

Algèbre 1

Cécile Armana

Licence de mathématiques L3
Université de Franche-Comté
2018-2019

Table des matières

Présentation de l'unité	iii
I Le cours	1
1 Permutations d'un ensemble	3
Introduction	3
1.1 Permutations et groupe symétrique	3
1.2 Cycles et décomposition en cycles	6
1.3 Signature d'une permutation	11
2 Généralités sur les groupes	17
Introduction	17
2.1 Définitions et premières propriétés	17
2.2 Morphismes de groupes	21
2.3 Sous-groupes	25
2.4 Sous-groupe engendré par une partie	28
2.5 Produit direct	30
3 Ordre d'un élément, classes modulo un sous-groupe	35
Introduction	35
3.1 Ordre d'un élément	35
3.2 Le groupe additif $\mathbb{Z}/n\mathbb{Z}$	38
3.3 Classification des groupes monogènes et des groupes cycliques . .	41
3.4 Classes à gauche et à droite modulo un sous-groupe	43
4 Groupes quotients, théorème d'isomorphisme	47
Introduction	47
4.1 Sous-groupes normaux	47
4.2 Groupe quotient, théorème d'isomorphisme	50
4.3 Sous-groupes d'un groupe quotient	54
4.4 Produit semi-direct	55
4.5 Groupe diédral	58

5	Actions de groupes, théorèmes de Sylow	61
	Introduction	61
5.1	Action d'un groupe sur un ensemble	61
5.2	Stabilisateurs, orbites, équation des classes	64
5.3	p -groupes et théorèmes de Sylow	69
6	Arithmétique dans \mathbb{Z}	75
	Introduction	75
6.1	L'anneau \mathbb{Z} et son arithmétique	75
6.2	L'anneau $\mathbb{Z}/n\mathbb{Z}$ et son arithmétique	85
6.3	Constructions de \mathbb{N} et de \mathbb{Z}	93
	Annexe 1 : relation d'équivalence, ensemble quotient	99
	Annexe 2 : synthèse des groupes rencontrés	103
II	Les exercices	105
	Exercices du chapitre 1	107
	Exercices du chapitre 2	111
	Exercices du chapitre 3	115
	Exercices du chapitre 4	119
	Exercices du chapitre 5	123
	Exercices du chapitre 6	127
III	Les corrigés des exercices	131
	Corrigé des exercices du chapitre 1	133
	Corrigé des exercices du chapitre 2	141
	Corrigé des exercices du chapitre 3	151
	Corrigé des exercices du chapitre 4	159
	Corrigé des exercices du chapitre 5	169
	Corrigé des exercices du chapitre 6	177

Présentation de l'unité

L'unité *Algèbre 1* vise à :

- d'une part acquérir des connaissances de base et avancées sur les *groupes*, qui sont des structures algébriques fondamentales ;
- d'autre part étudier l'*arithmétique* des entiers, dans laquelle intervient la théorie des groupes, et qui fournit aussi les premiers exemples d'anneaux que sont \mathbb{Z} et $\mathbb{Z}/n\mathbb{Z}$.

L'étude des anneaux sera développée et approfondie au semestre 6 avec l'unité *Algèbre 2*.

Prérequis

Nous supposerons acquis les notions et résultats usuels de théorie des ensembles, ainsi que l'arithmétique élémentaire. Pour cette dernière, une partie du chapitre 6 peut tenir lieu de rappels et être lue indépendamment des chapitres précédents. Afin de mieux comprendre les enjeux de cette unité et de la replacer dans un contexte mathématique plus général, le cours sera régulièrement illustré d'exemples et exercices faisant appel à vos connaissances antérieures d'algèbre linéaire et bilinéaire.

Le cours

Le contenu du cours s'organise selon le plan suivant :

Chapitre 1 : Permutations d'un ensemble ;

Chapitre 2 : Généralités sur les groupes ;

Chapitre 3 : Ordre d'un élément, classes modulo un sous-groupe ;

Chapitre 4 : Groupes quotients, théorème d'isomorphisme ;

Chapitre 5 : Actions de groupes, théorèmes de Sylow ;

Chapitre 6 : Arithmétique dans \mathbb{Z} .

Les chapitres 1 à 5 portent sur la théorie des groupes. Le chapitre 6 est consacré à l'arithmétique des entiers. Il n'est pas tout à fait indépendant des précédents : on y démontre certains résultats sur les groupes ou qui utilisent la théorie des groupes. Inversement, les cinq premiers chapitres peuvent faire appel à des résultats d'arithmétique élémentaire qui sont supposés connus (en cas de besoin, des rappels sont donnés dans le chapitre 6).

Le cours est suivi de deux annexes :

- la première, page 99, reprend, sans démonstration, des prérequis sur les relations d'équivalences et leurs ensembles quotients, indispensables pour aborder cette unité ;
- la seconde, page 103, présente une synthèse des principaux groupes et procédés de construction de groupes rencontrés dans le cours.

Les exercices

Les différents types d'exercices sont identifiés par la nomenclature suivante qui concerne la priorité d'apprentissage (et non nécessairement la difficulté) :

-  exercice fondamental
-  exercice important
-  exercice d'approfondissement.

Au fil de chaque chapitre seront indiqués les exercices qui peuvent être traités.

Il est conseillé de travailler prioritairement tous les exercices signalés comme fondamentaux, d'application directe du cours, ou importants. Les exercices d'approfondissement sont aussi à étudier : ils ne sont pas toujours plus difficiles que les autres et permettent de consolider vos connaissances en vue de l'examen.

Une bibliographie

Une liste d'ouvrages couvrant les thèmes de l'unité est donnée ci-dessous. Il n'est pas indispensable de les consulter mais ils peuvent apporter à ce cours, compléments, précisions, et exercices d'entraînement supplémentaires.

- Josette Calais, *Éléments de théorie des groupes*, Presses Universitaires de France, 1998
- Jean Delcourt, *Théorie des groupes*, Eyrolles, 2007
- Jean-Pierre Escofier, *Toute l'algèbre de la licence*, Dunod, 2011.

Première partie

Algèbre 1
Le cours

Chapitre 1

Permutations d'un ensemble

Introduction

Nous commençons ce cours par l'étude d'un groupe particulier : le groupe symétrique c'est-à-dire le groupe des permutations d'un ensemble. Il joue un rôle important pour des raisons historiques (c'est par son étude que la notion de groupe abstrait a commencé à apparaître, notamment via les travaux de Galois) et mathématiques (le théorème de Cayley, qui sera démontré au chapitre 2, affirme que tout groupe peut se voir comme sous-groupe d'un groupe symétrique).

Vous avez déjà rencontré le groupe symétrique à travers la notion de déterminant d'une matrice en algèbre linéaire. Comme il se manipule de manière concrète, c'est un exemple de groupe qui vous sera utile pour appréhender les concepts fondamentaux des chapitres suivants.

1.1 Permutations et groupe symétrique

Soit E un ensemble non vide.

Définition 1.1

Une *permutation de E* est une bijection de E dans E . L'ensemble des permutations de E est noté \mathcal{S}_E , ou encore \mathfrak{S}_E , et appelé le *groupe symétrique de E* .

Un cas particulier important est celui où E est un ensemble fini. S'il est de cardinal n , alors quitte à numéroter ses éléments on peut supposer que $E = \{1, \dots, n\}$ et on note son groupe symétrique \mathcal{S}_n . Les éléments du groupe symétrique, c'est-à-dire les permutations de E , sont souvent désignés par la lettre grecque σ (sigma).

Proposition 1.2

Le cardinal de \mathcal{S}_n est $n!$.

Démonstration. Une permutation σ de $\{1, \dots, n\}$ est déterminée par le n -uplet de ses valeurs $(\sigma(1), \dots, \sigma(n))$, qui doivent être deux à deux distinctes dans $\{1, \dots, n\}$

par injectivité de σ . De plus, à tout n -uplet (a_1, \dots, a_n) avec $a_i \in \{1, \dots, n\}$ et les a_i deux à deux distincts, on associe l'application $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ donnée par $\sigma(i) = a_i$; l'application σ est alors injective par construction, et bijective car c'est une application injective entre deux ensembles à n éléments; donc σ est une permutation.

Dénombrer \mathcal{S}_n revient donc à dénombrer les n -uplets (a_1, \dots, a_n) avec $a_i \in \{1, \dots, n\}$ et les a_i deux à deux distincts. Pour a_1 , il y a n choix possibles dans $\{1, \dots, n\}$. Le choix de a_1 étant effectué, il y a ensuite $n - 1$ choix possibles pour a_2 car $a_2 \neq a_1$. De même il y a ensuite $n - 2$ choix possibles pour a_3 , puisque $a_3 \neq a_1$ et $a_3 \neq a_2$. On procède ainsi par récurrence sur n : le nombre de choix possibles pour le n -uplet (a_1, \dots, a_n) est $n(n - 1) \cdots 1 = n!$. \square

Pour bien se rendre compte du nombre d'éléments du groupe symétrique \mathcal{S}_n , rappelons les premières valeurs prises par la factorielle¹ :

n	1	2	3	4	5	6	7	8	9	10
$n!$	1	2	6	24	120	720	5040	40320	362880	3628800

On représente de manière conventionnelle la permutation σ sous forme d'un tableau à deux lignes comme suit :

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

Exemple 1.3. Les deux éléments de \mathcal{S}_2 sont :

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

et les six éléments de \mathcal{S}_3 sont :

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$t_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, t_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, t_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Composer deux permutations d'un même ensemble E donne à nouveau une permutation de E . La composition, notée \circ et qui se lit « rond », est donc une loi interne sur l'ensemble \mathcal{S}_E .

Exemple 1.4. Dans \mathcal{S}_3 , on a

$$(s_1 \circ t_3)(1) = s_1(t_3(1)) = s_1(2) = 3,$$

$$(s_1 \circ t_3)(2) = s_1(t_3(2)) = s_1(1) = 2,$$

$$(s_1 \circ t_3)(3) = s_1(t_3(3)) = s_1(3) = 1$$

1. On rappelle que $n!$ se lit « factorielle n ».

donc $s_1 \circ t_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = t_2$. Un calcul similaire donne $t_3 \circ s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = t_1$.

On remarque que $s_1 \circ t_3 \neq t_3 \circ s_1$ donc la loi \circ n'est pas commutative dans \mathcal{S}_3 .

