin{aligned} \text{la } i\text{-ème ligne de } B(C+D) &= \sum_{j=1}^{n}(b_{ij}C_j + b_{ij}D_j) \\ &= \sum_{j=1}^{n} b_{ij}C_j + \sum_{j=1}^{n} b_{ij}D_j \\ &= \text{la } i\text{-ème ligne de } BC + BD \end{aligned}$$

Donc $B(C+D) = BC + BD$.

(2) La i-ème ligne de $(C+D)B = \sum_{j=1}^{n}(c_{ij} + d_{ij})B_j$.

D'autre part la i-ème ligne de $CB + DB = \sum_{j=1}^{n} c_{ij}B_j + \sum_{j=1}^{n} d_{ij}B_j$.

Or on a $(c_{ij} + d_{ij})B_j = c_{ij}B_j + d_{ij}B_j$, par la même remarque qu'en (1).

D'où

$$\begin{aligned}\text{la } i\text{-ème ligne de } (C+D)B &= \sum_{j=1}^{n}(c_{ij}B_j + d_{ij}B_j)\\ &= \sum_{j=1}^{n} c_{ij}B_j + \sum_{j=1}^{n} d_{ij}B_j\\ &= \text{la } i\text{-ème ligne de } CB + DB.\end{aligned}$$

N.B. : Dans la vérification des propriétés du produit de $M_n(A)$ on a utilisé les propriétés de l'addition de A, en particulier l'associativité qui nous a permis de regrouper des termes dans une somme (composante à composante dans les matrices lignes).

(d) On a $(A[X_1, \ldots, X_n], +, -, \cdot, 0, 1)$, où A est un anneau unitaire commutatif, avec les opérations habituelles sur les polynômes.

On sait déjà que $A[X, \ldots, X_n]$ forme un anneau dans le cas où A est un corps. Il s'agit de se rendre compte que les seules propriétés des corps utilisées dans ce cas sont celles d'anneau unitaires commutatif. Nous ne donnons pas les détails.

8.7.2

Soit A un anneau.

i) Soit $a \in A$. **À voir** : $a \cdot 0 = 0 = 0 \cdot a$.

Notons $\begin{aligned} a \cdot 0 &= a \cdot (0+0)\\ &= a \cdot 0 + a \cdot 0, \text{ par distributivité}\end{aligned}$

d'où $a \cdot 0 = 0$, puisque $(A, +, -, 0)$ forme un groupe.

De même $\begin{aligned} 0 \cdot a &= (0+0) \cdot a\\ &= 0 \cdot a + 0 \cdot a\end{aligned}$

d'où $0 \cdot a = 0$.

ii) Soit $a, b \in A$. **À voir** : $(-a)b = a(-b) = -(ab)$ si A est unitaire : $-a = (-1)a$.

Notons $\begin{aligned} (-a)b + ab &= (-a+a)b, \quad \text{par distributivité}\\ &= 0 \cdot b\\ &= 0, \quad \text{par } i)\end{aligned}$

d'où $(-a)b = -(ab)$, puisque $(A, +, -, 0)$ forme un groupe abélien.

De même $\begin{aligned} a(-b) + ab &= a(-b+b),\\ &= a \cdot 0\\ &= 0\end{aligned}$

d'où $a(-b) = -(ab)$.

iii) Soit $a_1, \ldots, a_n, b_1, \ldots, b_m \in A$.
À voir :

$$(a_1 + \cdots + a_n)(b_1 + \cdots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$$

Par induction sur m : $m = 1$: c'est la distributivité

$$\begin{aligned} m > 1 : (a_1 + \cdots + a_n)(b_1 + \cdots + b_m) \\ &= (a_1 + \cdots + a_n)b_1 + (a_1 + \cdots + a_n)(b_2 + \cdots + b_m) \\ &= a_1 b_1 + \cdots + a_n b_1 + \sum_{i=1}^{n} \sum_{j=2}^{m} a_i b_j, \text{ par induction \& distributivité} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j, \text{ puisque l'addition est commutative et associative.} \end{aligned}$$

iv) soit $a, b \in A, k \in \mathbb{Z}$, **À voir** : $k(ab) = (ka)b = a(kb)$.
Notons :

$$kx = \begin{cases} \underbrace{x + x + \cdots + x}_{k \text{ fois}} & , \text{ si } k > 0 \\ 0 & , \text{ si } k = 0 \\ -\underbrace{x + \cdots + x}_{|k| \text{ fois}} & , \text{ si } k < 0 \end{cases}$$