Plus généralement, elle n'est pas commutative dans \mathcal{S}_n dès que $n \geq 3$ (cela se démontre par un calcul similaire faisant intervenir les permutations s et t de \mathcal{S}_n obtenues en prolongeant respectivement s_1 et t_3 par $s(i) = i$ et $t(i) = i$ pour tout $i > 3$).

Définition 1.5

La permutation id_E , définie par $\text{id}_E(x) = x$ pour tout $x \in E$, est appelée la *permutation identité* de E . Si $E = \{1, \dots, n\}$, on la note id_n , ou id s'il n'y a pas de confusion possible.

Proposition 1.6

1. (Associativité de \circ) Pour tous $\sigma_1, \sigma_2, \sigma_3$ dans \mathcal{S}_E , on a

$$\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3.$$

2. (id_E est l'élément neutre de \circ) Pour tout $\sigma \in \mathcal{S}_E$ on a

$$\text{id}_E \circ \sigma = \sigma = \sigma \circ \text{id}_E.$$

3. (Existence d'un inverse à tout élément de \mathcal{S}_E) Pour tout $\sigma \in \mathcal{S}_E$ il existe une unique permutation $\rho \in \mathcal{S}_E$ telle que

$$\sigma \circ \rho = \text{id}_E = \rho \circ \sigma.$$

Cet inverse ρ est noté σ^{-1} .

Démonstration. 1. La composition des applications est toujours associative.

2. C'est une vérification immédiate.

3. La permutation ρ n'est autre que la bijection réciproque σ^{-1} de σ . □

Au chapitre suivant, nous verrons la notion de groupe en toute généralité et la proposition 1.6 traduira le fait que l'ensemble \mathcal{S}_E muni de la loi de composition est un groupe.

Définition 1.7

Soit $\sigma \in \mathcal{S}_E$. Un élément $x \in E$ est dit *fixe* par σ lorsque $\sigma(x) = x$. On parle aussi de *point fixe* de σ . Le *support* de σ est l'ensemble des $x \in E$ tels que $\sigma(x) \neq x$. On le note $\text{supp}(\sigma)$.

Le support est donc l'ensemble des éléments non fixes par σ .

Exemple 1.8. La permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ dans \mathcal{S}_4 a pour points fixes 2 et 4. Son support est $\{1, 3\}$.

Voici une situation importante où deux permutations sont autorisées à commuter.

Proposition 1.9

Pour toutes permutations σ, σ' à supports disjoints (c'est-à-dire satisfaisant $\text{supp}(\sigma) \cap \text{supp}(\sigma') = \emptyset$) on a $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Démonstration. Voir l'exercice 1.4. □

☞ *Exercices pouvant être traités :*

- exercice 1.4  
- exercice 1.6  
- exercice 1.9 (sauf la question 3)   

1.2 Cycles et décomposition en cycles

Pour alléger les notations, on écrit dorénavant $\sigma_1\sigma_2$ au lieu de $\sigma_1 \circ \sigma_2$ lorsque σ_1 et σ_2 sont deux permutations de E , et on parlera de *produit* au lieu de composition. Comme vu auparavant, il faut prendre garde à ce que σ_1 et σ_2 ne commutent pas en général pour cette loi.

Définition 1.10

Si $\ell \in \mathbb{N}, \ell \geq 1$, on note σ^ℓ la permutation $\underbrace{\sigma \circ \dots \circ \sigma}_{\ell \text{ fois}}$. On pose $\sigma^0 = \text{id}_E$.
Si $\ell \in \mathbb{Z}, \ell < 0$, on note σ^ℓ la permutation $(\sigma^{-1})^{-\ell}$.

On peut alors montrer qu'on a les règles de calcul, valables pour tous k et ℓ dans \mathbb{Z} :

$$\sigma^k \sigma^\ell = \sigma^{k+\ell} = \sigma^\ell \sigma^k \quad \text{et} \quad (\sigma^k)^\ell = \sigma^{k\ell} = (\sigma^\ell)^k.$$

Jusqu'à la fin de ce chapitre, nous supposons que $E = \{1, \dots, n\}$ et nous intéressons au groupe symétrique \mathcal{S}_n .

1.2.1 Cycles

Nous introduisons les permutations qui permutent de manière cyclique un certain nombre d'éléments : elles jouent un rôle particulier dans l'étude de \mathcal{S}_n .

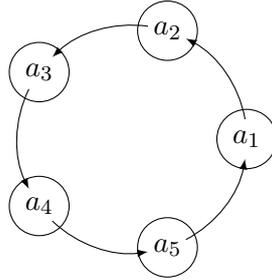
Définition 1.11

Soit k un entier supérieur ou égal à 2. Une permutation $\sigma \in \mathcal{S}_n$ est appelée un *cycle de longueur k* s'il existe k éléments deux à deux distincts a_1, \dots, a_k dans $\{1, \dots, n\}$ tels que $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$ et si tout élément de $\{1, \dots, n\}$ distinct de a_1, \dots, a_k est fixe par σ .

On dira aussi *k-cycle* pour un cycle de longueur k . Noter que l'entier k est nécessairement inférieur ou égal à n .

On note (a_1, a_2, \dots, a_k) le k -cycle de la définition 1.11, les points fixes étant omis de l'écriture. Cette notation a le mérite d'être plus compacte que celle comme tableau à deux lignes mais elle existe *uniquement pour les cycles*. Le support du k -cycle (a_1, \dots, a_k) est $\{a_1, \dots, a_k\}$.

Voici une représentation graphique d'un 5-cycle $(a_1, a_2, a_3, a_4, a_5)$:



On constate que si σ est un k -cycle dans \mathcal{S}_n alors $\sigma^k = \text{id}_n$ et pour tout $i \in \{1, \dots, k-1\}$ on a $\sigma^i \neq \text{id}_n$. Dans le langage du chapitre 3, nous dirons qu'un k -cycle est d'ordre k .

Définition 1.12

| Une *transposition* est un 2-cycle dans \mathcal{S}_n .

Exemple 1.13. Dans l'exemple 1.3 de \mathcal{S}_3 , on peut écrire :

$$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3), \quad s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2),$$

$$t_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3), \quad t_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1, 3), \quad t_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2).$$

Les permutations t_1, t_2, t_3 sont des transpositions et s_1, s_2 sont des 3-cycles.

De manière générale lorsque $n \geq 4$, *il existe des permutations dans \mathcal{S}_n qui ne sont pas des cycles* : par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ dans \mathcal{S}_4 . Néanmoins un résultat important du chapitre sera qu'une permutation quelconque se décompose en produit de cycles.

Remarque 1.14. Attention : *l'écriture en ligne d'un cycle n'est pas unique*. Un même cycle peut s'écrire des k façons différentes qui suivent :

$$(a_1, a_2, \dots, a_{k-1}, a_k) = (a_2, \dots, a_{k-1}, a_k, a_1) = \dots = (a_k, a_1, a_2, \dots, a_{k-1}).$$

Par exemple le 5-cycle $(4, 3, 5, 1, 2)$ peut s'écrire :

$$(4, 3, 5, 1, 2) = (3, 5, 1, 2, 4) = (5, 1, 2, 4, 3) \\ = (1, 2, 4, 3, 5) = (2, 4, 3, 5, 1).$$

Noter que ce cycle n'est pas le même que $(1, 2, 3, 4, 5)$, par exemple.

L'énoncé qui suit présente le comportement des cycles vis-à-vis de la conjugaison, une opération que nous retrouverons dans l'étude générale des groupes.

Proposition 1.15

1. Si $\sigma \in \mathcal{S}_n$ et si (a_1, \dots, a_k) est un k -cycle alors $\sigma(a_1, \dots, a_k)\sigma^{-1}$ est le k -cycle $(\sigma(a_1), \dots, \sigma(a_k))$.
2. Si c_1 et c_2 sont deux cycles dans \mathcal{S}_n de même longueur, il existe $\sigma \in \mathcal{S}_n$ tel que $c_2 = \sigma c_1 \sigma^{-1}$ (on dit que c_1 et c_2 sont *conjugués* dans \mathcal{S}_n).

Démonstration. Voir l'exercice 1.8. □

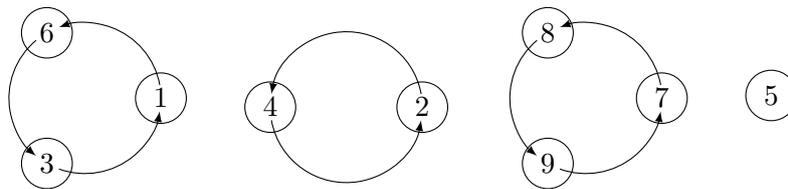
1.2.2 Décomposition en cycles

Exemple 1.16. Avant d'étudier le principe général, voyons comment décomposer une permutation donnée en produit de cycles à supports deux à deux disjoints.

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix} \in \mathcal{S}_9$. Comme $\sigma(1) = 6$, la permutation commence par le cycle $(1, 6, \dots)$. Comme $\sigma(6) = 3$, elle continue en $(1, 6, 3, \dots)$. Enfin $\sigma(3) = 1$, qui était la première valeur du cycle donc la parenthèse est fermée et σ contient le cycle $(1, 6, 3)$ dans sa décomposition. Le plus petit entier qui n'est pas intervenu dans cette discussion est 2 : par le même procédé, on écrit $(1, 6, 3)(2, \dots)$ puis $(1, 6, 3)(2, 4)$ car $\sigma(2) = 4$ et $\sigma(4) = 2$. Le plus petit entier qui n'est pas intervenu étant 5, on regarde $\sigma(5)$. Comme $\sigma(5) = 5$, 5 est un point fixe : il ne donne lieu à aucun cycle. On termine en regardant de même $\sigma(7)$, $\sigma(\sigma(7))$, etc. L'ensemble $\{1, \dots, 9\}$ ayant été épuisé, on obtient

$$\sigma = (1, 6, 3)(2, 4)(7, 8, 9).$$

On peut représenter graphiquement cette décomposition comme suit :



Si nous avons commencé la procédure en regardant, par exemple, l'image de 2 au lieu de celle de 1, la décomposition obtenue aurait eu les mêmes cycles mais dans un ordre différent (nous conseillons aux lecteurs d'écrire cette décomposition). Le théorème 1.21 généralisera ces observations.

Exemple 1.17. Considérons une permutation donnée par un produit de cycles non nécessairement à supports disjoints. On peut utiliser la procédure précédente pour la décomposer en produit de cycles à supports deux à deux disjoints, en prenant garde au sens de calcul de la composée, qui s'effectue « de droite

à gauche » : $(\sigma_1\sigma_2\sigma_3)(x) = \sigma_1(\sigma_2(\sigma_3(x)))$. Par exemple, pour décomposer la permutation $(1, 3, 2)(1, 3)(1, 4)$ dans \mathcal{S}_4 , on écrit :

$$\begin{array}{c} \boxed{1} \xrightarrow{(1,4)} 4 \xrightarrow{(1,3)} 4 \xrightarrow{(1,3,2)} \boxed{4}, \\ \boxed{4} \xrightarrow{(1,4)} 1 \xrightarrow{(1,3)} 3 \xrightarrow{(1,3,2)} \boxed{2}, \\ \boxed{2} \xrightarrow{(1,4)} 2 \xrightarrow{(1,3)} 2 \xrightarrow{(1,3,2)} \boxed{1}, \\ 3 \xrightarrow{(1,4)} 3 \xrightarrow{(1,3)} 1 \xrightarrow{(1,3,2)} 3. \end{array}$$

Donc

$$(1, 3, 2)(1, 3)(1, 4) = (1, 4, 2).$$

Le procédé vu dans l'exemple 1.16 nous amène à introduire la relation suivante.

Définition 1.18

Soient x et y dans $\{1, \dots, n\}$. On dit que x est σ -équivalent à y lorsqu'il existe $m \in \mathbb{Z}$ tel que $x = \sigma^m(y)$.

La σ -équivalence est une relation réflexive, symétrique, et transitive : en effet, $x = \sigma^0(x)$, puis $x = \sigma^m(y)$ implique $y = \sigma^{-m}(x)$, et enfin $x = \sigma^m(y)$ avec $y = \sigma^k(z)$ entraîne $x = \sigma^{m+k}(z)$. C'est donc une relation d'équivalence sur l'ensemble $\{1, \dots, n\}$ (voir l'annexe page 99 pour des rappels).

Définition 1.19

Une classe d'équivalence pour la relation de σ -équivalence est appelée une σ -orbite.

Exemple 1.20. Dans l'exemple 1.16, la σ -orbite de 1 est $\{1, 3, 6\}$ et la σ -orbite de 5 est $\{5\}$.

Théorème 1.21

Toute permutation de \mathcal{S}_n distincte de id_n est un produit de cycles à supports deux à deux disjoints. De plus cette écriture est unique à l'ordre près des cycles.

Cette décomposition ne peut pas être unique au sens strict puisqu'on sait que deux permutations à supports disjoints commutent (proposition 1.9).

Démonstration. Suivons le principe de l'exemple 1.16. Comme toute relation d'équivalence, l'ensemble $\{1, \dots, n\}$ admet une partition en classes d'équivalence c'est-à-dire en σ -orbites, notées C_1, \dots, C_r :

$$\{1, \dots, n\} = C_1 \sqcup \dots \sqcup C_r.$$

Considérons une telle σ -orbite C . Elle est :

— soit ponctuelle c'est-à-dire $C = \{x\}$, auquel cas x est un point fixe de σ ;

- soit de cardinal au moins égal à 2, auquel cas on peut lui associer un cycle de support C par le procédé suivant. Par définition, il existe $x \in C$ tel que $C = \{\sigma^m(x) \mid m \in \mathbb{Z}\}$. L'ensemble C étant fini, il existe $m > k$ dans \mathbb{Z} satisfaisant $\sigma^m(x) = \sigma^k(x)$ d'où $\sigma^{m-k}(x) = x$. Soit donc ℓ le plus petit entier strictement positif tel que $\sigma^\ell(x) = x$. De plus ℓ est supérieur ou égal à 2 : sinon x serait un point fixe, donc l'orbite serait ponctuelle, ce qui est exclu. On a alors $C = \{x, \sigma(x), \dots, \sigma^{\ell-1}(x)\}$. Posons $c = (x, \sigma(x), \dots, \sigma^{\ell-1}(x))$: c'est un ℓ -cycle de support C qui satisfait $c|_C = \sigma|_C$.

Pour reprendre l'exemple 1.17 : si C est la σ -orbite $\{1, 3, 6\}$ alors posons par exemple $x = 6$ dans C ; on a $\sigma(x) = 3, \sigma^2(x) = 1, \sigma^3(x) = 6 = x$ donc $\ell = 3$ et le cycle construit à partir de C est $c = (6, 3, 1) = (1, 6, 3)$.

Notons c_1, \dots, c_s les cycles ainsi associés aux σ -orbites non ponctuelles (il en existe au moins un car $\sigma \neq \text{id}_n$). Par construction, leurs supports sont deux à deux disjoints. Enfin en comparant $\sigma(y)$ et $(c_1 \cdots c_s)(y)$ pour tout $y \in \{1, \dots, n\}$, on voit que $\sigma = c_1 \cdots c_s$.

Pour l'unicité de l'écriture à l'ordre près : supposons avoir :

$$\sigma = c_1 \cdots c_s = d_1 \cdots d_t$$

où les c_i (resp. d_i) sont des cycles à supports deux à deux disjoints. Notons C_i (resp. D_i) le support de c_i (resp. d_i). Soit x appartenant à D_i . Comme les supports sont disjoints deux à deux, parmi les d_1, \dots, d_t seul le cycle d_i ne fixe pas x . On a donc $\sigma(x) = d_i(x)$ d'où, pour tout $k \in \mathbb{Z}$, $\sigma^k(x) = d_i^k(x)$. Ainsi D_i est une σ -orbite non ponctuelle, celle de x , et $d_i = \sigma|_{D_i}$. Un argument similaire montre que C_i est aussi une σ -orbite non ponctuelle. Or la partition en σ -orbites est unique. Comme C_i et D_i sont non ponctuelles, on a donc $D_i = C_i$, quitte à renuméroter les orbites. On en déduit $d_i|_{D_i} = \sigma|_{D_i} = \sigma|_{C_i} = c_i|_{C_i}$. Un cycle étant déterminé par sa restriction à son support, on conclut que $d_i = c_i$. Ceci étant valable pour tout i , on a aussi $s = t$. \square

Corollaire 1.22

Supposons $n \geq 2$. Toute permutation de \mathcal{S}_n est un produit de transpositions. Dans cette écriture, on peut se restreindre aux transpositions de la forme $(1, i)$ avec $2 \leq i \leq n$, ou encore de la forme $(i, i+1)$ avec $1 \leq i \leq n-1$.

Démonstration. La permutation identité est produit de transpositions car comme $n \geq 2$ elle s'écrit $\text{id}_n = (1, 2)(1, 2)$.

D'après le théorème 1.21, toute permutation distincte de id_n est un produit de cycles. Il reste à montrer que tout cycle est un produit de transpositions. Or si $k \geq 2$ on a :

$$\begin{aligned} (a_1, \dots, a_k) &= (a_1, a_k)(a_1, \dots, a_{k-1}) \\ &= (a_1, a_k)(a_1, a_{k-1})(a_1, \dots, a_{k-2}) \\ &= \dots \\ &= (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2). \end{aligned}$$

Cela prouve la première assertion du corollaire. Pour se restreindre aux transpositions de la forme $(1, i)$, il suffit de constater que $(i, j) = (1, j)(1, i)(1, j)$. Enfin on a $(1, i) = (i-1, i)(1, i-1)(i-1, i)$, puis une récurrence sur $i \geq 2$ montre que toute transposition de la forme $(1, k)$ s'écrit comme produit de transpositions de la forme $(i, i+1)$. \square

- Remarque 1.23.**
1. L'énoncé du corollaire est encore vrai pour $n = 1$: dans ce cas le produit est vide et désigne par convention l'identité.
 2. L'énoncé ne contient aucune assertion sur les supports, contrairement au théorème 1.21. En particulier, ces transpositions ne commutent généralement pas entre elles.
 3. Il peut être utile de connaître, ou de savoir retrouver, les formules suivantes vues dans la démonstration du corollaire :

$$(a_1, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2)$$

$$(i, j) = (1, j)(1, i)(1, j).$$

4. Contrairement à celle en produit de cycles, la décomposition en produit de transpositions n'est pas unique, même à l'ordre près. En décomposant en cycles à supports deux à deux disjoints puis en utilisant la preuve du corollaire 1.22, on obtient pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 6 & 4 \end{pmatrix}$, les décompositions suivantes :

$$\begin{aligned} \sigma &= (2, 3)(4, 5, 6) = (2, 3)(4, 6)(4, 5) \\ &= (1, 3)(1, 2)(1, 3)(1, 6)(1, 4)(1, 6)(1, 5)(1, 4)(1, 5). \end{aligned}$$

Noter que le nombre de facteurs dans les deux décompositions en transpositions est respectivement 3 et 9, qui sont distincts mais tous deux impairs. Nous démontrerons de manière générale que la parité du nombre de transpositions dans une décomposition de σ ne dépend que de σ . La notion de signature expliquera ce fait.

 *Exercices pouvant être traités :*

- exercice 1.1 (sauf la question 1c) 
- exercice 1.2 (sauf ce qui concerne la signature et le groupe alterné) 
- exercice 1.3  
- exercice 1.8   

1.3 Signature d'une permutation

Définition 1.24

Soit $\sigma \in \mathcal{S}_n$. Une *inversion* de σ est un couple (i, j) avec i et j dans $\{1, \dots, n\}$ vérifiant $i < j$ et $\sigma(i) > \sigma(j)$. Le nombre d'inversions de σ est noté $I(\sigma)$. La *signature* de σ est le nombre $\varepsilon(\sigma) = (-1)^{I(\sigma)}$ c'est-à-dire la

parité du nombre d'inversions. Si $\varepsilon(\sigma)$ vaut 1 (resp. -1), on dit que σ est une permutation *paire* (resp. *impaire*).

On définit ainsi l'application signature $\varepsilon : \mathcal{S}_n \rightarrow \{\pm 1\}$ (c'est la lettre grecque epsilon). Elle dépend de n , mais on ne fait pas apparaître cette dépendance dans la notation ε . Rappelons que la signature intervient en algèbre linéaire dans la définition du déterminant d'une matrice (voir aussi l'exercice 1.9 à ce sujet).