Cas 1 $k = 0 : 0(ab) = (0a)b = a(0b)$, par i)

Cas 2 $k > 0 :$ $\begin{aligned} (ka)b &= (a + a + \cdots + a)b \\ &= ab + ab + \cdots + ab, \text{ par distributivité} \\ &= k(ab) \end{aligned}$

et $\begin{aligned} a(kb) &= a(b + \cdots + b) \\ &= ab + \cdots + ab, \text{ par distributivité} \\ &= k(ab) \end{aligned}$

Cas 3 $k < 0 :$ $\begin{aligned} (ka)b &= -(a + \cdots + a)b \\ &= -[(a + \cdots + a)b], \text{ par ii)} \\ &= -(ab + \cdots + ab) \\ &= k(ab) \end{aligned}$

de même $a(kb) = a(-(b + \cdots + b)) = -[a(b + \cdots + b)] = -(ab + \cdots + ab) = k(ab)$.

8.7.3

(a) On a A un anneau unitaire

$$U(A) = \{a \in A : \ a \text{ est inversible}\}$$

À voir : $(U(A), \cdot, 1)$ forme un groupe,
c.-à-d. (a.1) $x, y \in U(A)$ entraîne $xy \in U(A)$
(a.2) $x \in U(A)$ entraîne $x^{-1} \in U(A)$

(a.1), (a.2) suffisent puisque $1 \in U(A)$ et qu'on sait que la multiplication est associative.

(a.1) soit $x, y \in U(A)$, soit x^{-1}, y^{-1} l'inverse de x et y.

$$xyy^{-1}x^{-1} = x\ 1\ x^{-1} = xx^{-1} = 1$$

et

$$y^{-1}x^{-1}xy = y^{-1}\ 1\ y = y^{-1}y = 1$$

Donc xy est inversible et $(xy)^{-1} = y^{-1}x^{-1}$.

(a.2) soit $x \in U(A)$, alors $xx^{-1} = 1,\ x^{-1}x = 1$. Donc x^{-1} est inversible et son inverse est x! c.-à-d. $(x^{-1})^{-1} = x$.

8.7.4

On a le groupe symétrique S_3

$$S_3 = \left\{ \binom{123}{123}, \binom{123}{213}, \binom{123}{321}, \binom{123}{132}, \binom{123}{231}, \binom{123}{312} \right\}$$

À voir : Trouver tous les sous-groupes et tous les sous-groupes normaux.
On a S_3 qui est d'ordre 6 (c.-à-d. possède 6 éléments). Par le théorème de Lagrange l'ordre d'un sous-groupe doit être un diviseur de 6, les possibilités sont donc $1, 2, 3, 6$. On note que $\binom{123}{213}, \binom{123}{321}, \binom{123}{132}$ sont des éléments d'ordre 2, donc chacun donne un sous-groupe d'ordre 2. D'autre part $\binom{123}{231}$ et $\binom{123}{312}$ sont des éléments d'ordre 3, mais on a $\binom{123}{231} \circ \binom{123}{231} = \binom{123}{312}$, de sorte qu'on obtient un seul sous-groupe d'ordre 3. Voici donc la liste cherchée :

ordre 1 : $H_1 = \left\{ \binom{123}{123} \right\}$

ordre 2 : $H_2 = \left\{ \binom{123}{123} \binom{123}{213} \right\}$ $H_4 = \left\{ \binom{123}{123} \binom{123}{132} \right\}$

$$H_3 = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix} \begin{pmatrix} 123 \\ 321 \end{pmatrix} \right\}$$

ordre 3 : $H_5 = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\}$

ordre 6 : S_3

Sous-groupes normaux : il y a bien sûr H_1 et S_3.
H_2 n'est pas normal : par exemple

$$\begin{pmatrix} 123 \\ 321 \end{pmatrix}^{-1} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 321 \end{pmatrix} = \begin{pmatrix} 123 \\ 321 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 321 \end{pmatrix} = \begin{pmatrix} 123 \\ 132 \end{pmatrix}$$

et $\begin{pmatrix} 123 \\ 132 \end{pmatrix} \notin H_2$.