Exemple 1.25. $\varepsilon(\text{id}_n) = 1$; $\varepsilon\left(\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right) = -1$; $\varepsilon\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\right) = (-1)^3 = -1$ car il y a trois inversions $((1, 4), (2, 4)$ et $(3, 4))$; $\varepsilon\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\right) = (-1)^2 = 1$ car il y a deux inversions $((1, 2)$ et $(3, 4))$.

Calculer la signature à partir du nombre d'inversions s'avère fastidieux dès que n est un peu grand (donnez-vous une permutation quelconque de \mathcal{S}_9 et essayez de calculer sa signature ainsi...).

Nous allons voir une méthode de calcul beaucoup plus aisée qui repose sur des propriétés fondamentales de la signature.

Lemme 1.26

On a

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Démonstration. Par bijectivité de σ , le numérateur $\prod_{1 \leq i < j \leq n} (\sigma(i) - \sigma(j))$ et le dénominateur $\prod_{1 \leq i < j \leq n} (i - j)$ sont non nuls, et égaux au signe près. De plus le signe du produit :

$$\prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

est donné par la parité de $I(\sigma)$ c'est-à-dire $(-1)^{I(\sigma)}$. □

Au chapitre 2 on résumera la propriété suivante en disant que la signature est un morphisme de groupes.

Théorème 1.27

Pour tous σ_1 et σ_2 dans \mathcal{S}_n , on a $\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$.

Démonstration. On écrit, en utilisant le lemme précédent et la bijectivité de σ_2 ,

$$\begin{aligned}\varepsilon(\sigma_1\sigma_2) &= \prod_{1 \leq i < j \leq n} \frac{\sigma_1(\sigma_2(i)) - \sigma_1(\sigma_2(j))}{i - j} \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma_1(\sigma_2(i)) - \sigma_1(\sigma_2(j))}{\sigma_2(i) - \sigma_2(j)} \prod_{1 \leq i < j \leq n} \frac{\sigma_2(i) - \sigma_2(j)}{i - j} \\ &= \prod_{1 \leq x < y \leq n} \frac{\sigma_1(x) - \sigma_1(y)}{x - y} \prod_{1 \leq i < j \leq n} \frac{\sigma_2(i) - \sigma_2(j)}{i - j} = \varepsilon(\sigma_1)\varepsilon(\sigma_2)\end{aligned}$$

On a posé $(x, y) = (\sigma_2(i), \sigma_2(j))$ si $\sigma_2(i) \leq \sigma_2(j)$, et $(x, y) = (\sigma_2(j), \sigma_2(i))$ sinon. On peut montrer que $(i, j) \mapsto (x, y)$ est une bijection de $\{1, \dots, n\}^2$ dans lui-même, ce qui permet de faire un changement d'indices dans le produit comme ci-dessus. \square

Corollaire 1.28

1. La signature d'une transposition est -1 .
2. La signature d'un cycle de longueur k est $(-1)^{k-1}$.
3. Soit $\sigma \in \mathcal{S}_n$. Si r est le nombre de σ -orbites alors $\varepsilon(\sigma) = (-1)^{n-r}$.

Démonstration. 1. L'égalité $(1, i) = (i-1, i)(1, i-1)(i-1, i)$ et le théorème 1.27 montrent que $\varepsilon((1, i)) = \varepsilon((i-1, i))^2 \varepsilon((1, i-1)) = \varepsilon((1, i-1))$. Par une récurrence sur i on en déduit $\varepsilon((1, i)) = \varepsilon((1, 2))$ pour tout $i \geq 2$. Or la transposition $(1, 2)$ de \mathcal{S}_n n'a qu'une inversion donc sa signature vaut -1 . On conclut pour une transposition quelconque en utilisant la relation

$$(i, j) = (1, j)(1, i)(1, j).$$

2. Soit c le cycle (a_1, \dots, a_k) . L'égalité $c = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2)$, combinée au théorème et au premier point du corollaire, donne directement $\varepsilon(c) = (-1)^{k-1}$.
3. Notons $\{1, \dots, n\} = C_1 \sqcup \cdots \sqcup C_r$ la partition en σ -orbites. Quitte à les renuméroter, on peut supposer que C_1, \dots, C_s sont les orbites non ponctuelles (c'est-à-dire non réduites à un singleton) et C_{s+1}, \dots, C_r les orbites ponctuelles. À partir de C_1, \dots, C_s on construit les cycles c_1, \dots, c_s à supports deux à deux disjoints comme dans la preuve du théorème 1.21 et on a montré que $\sigma = c_1 \cdots c_s$. La considération des cardinaux dans la partition donne $n = \ell(c_1) + \dots + \ell(c_s) + (r - s)$ où $\ell(c_i)$ désigne la longueur du cycle c_i et $r - s$ est le nombre d'orbites ponctuelles c'est-à-dire le nombre de points fixes. D'après le théorème 1.27 la signature de σ est donc

$$\begin{aligned}\varepsilon(\sigma) &= \varepsilon(c_1) \cdots \varepsilon(c_s) = (-1)^{\ell(c_1)-1} \cdots (-1)^{\ell(c_s)-1} = (-1)^{\ell(c_1)+\cdots+\ell(c_s)-s} \\ &= (-1)^{n-r}.\end{aligned}$$

\square

Le corollaire fournit une *méthode efficace pour calculer la signature* d'une permutation donnée : on la décompose d'abord en cycles à supports deux à deux disjoints, puis on utilise la propriété de morphisme de la signature et la connaissance de la signature des cycles. Cette manière de calculer la signature est, en général, largement préférable à celle reposant sur le nombre d'inversions.

Exemple 1.29. En utilisant la décomposition en cycles à supports deux à deux disjoints, on a :

$$\varepsilon\left(\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 8 & 6 & 5 & 4 & 3 & 7 & 1 \end{pmatrix}\right) = \varepsilon((1, 2, 8)(3, 6)(4, 5)) = (-1)^{3-1}(-1)(-1) = 1.$$

Noter que cette permutation a quatre σ -orbites : $\{1, 2, 8\}$, $\{3, 6\}$, $\{4, 5\}$, $\{7\}$. On retrouve ainsi que la signature est $(-1)^{8-4} = 1$.

Le premier point du corollaire 1.28 entraîne que l'application signature

$$\varepsilon : \mathcal{S}_n \longrightarrow \{\pm 1\}$$

est surjective quand $n \geq 2$. Il montre aussi que si $\sigma = \tau_1 \cdots \tau_m = \tau'_1 \cdots \tau'_k$ sont deux décompositions en transpositions d'une même permutation σ , alors $(-1)^{I(\sigma)} = \varepsilon(\sigma) = (-1)^m = (-1)^k$: ainsi les entiers m et k ont même parité, qui est aussi la parité de $I(\sigma)$. Cela explique l'observation de la remarque 1.23.4.

Définition 1.30

Pour $n \geq 2$, le *groupe alterné* est l'ensemble des permutations paires c'est-à-dire de signature 1. On le note \mathcal{A}_n , ou encore \mathfrak{A}_n .

D'après le théorème 1.27, le groupe alterné est stable par multiplication (le produit de deux permutations paires est une permutation paire).

Proposition 1.31

Le groupe alterné \mathcal{A}_n est de cardinal $n!/2$.

Démonstration. Soit τ (lettre grecque tau) une transposition quelconque de \mathcal{S}_n . Si σ est paire alors $\sigma\tau$ est impaire d'après le théorème 1.27. On a ainsi une application

$$\begin{aligned} f : \mathcal{A}_n &\longrightarrow \mathcal{S}_n - \mathcal{A}_n \\ \sigma &\longmapsto \sigma\tau. \end{aligned}$$

De plus f est bijective, de bijection réciproque

$$\begin{aligned} g : \mathcal{S}_n - \mathcal{A}_n &\longrightarrow \mathcal{A}_n \\ \sigma &\longmapsto \sigma\tau. \end{aligned}$$

(vérifier que $f \circ g = \text{id}$ et $g \circ f = \text{id}$). Donc on a $\text{Card}(\mathcal{A}_n) = \text{Card}(\mathcal{S}_n - \mathcal{A}_n)$. Comme $\mathcal{S}_n = \mathcal{A}_n \sqcup (\mathcal{S}_n - \mathcal{A}_n)$, on en déduit le cardinal de \mathcal{A}_n . \square

Nous poursuivrons l'étude du groupe symétrique et du groupe alterné au fil des prochains chapitres.

Concluons ce chapitre par quelques remarques de synthèse. Nous avons vu qu'il existe différentes façons de noter une permutation :

- celle comme un tableau à deux lignes : par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$; cette notation est valable pour toute permutation et ne contient aucune ambiguïté;
- celle comme un cycle $(1, 5, 4, 8)$: elle est plus compacte que la précédente, puisque les points fixes sont omis, mais n'est valable que pour un cycle. Par ailleurs cette écriture n'est pas unique, au sens où $(1, 5, 4, 8)$, $(5, 4, 8, 1)$, $(4, 8, 1, 5)$ et $(8, 1, 5, 4)$ représentent le même cycle (mais $(1, 4, 8, 5)$ est un cycle différent).

Nous avons aussi démontré plusieurs résultats de factorisation d'une permutation :

- celle comme produit de cycles à supports deux à deux disjoints : elle a l'avantage d'être unique, à l'ordre près des termes, et ses termes commutent. Elle permet aussi de calculer la signature de la permutation. Nous verrons au chapitre 3 qu'elle facilitera aussi le calcul de l'ordre de la permutation.
- celle comme produit de transpositions : elle n'est pas unique et les transpositions qui la constituent ne commutent pas entre elles de manière générale. Néanmoins cette factorisation contient la signature de la permutation : c'est la parité du nombre de transpositions.

☞ *Exercices pouvant être traités :*

- exercice 1.1 (question 1c) 
- exercice 1.2 (ce qui concerne la signature et le groupe alterné) 
- exercice 1.5 
- exercice 1.7   
- exercice 1.9   

Chapitre 2

Généralités sur les groupes

Introduction

Nous abordons à proprement parler la notion de groupe. Après avoir donné quelques exemples classiques, dont le groupe symétrique défini au chapitre 1, nous définissons des concepts usuels associés à cette structure algébrique : morphismes, sous-groupes, sous-groupes engendrés, produit direct. Les notions spécifiques aux groupes, notamment celle d'ordre d'un élément, seront étudiées au chapitre suivant.

2.1 Définitions et premières propriétés

On rappelle qu'une *loi (de composition) interne* sur un ensemble E est une application de $E \times E$ à valeurs dans E .

Définition 2.1

Un *groupe* est la donnée d'un ensemble G et d'une loi interne $*$ sur G satisfaisant :

1. (associativité de $*$) Pour tous x, y, z dans G on a $x*(y*z) = (x*y)*z$.
2. (existence d'un élément neutre pour $*$) Il existe e_G dans G vérifiant :

$$\forall x \in G, \quad e_G * x = x \quad \text{et} \quad x * e_G = x.$$

3. (existence d'un inverse pour $*$ dans G à chaque élément) Pour tout $x \in G$ il existe $y \in G$ tel que

$$x * y = e_G \quad \text{et} \quad y * x = e_G.$$

Un groupe $(G, *)$ est dit *commutatif*, ou encore *abélien*, lorsque la loi $*$ est commutative c'est-à-dire qu'elle satisfait, pour tous x, y dans G , $x * y = y * x$.

Pour simplifier, on écrit souvent « soit G un groupe ». Cependant il faut bien avoir à l'esprit qu'un groupe est la donnée d'un ensemble *et* d'une loi interne satisfaisant les axiomes requis. Lorsque la loi n'est pas précisée, c'est qu'elle est

explicitée ailleurs dans l'énoncé, ou implicite car il s'agit d'un groupe usuel. Il est donc indispensable de connaître les exemples classiques de groupes vus dans le cours avant d'aborder les énoncés des exercices.

Du fait de l'associativité, il est inutile de garder les parenthèses dans un produit d'éléments x_1, \dots, x_n de G : on écrit simplement ce produit $x_1 * \dots * x_n$.

Proposition 2.2

Dans un groupe donné, l'élément neutre est unique et tout élément admet un unique inverse.

Démonstration. Soient e_G et e'_G deux éléments neutres d'un groupe $(G, *)$. Comme e_G est un élément neutre, on a $e_G * e'_G = e'_G$. Comme e'_G est un élément neutre, on a aussi $e_G * e'_G = e_G$. Donc $e_G = e'_G$.

Soient $x \in G$ et y, y' deux inverses de x dans G pour la loi $*$. En utilisant l'associativité et l'élément neutre, on a

$$y = y * e_G = y * (x * y') = (y * x) * y' = e_G * y' = y'$$

d'où l'unicité de l'inverse. □

Exemple 2.3. 1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sont des groupes abéliens. Leur élément neutre est 0.

2. Soit $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ou plus généralement un corps commutatif. Notons $K[X]$ l'ensemble des polynômes à coefficients dans K . Alors $(K[X], +)$ est un groupe abélien. De même, si $K(X)$ désigne l'ensemble des fractions rationnelles à coefficients dans K , alors $(K(X), +)$ est un groupe abélien.
3. $(\mathbb{N}, +)$ n'est pas un groupe : l'élément 1, par exemple, n'admet pas d'opposé dans \mathbb{N} .
4. $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$ sont des groupes abéliens, d'élément neutre 1 (on rappelle la notation : si K est un corps, K^* désigne $K - \{0\}$).
5. (\mathbb{Z}, \cdot) n'est pas un groupe car l'élément 0 n'admet pas d'inverse dans \mathbb{Z} . Même chose pour $(\mathbb{Z} - \{0\}, \cdot)$ car 2 n'admet pas d'inverse dans $\mathbb{Z} - \{0\}$.
6. Si E est un ensemble non vide, le groupe symétrique (\mathcal{S}_E, \circ) est un groupe d'après la proposition 1.6. Il n'est pas abélien en général.
7. Soit E un espace vectoriel sur un corps K . Alors $(E, +)$, où $+$ désigne l'addition des vecteurs, est un groupe abélien.
8. Soit $M_n(K)$ l'ensemble des matrices carrées de taille n à coefficients dans un corps K . Alors $(M_n(K), +)$, où $+$ désigne l'addition des matrices, est un groupe abélien. Cependant $(M_n(K), \cdot)$ n'est pas un groupe : la matrice nulle, par exemple, n'est pas inversible.
9. Soit $GL_n(K)$ l'ensemble des matrices carrées de taille n et inversibles à coefficients dans K . Alors $(GL_n(K), \cdot)$ est un groupe, qu'on appelle le *groupe général linéaire*. Il n'est pas abélien si $n > 1$. Par contre $(GL_n(K), +)$ n'est pas un groupe car la somme de deux matrices inversibles n'est généralement pas inversible (la loi $+$ n'est donc pas interne).

Parmi ces exemples certains, comme \mathbb{Z} , $K[X]$, $M_n(K)$, possèdent une seconde loi, la multiplication, qui leur confère une structure plus riche : c'est la notion d'anneau qui sera abordée dans le chapitre 6 et étudiée en détail dans l'unité *Anneaux*.

Notation multiplicative, notation additive. De manière usuelle la loi $*$ est notée multiplicativement par le symbole \cdot . On écrit $x \cdot y$ ou encore xy au lieu de $x * y$. Lorsque le groupe est abélien, la loi pourra être notée additivement : on écrit alors $x + y$ au lieu de $x * y$. Le tableau suivant récapitule les usages selon les différentes notations.

symbole	$*$	\cdot	$+$
loi	$x * y$	$x \cdot y$ ou xy	$x + y$
terminologie		groupe multiplicatif	groupe additif
élément neutre	e_G	e_G ou 1_G	0_G
inverse de $x \in G$	x^{-1}	x^{-1}	$-x$

Définition 2.4

Un groupe G est dit *fini* s'il ne possède qu'un nombre fini d'éléments. L'*ordre* de G , noté $\text{ord}(G)$ ou encore $\text{Card}(G)$, est alors le cardinal de G . Si G a une infinité d'éléments, on dit que G est un groupe *infini*.

Exemple 2.5. 1. Le groupe symétrique \mathcal{S}_E est fini si et seulement si l'ensemble E est de cardinal fini. Si E est de cardinal n , l'ordre de \mathcal{S}_E est $n!$ d'après la proposition 1.2.
2. Le groupe $(\mathbb{Z}, +)$ est infini.

Définition 2.6

Soit G un groupe fini. La *table de Cayley* de G est la table de multiplication de sa loi, une fois qu'on ordonne l'ensemble de ses éléments : si x_1, \dots, x_n sont ses éléments, la valeur inscrite à l'intersection de la i -ème ligne et de la j -ème colonne est l'élément $x_i x_j$.

Voici par exemple la table de \mathcal{S}_2 :

(\mathcal{S}_2, \circ)	id	(1, 2)
id	id	(1, 2)
(1, 2)	(1, 2)	id

et celle de \mathcal{S}_3 :

(\mathcal{S}_3, \circ)	id	(1, 2)	(2, 3)	(1, 3)	(1, 2, 3)	(1, 3, 2)
id	id	(1, 2)	(2, 3)	(1, 3)	(1, 2, 3)	(1, 3, 2)
(1, 2)	(1, 2)	id	(1, 2, 3)	(1, 3, 2)	(2, 3)	(1, 3)
(2, 3)	(2, 3)	(1, 3, 2)	id	(1, 2, 3)	(1, 3)	(1, 2)
(1, 3)	(1, 3)	(1, 2, 3)	(1, 3, 2)	id	(1, 2)	(2, 3)
(1, 2, 3)	(1, 2, 3)	(1, 3)	(1, 2)	(2, 3)	(1, 3, 2)	id
(1, 3, 2)	(1, 3, 2)	(2, 3)	(1, 3)	(1, 2)	id	(1, 2, 3)

On vérifie sur ces tables que id est un élément neutre, que chaque élément est inversible (l'élément neutre figurant une fois et une seule sur chaque ligne ainsi que sur chaque colonne) et enfin l'associativité de la loi.

Certaines propriétés d'un groupe se lisent sur sa table de Cayley. Par exemple un groupe est abélien si et seulement si sa table est symétrique par rapport à la diagonale (c'est le cas pour \mathcal{S}_2 mais pas pour \mathcal{S}_3).

L'énoncé suivant recense des règles de calcul dans les groupes. La dernière affirme que tout inverse à droite d'un élément est aussi son inverse à gauche.

Proposition 2.7

Soit G un groupe.

1. On a $e_G^{-1} = e_G$.
2. Pour tout $x \in G$, on a $(x^{-1})^{-1} = x$.
3. Pour tous x, y, z dans G , on a :

$$x * y = x * z \implies y = z \quad \text{et} \quad y * x = z * x \implies y = z.$$

4. Si x et y sont deux éléments de G alors $(x * y)^{-1} = y^{-1} * x^{-1}$.
5. Soit $x \in G$. S'il existe $y \in G$ satisfaisant $x * y = e_G$ alors $y = x^{-1}$.

Démonstration. Elle fait manipuler les axiomes d'un groupe et ne présente pas de difficulté particulière. Voir l'exercice 2.2. \square

Remarque 2.8. Dans un groupe G , les éléments $(x * y)^{-1}$ et $x^{-1} * y^{-1}$ ne coïncident pas a priori.

Soient x un élément d'un groupe $(G, *)$ et n un entier naturel. On note x^n l'élément $\underbrace{x * \dots * x}_{n \text{ fois}}$ si n est positif avec par convention $x^0 = e_G$. Pour n entier négatif, on note $x^n = (x^{-1})^{-n}$. On a alors les règles de calcul, pour tous m et n dans \mathbb{Z} :

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

En notation multiplicative, on écrit x^n mais en notation additive, on préfère écrire nx .

 *Exercices pouvant être traités :*

- exercice 2.1 
- exercice 2.2  
- exercice 2.3 

2.2 Morphismes de groupes

Définition 2.9

Soient $(G, *)$ et $(G', *')$ deux groupes. Un *morphisme de groupes* de G dans G' est une application $f : G \rightarrow G'$ qui préserve les lois de groupe c'est-à-dire :

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

Pour définir un morphisme de groupes, il faut deux groupes : n'oublions donc pas le s à groupes, même si morphisme est au singulier.