H_3 n'est pas normal : par exemple

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix}^{-1} \circ \begin{pmatrix} 123 \\ 321 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} = \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 321 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} = \begin{pmatrix} 123 \\ 132 \end{pmatrix}$$

et $\begin{pmatrix} 123 \\ 132 \end{pmatrix} \notin H_3$.

H_4 n'est pas normal : par exemple

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix}^{-1} \circ \begin{pmatrix} 123 \\ 132 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} = \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 132 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} = \begin{pmatrix} 123 \\ 321 \end{pmatrix}$$

et $\begin{pmatrix} 123 \\ 321 \end{pmatrix} \notin H_4$.

$H_5 = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\}$ est un sous-groupe normal : il suffit de vérifier avec les autres éléments

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix}^{-1} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} = \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} = \begin{pmatrix} 123 \\ 312 \end{pmatrix}$$

$$\begin{pmatrix} 123 \\ 321 \end{pmatrix}^{-1} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 321 \end{pmatrix} = \begin{pmatrix} 123 \\ 321 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 321 \end{pmatrix} = \begin{pmatrix} 123 \\ 312 \end{pmatrix}$$

$$\begin{pmatrix} 123 \\ 132 \end{pmatrix}^{-1} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 132 \end{pmatrix} = \begin{pmatrix} 123 \\ 132 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 132 \end{pmatrix} = \begin{pmatrix} 123 \\ 312 \end{pmatrix}$$

$$\begin{pmatrix}123\\213\end{pmatrix}^{-1}\circ\begin{pmatrix}123\\312\end{pmatrix}\circ\begin{pmatrix}123\\213\end{pmatrix}=\begin{pmatrix}123\\213\end{pmatrix}\circ\begin{pmatrix}123\\312\end{pmatrix}\circ\begin{pmatrix}123\\213\end{pmatrix}=\begin{pmatrix}123\\231\end{pmatrix}$$
$$\begin{pmatrix}123\\321\end{pmatrix}^{-1}\circ\begin{pmatrix}123\\312\end{pmatrix}\circ\begin{pmatrix}123\\321\end{pmatrix}=\begin{pmatrix}123\\321\end{pmatrix}\circ\begin{pmatrix}123\\312\end{pmatrix}\circ\begin{pmatrix}123\\321\end{pmatrix}=\begin{pmatrix}123\\231\end{pmatrix}$$
$$\begin{pmatrix}123\\132\end{pmatrix}^{-1}\circ\begin{pmatrix}123\\312\end{pmatrix}\circ\begin{pmatrix}123\\132\end{pmatrix}=\begin{pmatrix}123\\132\end{pmatrix}\circ\begin{pmatrix}123\\312\end{pmatrix}\circ\begin{pmatrix}123\\132\end{pmatrix}=\begin{pmatrix}123\\231\end{pmatrix}$$

Les sous-groupes normaux sont donc

$$H_1=\left\{\begin{pmatrix}123\\123\end{pmatrix}\right\},\ H_5=\left\{\begin{pmatrix}123\\123\end{pmatrix},\begin{pmatrix}123\\231\end{pmatrix},\begin{pmatrix}123\\312\end{pmatrix}\right\},\ S_3.$$

8.7.6

Les entiers de Gauss $\mathbb{G}=\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$.
On a l'application $N:\mathbb{G}\to\mathbb{N}, N(a+bi)=(a+bi)^2=a^2+b^2$. Du point de vue gómtrique $N(a+bi)=$ carré du module (ou norme) de $a+bi=$ carré de la distance du point $a+bi$ à l'origine dans le plan complexe.