Proposition 2.10

Soit $f : G \rightarrow G'$ un morphisme de groupes. On a :

1. $f(e_G) = e_{G'}$;
2. pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$.

Démonstration. 1. Par propriété des éléments neutres, on a

$$e_{G'} *' f(e_G) = f(e_G) = f(e_G * e_G) = f(e_G) *' f(e_G)$$

donc $f(e_G) = e_{G'}$ par la règle de simplification de la proposition 2.7.

2. On a $f(x) *' f(x^{-1}) = f(x * x^{-1}) = f(e_G) = e_{G'}$, ce qui montre que $f(x)^{-1} = f(x^{-1})$ d'après le dernier point de la proposition 2.7. □

Définition 2.11

Un *isomorphisme* de groupes est un morphisme de groupes bijectif. Un groupe G est dit *isomorphe à un groupe G'* s'il existe un isomorphisme de groupes de G dans G' .

Un *automorphisme* d'un groupe G est un isomorphisme de groupes de G dans lui-même. On note $\text{Aut}(G)$ l'ensemble des automorphismes de G .

Exemple 2.12. 1. L'application $G \rightarrow G'$, $x \mapsto e_{G'}$ est un morphisme de groupes. On l'appelle parfois *morphisme trivial*.

2. L'application identité de G dans G , qui à x associe x , est un automorphisme de G .
3. Soit $n \in \mathbb{Z}$. L'application $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$, $x \mapsto nx$ est un morphisme de groupes : en effet si x, x' appartiennent à \mathbb{Z} , on a

$$f(x + x') = n(x + x') = nx + nx' = f(x) + f(x')$$

(prendre garde à la notation additive).

4. Si K est un corps, l'application déterminant

$$\begin{aligned} \det : (\text{GL}_n(K), \cdot) &\longrightarrow (K^*, \cdot) \\ M &\longmapsto \det M \end{aligned}$$

est un morphisme de groupes car $\det(MM') = \det(M)\det(M')$ pour toutes matrices M et M' de $\text{GL}_n(K)$, formule bien connue d'algèbre linéaire.

5. L'application signature

$$\begin{aligned} \varepsilon : \mathcal{S}_n &\longrightarrow \{\pm 1\} \\ \sigma &\longmapsto \varepsilon(\sigma) \end{aligned}$$

est un morphisme de groupes. En effet on constate que $\{\pm 1\}$ muni de la multiplication est un groupe, puis on utilise le théorème 1.27 qui établit la propriété de morphisme.

6. L'application exponentielle

$$\begin{aligned} \exp : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}_+^*, \cdot) \\ x &\longmapsto \exp(x) \end{aligned}$$

est un morphisme de groupes car $\exp(a+b) = \exp(a)\exp(b)$ pour tous a, b réels. C'est même un isomorphisme, de morphisme réciproque l'application logarithme \ln .

Remarque 2.13. Le groupe G est isomorphe au groupe G' si et seulement s'il existe une bijection $f : G \rightarrow G'$ telle que l'image par f de la table de Cayley de G est la table de Cayley de G' . Illustrons ceci sur un exemple très simple avec les tables de $(\{\pm 1\}, \cdot)$ et (\mathcal{S}_2, \circ) :

$(\{\pm 1\}, \cdot)$	1	-1	(\mathcal{S}_2, \circ)	id	(1, 2)
1	1	-1	id	id	(1, 2)
-1	-1	1	(1, 2)	(1, 2)	id

L'application $f : \{\pm 1\} \rightarrow \mathcal{S}_2$ définie par $f(1) = \text{id}$ et $f(-1) = (1, 2)$ est bijective, et l'image par f de la première table est la seconde. Donc f est un isomorphisme de groupes et $\{\pm 1\}$ est isomorphe à \mathcal{S}_2 .

Pour alléger les notations, les groupes des énoncés seront dorénavant notés multiplicativement, l'élément neutre de G sera alors 1_G .

Proposition 2.14

1. Soient G, G', G'' trois groupes. Si $f : G \rightarrow G'$ et $g : G' \rightarrow G''$ sont des morphismes de groupes alors $g \circ f : G \rightarrow G''$ est un morphisme de groupes.
2. Soit $f : G \rightarrow G'$ un isomorphisme de groupes. Alors l'application réciproque $f^{-1} : G' \rightarrow G$ est un morphisme de groupes, et donc un isomorphisme de groupes.

Démonstration. 1. Immédiat, laissé en exercice.

2. Soit $f : G \rightarrow G'$ un isomorphisme. Notons $g = f^{-1} : G' \rightarrow G$ son application réciproque. Montrons que g est un morphisme de groupes. Soient x' et y' deux éléments de G' . Il existe x et y dans G tels que $x' = f(x)$ et $y' = f(y)$. On a alors $g(x'y') = g(f(x)f(y)) = g(f(xy)) = xy = g(x')g(y')$, ce qui conclut.

□

Définition 2.15

Comme conséquence de la proposition, si G est isomorphe à G' alors G' est isomorphe à G . On note $G \simeq G'$ pour dire qu'il existe un isomorphisme de G dans G' (ou, de manière équivalente, qu'il en existe un de G' dans G). On dit alors que G et G' sont *isomorphes*.

L'isomorphie est une relation d'équivalence. En théorie des groupes, on cherche à classer les groupes à isomorphisme près. En effet les propriétés des groupes sont invariantes par isomorphisme : par exemple si $G \simeq G'$, alors G est abélien si et seulement si G' est abélien.

Profitons de l'occasion pour rappeler le résultat très utile suivant. Si G et G' sont deux ensembles *finis* et $f : G \rightarrow G'$ une application alors :

1. si f est bijective, G et G' ont même cardinal ;
2. si G et G' ont même cardinal alors : f injective $\iff f$ bijective $\iff f$ surjective.

Proposition 2.16

Si G est un groupe, l'ensemble $\text{Aut}(G)$ des automorphismes de G , muni de la composition, est un groupe.

Démonstration. La composée de deux automorphismes de G est encore un automorphisme de G , d'après la proposition 2.14. La composition est donc une loi interne sur $\text{Aut}(G)$. Son associativité est bien connue. Son élément neutre est l'automorphisme identité. L'inverse d'un automorphisme f est f^{-1} , qui est bien un automorphisme par la proposition 2.14, donc tout élément est inversible. □

L'exemple d'isomorphisme qui suit nous donne l'occasion de revenir un instant sur le groupe symétrique.

Proposition 2.17

Soient E et F deux ensembles non vides. Si E et F sont en bijection alors les groupes (\mathcal{S}_E, \circ) et (\mathcal{S}_F, \circ) sont isomorphes.

Démonstration. Soit f une bijection de E dans F . Considérons l'application :

$$\begin{aligned} \varphi : \mathcal{S}_E &\longrightarrow \mathcal{S}_F \\ \sigma &\longmapsto f \circ \sigma \circ f^{-1} \end{aligned}$$

et montrons que c'est un isomorphisme de groupes. D'abord $f \circ \sigma \circ f^{-1}$ est une bijection de F dans lui-même donc $\varphi(\sigma) \in \mathcal{S}_F$ pour tout $\sigma \in \mathcal{S}_E$. De plus φ est un morphisme de groupes : en effet, pour tous σ, σ' dans \mathcal{S}_E on a

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

Enfin on vérifie directement que l'application $\mathcal{S}_F \rightarrow \mathcal{S}_E$, $\sigma \mapsto f^{-1} \circ \sigma \circ f$ est l'application réciproque de φ . Donc φ est une bijection, ainsi qu'un isomorphisme. \square

Définition 2.18

Soit $f : G \rightarrow G'$ un morphisme de groupes. Le *noyau* de f , noté $\text{Ker } f$, est l'ensemble $f^{-1}(\{1_{G'}\}) = \{x \in G \mid f(x) = 1_{G'}\}$. L'*image* de f , notée $\text{Im } f$, est l'ensemble $f(G) = \{f(x) \mid x \in G\}$.

Noter que $\text{Ker } f$ est un sous-ensemble de G tandis que $\text{Im } f$ est un sous-ensemble de G' .

Exemple 2.19. Soit E, F des espaces vectoriels et $f : E \rightarrow F$ une application linéaire. Comme $f(x+y) = f(x) + f(y)$ pour tous x, y dans E , f est un morphisme de groupes de $(E, +)$ dans $(F, +)$. Le noyau (resp. l'image) de f comme application linéaire coïncide avec le noyau (resp. l'image) de f comme morphisme de groupes : $\text{Ker } f = \{x \in E \mid f(x) = 0_F\}$ et $\text{Im } f = \{f(x) \mid x \in E\}$.

Le critère suivant est très utile pour démontrer l'injectivité d'un morphisme.

Théorème 2.20

- Soit $f : G \rightarrow G'$ un morphisme de groupes. Alors :
1. f est injectif si et seulement si $\text{Ker } f = \{1_G\}$;
 2. f est surjectif si et seulement si $\text{Im } f = G'$.

Démonstration. La seconde affirmation est immédiate. La démonstration de la première est à retenir. Supposons $\text{Ker } f = \{1_G\}$. Si $f(x) = f(y)$ avec x, y dans G , on en déduit $1_{G'} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$. Par hypothèse on a donc $xy^{-1} = 1_G$ c'est-à-dire $x = y$. L'application f est injective. Réciproquement supposons f injective. Soit $x \in \text{Ker } f$: comme $f(1_G) = 1_{G'} = f(x)$ on a alors $1_G = x$. Donc $\text{Ker } f$ est réduit à $\{1_G\}$. \square

Exemple 2.21. 1. Soit $n \in \mathbb{Z}$ et $n \neq 0$. Le morphisme de groupes $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$, $x \mapsto nx$, est de noyau $\{0\}$ donc injectif. Son image est l'ensemble $n\mathbb{Z}$ des multiples entiers de n .

2. Le morphisme $\det : \text{GL}_n(K) \rightarrow K^*$, $M \mapsto \det M$ est surjectif car pour tout $\lambda \in K^*$, la matrice

$$A = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$$

vérifie $\det A = \lambda$. Le noyau du morphisme \det est l'ensemble des matrices carrées de déterminant 1 : on le note $SL_n(K)$ et on l'appelle le *groupe spécial linéaire* (nous verrons un peu plus tard que c'est un groupe).

3. Si $n \geq 2$, le morphisme signature $\varepsilon : \mathcal{S}_n \rightarrow \{\pm 1\}$ est surjectif et de noyau le groupe alterné \mathcal{A}_n , d'après le chapitre 1.

☞ *Exercices pouvant être traités :*

- exercice 2.4 
- exercice 2.6   
- exercice 2.7  

2.3 Sous-groupes

Définition 2.22

Soit G un groupe. Un sous-ensemble H de G est un *sous-groupe* de G lorsqu'il vérifie les conditions suivantes :

1. H est stable pour la loi de G : pour tous x, y dans H , xy appartient à H ;
2. (H, \cdot) est un groupe.

On note $H < G$ pour dire que H est un sous-groupe de G .

Voyons plusieurs critères pratiques pour démontrer qu'un sous-ensemble est un sous-groupe.

Proposition 2.23

Soit H un sous-ensemble de G . Alors H est un sous-groupe de G si et seulement s'il satisfait les conditions suivantes :

1. H est non vide ;
2. pour tous x, y dans H , xy appartient à H ;
3. pour tout x dans H , x^{-1} appartient à H .

De manière équivalente, H est un sous-groupe de G si et seulement s'il satisfait :

1. H est non vide ;
2. pour tous x, y dans H , xy^{-1} appartient à H .

Enfin dans ces deux critères, la condition « H est non vide » peut être remplacée par « 1_G appartient à H ».

Un sous-groupe H a donc même élément neutre que le groupe G : $1_H = 1_G$.

Démonstration. C'est un bon exercice, laissé aux lecteurs, pour manipuler la définition de sous-groupe. Expliquons pourquoi on peut substituer la condition « 1_G appartient à H » à « H est non vide » dans le premier critère. Si H satisfait les conditions du premier critère, H est non vide : il existe donc un élément $h \in H$.

Or H est stable par passage à l'inverse donc $h^{-1} \in H$. Enfin H est stable par la loi donc $1_G = hh^{-1} \in H$. Supposons maintenant que H satisfait le premier critère avec « 1_G appartient à H » au lieu de « H est non vide ». Alors H contenant 1_G , il est non vide et le premier critère est vérifié. \square

Remarque 2.24. Pour montrer qu'un ensemble est un groupe, il est souvent plus facile de montrer que c'est un sous-groupe d'un groupe, lorsque c'est possible.

- Exemple 2.25.**
1. Les ensembles $\{1_G\}$ et G sont des sous-groupes de G . Ce sont les *sous-groupes triviaux* de G . Les sous-groupes non triviaux, s'il en existe, sont appelés les *sous-groupes propres* de G .
 2. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, qui est un sous-groupe de $(\mathbb{R}, +)$, qui est lui-même un sous-groupe de $(\mathbb{C}, +)$.
 3. Si F un sous-espace vectoriel d'un espace vectoriel E alors $(F, +)$ est un sous-groupe de $(E, +)$.
 4. Si $n \in \mathbb{Z}$, l'ensemble $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$. Nous verrons dans l'exercice 2.12 que tout sous-groupe de $(\mathbb{Z}, +)$ est de cette forme.
 5. Pour $n \in \mathbb{N}$, posons $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$, l'ensemble des racines n -èmes de l'unité. Alors (U_n, \cdot) est un sous-groupe de (\mathbb{C}^*, \cdot) .

Proposition 2.26

Soit $f : G \rightarrow G'$ un morphisme de groupes.

1. Si H est un sous-groupe de G alors son image directe $f(H)$ est un sous-groupe de G' .
2. Si H' est un sous-groupe de G' alors son image réciproque $f^{-1}(H')$ est un sous-groupe de G .
3. En particulier $\text{Im } f$ et $\text{Ker } f$ sont des sous-groupes de G' et G respectivement.

Démonstration. Cette démonstration est à connaître.

1. On a $1_{G'} = f(1_G) \in f(H)$. Soient x', y' dans $f(H)$. Il existe x, y dans H tels que $x' = f(x)$ et $y' = f(y)$. On a alors

$$x'y'^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$$

car xy^{-1} appartient au sous-groupe H . Donc $f(H)$ est un sous-groupe de G' .

2. On a $f(1_G) = 1_{G'} \in H'$ d'où $1_G \in f^{-1}(H')$. Soient x, y dans $f^{-1}(H')$. Donc $f(x)$ et $f(y)$ appartiennent à H' . Ainsi on a $f(xy^{-1}) = f(x)f(y)^{-1}$ qui appartient à H' car H' est un sous-groupe. Donc $xy^{-1} \in f^{-1}(H')$. Ainsi $f^{-1}(H')$ est un sous-groupe de G .

\square

- Exemple 2.27.**
1. Le groupe alterné \mathcal{A}_n est un sous-groupe de \mathcal{S}_n car c'est le noyau du morphisme signature $\varepsilon : \mathcal{S}_n \rightarrow \{\pm 1\}$.

2. Le groupe spécial linéaire $SL_n(K)$ est un sous-groupe de $GL_n(K)$ car c'est le noyau du morphisme déterminant $\det : GL_n(K) \rightarrow K^*$.

Proposition 2.28

L'intersection d'une famille quelconque de sous-groupes d'un groupe G est un sous-groupe de G .

Démonstration. Soit $(H_i)_{i \in I}$ une famille de sous-groupes de G . Posons $H = \bigcap_{i \in I} H_i$. Cet ensemble contient 1_G car 1_G appartient à tous les sous-groupes H_i . Soient x et y dans H . Alors pour tout i , le sous-groupe H_i contient x et y donc aussi xy^{-1} . On en déduit $xy^{-1} \in H$. Ainsi H est un sous-groupe de G .

Remarque : par convention si l'ensemble I est vide, l'intersection est réduite à $\{1_G\}$. \square

Remarque 2.29. La réunion de deux sous-groupes *n'est pas* un sous-groupe en général. Par exemple $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$ car il n'est pas stable par addition : 2 et 3 appartiennent à $2\mathbb{Z} \cup 3\mathbb{Z}$ mais pas 5. Voir aussi l'exercice 2.11 à ce sujet.

Voici d'autres sous-groupes classiques d'un groupe G sont donnés (vérifier à titre d'exercice que ce sont bien des sous-groupes).

Exemple 2.30. 1. Soit A un sous-ensemble de G . L'ensemble

$$C_G(A) = \{x \in G \mid \forall a \in A, xa = ax\}$$

est un sous-groupe de G , appelé le *centralisateur de A dans G* .

2. L'ensemble

$$Z(G) = C_G(G) = \{x \in G \mid \forall y \in G, xy = yx\}$$

est un sous-groupe de G , appelé le *centre de G* . Le groupe G est abélien si et seulement si $Z(G) = G$. Dans l'exercice 1.6 nous avons déterminé le centre du groupe symétrique \mathcal{S}_n .

3. Soit A un sous-ensemble de G . Pour $x \in G$, notons

$$xAx^{-1} = \{xax^{-1} \mid a \in A\}.$$

L'ensemble

$$N_G(A) = \{x \in G \mid xAx^{-1} = A\}$$

est un sous-groupe de G , appelé le *normalisateur de A dans G* . Attention à cette définition : l'égalité d'ensembles $xAx^{-1} = A$ ne signifie pas que $xax^{-1} = a$ pour tout $a \in A$.

L'énoncé suivant justifie, dans une certaine mesure, l'intérêt porté au groupe symétrique dans l'étude des groupes.

Théorème 2.31 (Cayley)

Tout groupe G est isomorphe à un sous-groupe du groupe symétrique \mathcal{S}_G .

Démonstration. Pour g fixé dans G , considérons l'application

$$\begin{aligned} \varphi_g : G &\longrightarrow G \\ x &\longmapsto gx. \end{aligned}$$

C'est une bijection, d'application réciproque $x \mapsto g^{-1}x$ (mais φ_g n'est pas un morphisme de groupes puisque $\varphi_g(1_G) = g$). On peut donc voir φ_g comme une permutation de l'ensemble G et écrire $\varphi_g \in \mathcal{S}_G$. Considérons ensuite l'application

$$\begin{aligned} \varphi : G &\longrightarrow \mathcal{S}_G \\ g &\longmapsto \varphi_g. \end{aligned}$$

C'est un morphisme de groupes. En effet pour tout $x \in G$ on a

$$\varphi(gg')(x) = \varphi_{gg'}(x) = (gg')x = g(g'x) = \varphi_g(\varphi_{g'}(x)) = (\varphi_g \circ \varphi_{g'})(x)$$

donc $\varphi(gg') = \varphi(g) \circ \varphi(g')$. De plus φ est injective : en effet, si $g \in \text{Ker } \varphi$ alors on a $\varphi_g = \text{id}_G$ donc pour tout $x \in G$ on a $\varphi_g(x) = gx = x$; en prenant $x = 1_G$ on en déduit $g = 1_G$. Ainsi φ est un isomorphisme de G sur son image $\text{Im}(\varphi)$, qui est un sous-groupe de \mathcal{S}_G . \square

 Exercices pouvant être traités :

- exercice 2.8 
- exercice 2.9 
- exercice 2.11  
- exercice 2.12 

2.4 Sous-groupe engendré par une partie

Définition 2.32

Soit A une partie d'un groupe G . L'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G , appelé le *sous-groupe engendré par* A . On le note $\langle A \rangle$.

C'est le plus petit sous-groupe, au sens de l'inclusion, contenant A . Cela signifie que si H est un sous-groupe de G satisfaisant :

1. $A \subset H$;
2. si H' est un sous-groupe de G contenant A alors $H \subset H'$.

alors $H = \langle A \rangle$, et inversement.

Exemple 2.33. On a $\langle \emptyset \rangle = \{1_G\}$ et $\langle G \rangle = G$. Si H est un sous-groupe de G alors $\langle H \rangle = H$. Nous verrons des exemples moins triviaux d'ici peu.

L'énoncé qui suit décrit les éléments du sous-groupe engendré.

Proposition 2.34

Soit A une partie non vide d'un groupe G . On a

$$\langle A \rangle = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} \mid n \in \mathbb{N}^*, x_i \in A, \epsilon_i \in \{1, -1\}\}.$$

Démonstration. Posons $H = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} \mid n \in \mathbb{N}^*, x_i \in A, \epsilon_i \in \{1, -1\}\}$. Cet ensemble est non vide car $A \neq \emptyset$. Il est stable par la loi de G et par passage à l'inverse. Donc H est un sous-groupe de G d'après la proposition 2.23. De plus H contient A .