1) $\underline{\mathbb{Z}[i] \text{ est un sous-anneau de } \mathbb{C}}$: notons que $\mathbb{Z}\subseteq\mathbb{Z}[i]$.
$x,y\in\mathbb{Z}[i]$ entraîne $x+y\in\mathbb{Z}[i]$ et $x-y\in\mathbb{Z}[i]$: disons $x=a+ib, y=c+id,\ a,b,c,d\in\mathbb{Z}$, alors $x+y=a+c+i(b+d), x-y=a-c+i(b-d)$ et $a+c,\ b+d,\ a-c,\ b-d\in\mathbb{Z}$ d'où$x+y,\ x-y\in\mathbb{Z}[i]$.
$x,y\in\mathbb{Z}[i]$ entraîne $xy\in\mathbb{Z}[i]$: disons $x=a+ib,\ y=c+id,\ a,b,c,d\in\mathbb{Z}$, alors $xy=ac-bd+i(ad+bc)$ et $ac-bd, ad+bc\in\mathbb{Z}$ d'où $xy\in\mathbb{Z}[i]$. Cela montre que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
2) $\underline{\forall x,y\in\mathbb{G}, N(xy)=N(x)N(y)}$
Notons que c'est une propriété du module : $\forall x,y\in\mathbb{C}, |xy|=|x||y|$. Ainsi

$$\begin{aligned}N(xy) &= |xy|^2=|xy||xy|=|x||y||x||y|\\ &= |x|^2|y|^2\\ &= N(x)N(y).\end{aligned}$$

N.B. C'est donc une propriété qui n'est pas particulière à$\mathbb{Z}[i]$.
De faǫn plus explicite on vérifie l'identité suivante pour tous $a,b,c,d\in\mathbb{R}$:

$$(ac-bd)^2+(ad+bc)^2=(a^2+b^2)(c^2+d^2)$$

de sorte que pour $x=aib,\ y=c+id$, on a bien

$$N(xy)=N(x)N(y)$$

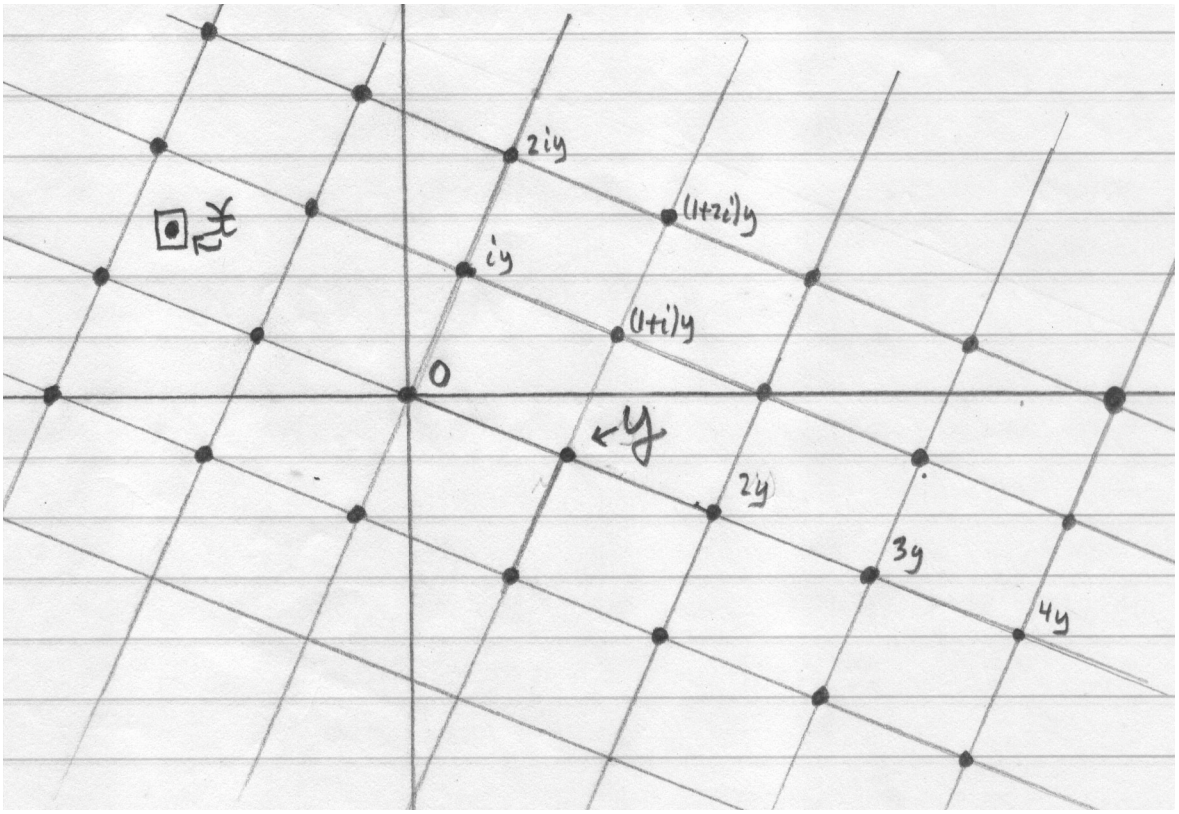
puisque $xy=(ac-bd)+i(ad+bc)$.

3) $\forall x, y \in \mathbb{G}, y \neq 0, \exists q, r \in \mathbb{G}$ tel que $x = qy + r$ et $N(r) < N(y)$

On trouve un argument purement algébrique dans Kostrikin, p. 400. On peut aussi faire l'argument géométriq
dans le plan complexe. Soit $x, y \in \mathbb{G}, y \neq 0$, fixés. Reformulons la question de la faqn suivante : on cherche un « multiple »qy de y tel que $N(x - qy) < N(y)$, donc dont la distance à x est plus petite que le module de y.

Dans le plan complexe l'ensemble $\{qy : q \in \mathbb{Z}[i]\}$ est formé des sommets du réseau orthogonal déterminé par le vecteur $\overrightarrow{0y}$.

Ce réseau forme un quadrillage du plan complexe par des carrés adjacents de côté égal à $|y|$.



Notons

(3.1) tout carré du quadrillage s'obtient par translation du carré « fondamental »D dont les sommets sont $0, y, iy, (1 + i)y$

(3.2) tout point sur le carré D ou à l'intérieur de D est àdistance plus petite que $|y|$ d'un des sommets : en effet D est un carré de côté égal à $|y|$.

Par (3.1) et (3.2), tout carré du quadrillage possède la propriété (3.2). Puisque x appartient à l'un des carrés du quadrillage, il s'ensuit que x est à distance plus petite que $|y|$ d'au moins un sommet

du réseau, ou autrement dit, x est à distance plus petite que $|y|$ d'au moins un « multiple »de y. C'est bien ce qu'on voulait.

8.7.7

On a K un corps fini de caractéristique p et ξ un générateur de K^*.
À voir : ξ^p est aussi un générateur de K^*.
On a que $\varphi_p : K \to K$, défini par $\varphi_p(x) = x^p$ est un automorphisme de corps de K.
En particulier, il induit un automorphisme du groupe multiplicatif $\varphi_p : K^* \to K^*$ qui enverra le générateur ξ sur un autre générateur $\varphi_p(\xi) = \xi^p$.
(Un automorphisme d'un groupe préserve l'ordre des éléments : $\varphi(x^n) = \varphi(x)^n = 1$ ssi $x^n = 1$)

Bibliographie

[1] J. Calais, *Eléments de théorie des groupes*, Presses Universitaires de France, 1984. (QA174.2C25)

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker et R. A. Wilson, *Atlas of finite groups*, Clarendon Press Oxford, 1985. (QA171A86)

[3] P. Damphousse, *L'arithmétique ou l'art de compter*, Quatre à quatre, Édition le Pommier, 2002.

[4] D. Guin, *Algèbre, Tome 1 : Groupes et anneaux*, Belin, 1997.

[5] A. Kostrikin, *Introduction à l'algèbre*, Éditions MIR, 1986. (QA154.2K6714)

[6] J. Labelle et C. Reutenauer, *MAT1000 : Algèbre 1.* Notes de cours, UQAM.

[7] S. Lang, *Structures algébriques*, InterEditions, 1976. (QA 251 L 2514)

[8] F. Liret et D. Martinais, *Algèbre 1re année, 2e édition*, Dunod, 2003. (QA155L47.2003)

[9] G. Polya, *Comment poser et résoudre un problème.* Dunod, 1962. (QA11P614)

[10] R. Smullyan, *Le livre qui rend fou*, Dunod, 1997.

N.B. Les expressions entre parenthèses indiquent la cote des livres disponibles dans les bibliothèques de l'UQAM (QA : sciences).