Soit H' un sous-groupe de G contenant A . Montrons que H' contient H . On sait que H' contient tous les éléments de A , et qu'il est stable par la loi et par passage à l'inverse puisque c'est un sous-groupe. Donc H' contient tous les éléments de la forme $x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}$ avec $n \geq 1, x_i \in A$ et $\epsilon_i \in \{1, -1\}$. Ainsi H' contient H .

Cela prouve que H est le plus petit sous-groupe de G contenant A d'où $H = \langle A \rangle$. \square

Dans le cas d'une partie finie $A = \{g_1, \dots, g_n\}$ on écrira $\langle g_1, \dots, g_n \rangle$ au lieu de $\langle \{g_1, \dots, g_n\} \rangle$ afin d'alléger les notations.

Exemple 2.35. Dans le groupe symétrique \mathcal{S}_3 , posons $\tau = (1, 2)$ et $\sigma = (1, 2, 3)$. Le sous-groupe $H = \langle \tau, \sigma \rangle$ contient, entre autres, les permutations $\text{id}, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma\tau, \sigma^2\tau, \dots$. En fait H contient toutes les transpositions de \mathcal{S}_3 : $\tau = (1, 2), \tau\sigma = (2, 3), \tau\sigma^2 = (1, 3)$. D'après le corollaire 1.22, on a donc $H = \mathcal{S}_3$.

Corollaire 2.36

Soit x un élément de G , alors $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

Dans le sous-groupe $\langle x \rangle$, on a bien évidemment $x^n x^m = x^{n+m} = x^m x^n$ pour tous n, m dans \mathbb{Z} . Le groupe $\langle x \rangle$ est donc abélien, même si G n'est pas lui-même abélien.

Définition 2.37

Soient G un groupe et A une partie de G . On dit que A engendre G , ou encore que A est une *partie génératrice de G* , lorsque $G = \langle A \rangle$. Le groupe G est dit *de type fini* quand il possède une partie génératrice finie. Il est dit *monogène* quand il est engendré par une partie réduite à un élément.

Un groupe monogène et fini s'appelle un *groupe cyclique*. Lorsque G est cyclique, tout élément $x \in G$ vérifiant $G = \langle x \rangle$ est appelé un *générateur* de G .

Parmi les groupes, ceux monogènes et cycliques ont la structure la plus simple. D'après une remarque précédente, ils sont toujours abéliens. Leur classification à isomorphisme près sera établie dans le prochain chapitre.

Exemple 2.38. 1. Le groupe $(\mathbb{Z}, +)$ est engendré par 1. En effet si $n \in \mathbb{Z}$ alors $n = \underbrace{1 + \cdots + 1}_{n \text{ fois}}$ si n est positif, et $n = -\underbrace{(1 + \cdots + 1)}_{-n \text{ fois}}$ si n est négatif.

Ainsi $(\mathbb{Z}, +)$ est de type fini, et même monogène. Cependant il n'est pas cyclique.

- Le groupe (U_n, \cdot) des racines complexes n -èmes de l'unité est engendré par $e^{2i\pi/n}$: en effet tout $z \in U_n$ s'écrit $z = e^{2ik\pi/n} = (e^{2i\pi/n})^k$ avec $k \in \{0, \dots, n-1\}$. Ainsi (U_n, \cdot) est de type fini, monogène, et même cyclique.

Plus généralement (U_n, \cdot) est engendré par toute racine primitive n -ème de l'unité i.e. un élément de la forme $e^{2i\pi\ell/n}$ où ℓ et n sont premiers entre eux. Démontrons cette affirmation.

Soit $k \in \{0, \dots, n-1\}$. On veut montrer qu'il existe $m \in \mathbb{Z}$ tel que $e^{2ik\pi/n} = (e^{2i\ell\pi/n})^m = e^{2i\ell m\pi/n}$ c'est-à-dire tel que n divise $k - \ell m$. Comme ℓ et n sont premiers entre eux, il existe des entiers u, v dans \mathbb{Z} tels que $\ell u + nv = 1$ par le théorème de Bézout (voir le chapitre 6 pour des rappels). Posons $m = ku$. On a alors $k - \ell m = k - \ell ku = k(1 - \ell u) = kvn$, qui est divisible par n , donc ce m convient.

- Le groupe symétrique \mathcal{S}_n est engendré par l'ensemble de ses cycles (théorème 1.21). Il est aussi engendré par l'ensemble de ses transpositions (corollaire 1.22).
- Tout groupe fini est de type fini puisque $G = \langle G \rangle$. La réciproque est fautive : $(\mathbb{Z}, +)$ est un groupe infini et de type fini.
- Le groupe $(\mathbb{Q}, +)$ n'est pas de type fini (exercice 2.13).

Remarque 2.39. Pour un groupe de type fini, il n'y a pas unicité de sa partie génératrice : par exemple $(\mathbb{Z}, +)$ est engendré par 1 mais aussi par -1 .

☞ *Exercices pouvant être traités :*

- exercice 2.5 
- exercice 2.10 
- exercice 2.13 

2.5 Produit direct

Dans cette section, $(G_i)_{i \in I}$ désigne une famille de groupes indexée par un ensemble non vide I .

Définition 2.40

Soit G le produit cartésien des G_i , autrement dit

$$G = \prod_{i \in I} G_i = \{(x_i)_{i \in I} \mid x_i \in G_i\}.$$

On munit l'ensemble G d'une structure de groupe en considérant la loi suivante :

$$(x_i)_{i \in I} \cdot (y_i)_{i \in I} = (x_i y_i)_{i \in I}$$

où $x_i y_i$ désigne le produit de x_i par y_i dans le groupe G_i . Le groupe G ainsi obtenu s'appelle le *produit direct* des groupes G_i .

Les lecteurs vérifieront à titre d'exercice que G muni de cette loi est bien un groupe, d'élément neutre $(1_{G_i})_{i \in I}$ et que l'inverse de $(x_i)_{i \in I}$ est l'élément $(x_i^{-1})_{i \in I}$. On voit aussi que G est abélien si et seulement si tous les groupes G_i sont abéliens.

Pour une famille finie de groupes G_1, \dots, G_n , leur produit direct est noté habituellement :

$$\prod_{i=1}^n G_i = G_1 \times \dots \times G_n$$

et se lit « G_1 fois G_2 ... fois G_n » (ou « croix » à la place de « fois »).

Ce procédé de produit direct permet de fabriquer de nouveaux groupes à partir de groupes existants.

Exemple 2.41. 1. Dans le groupe produit direct $(\mathbb{Z}, +) \times (\mathbb{C}^*, \cdot)$, on a :

$$(1, 2) \cdot (-1, 3) = (0, 6)$$

(on additionne sur la première composante et on multiplie sur la seconde).

2. Pour $n \in \mathbb{N}^*$, le groupe \mathbb{Z}^n est le produit direct de n copies du groupe additif $(\mathbb{Z}, +)$.
3. L'ensemble $\mathbb{Z}^{\mathbb{N}} = \prod_{i \in \mathbb{N}} \mathbb{Z}$ des suites d'éléments de \mathbb{Z} est un produit direct de copies du groupe additif $(\mathbb{Z}, +)$.

Remarque 2.42. Il existe une notion voisine du produit direct, celle de *somme directe* : il s'agit du sous-groupe de $\prod_{i \in I} G_i$ constitué des familles $(x_i)_{i \in I}$ pour lesquelles $x_i = 1_{G_i}$ sauf pour un nombre fini de $i \in I$. On note ce groupe $\bigoplus_{i \in I} G_i$.

Si la famille d'indices I est finie alors évidemment $\prod_{i \in I} G_i = \bigoplus_{i \in I} G_i$. Sinon l'inclusion $\bigoplus_{i \in I} G_i \subset \prod_{i \in I} G_i$ est généralement stricte. Par exemple, l'ensemble des suites d'éléments de \mathbb{Z} nulles à partir d'un certain rang est la somme directe $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}$; c'est un sous-groupe de $(\mathbb{Z}, +)^{\mathbb{N}}$.

Proposition 2.43

Soit $G = \prod_{i \in I} G_i$. Pour tout $j \in I$, l'application de projection sur la j -ème composante

$$p_j : \begin{array}{ccc} G & \longrightarrow & G_j \\ (x_i)_{i \in I} & \longmapsto & x_j \end{array}$$

est un morphisme de groupes surjectif, et de noyau isomorphe à $\prod_{i \neq j} G_i$.

Démonstration. Le cas d'un produit direct de deux groupes est traité dans l'exercice 2.14. Sa généralisation à $\prod_{i \in I} G_i$ est immédiate. \square

En théorie des groupes un problème important consiste à décomposer un groupe en produit direct de groupes, ou de sous-groupes, lorsque c'est possible. Bien entendu G est toujours isomorphe à $\{1\} \times G$ mais la situation intéressante est celle où aucun facteur n'est trivial. L'énoncé suivant explique à quelles conditions cela est possible.

Théorème 2.44 (Critère du produit direct)

Soient G, G_1, G_2 des groupes. Le groupe G est isomorphe au produit direct $G_1 \times G_2$ si et seulement si G contient deux sous-groupes H_1 et H_2 vérifiant les conditions suivantes :

1. $H_1 \simeq G_1$ et $H_2 \simeq G_2$;
2. pour tous $h_1 \in H_1$ et $h_2 \in H_2$ on a $h_1h_2 = h_2h_1$;
3. $H_1 \cap H_2 = \{1_G\}$;
4. $G = H_1H_2$, où H_1H_2 désigne le sous-ensemble $\{h_1h_2 \mid h_1 \in H_1, h_2 \in H_2\}$ de G .

Dans ce cas, tout élément de G s'écrit de façon unique sous la forme h_1h_2 avec $h_1 \in H_1$ et $h_2 \in H_2$.

Démonstration. Supposons que $G \simeq G_1 \times G_2$. Sans restreindre le raisonnement on peut supposer $G = G_1 \times G_2$. Soient p_1 et p_2 les projections de G sur G_1 et G_2 respectivement. Posons $H_1 = \text{Ker } p_2$ et $H_2 = \text{Ker } p_1$. Ce sont des sous-groupes de G , isomorphes respectivement à G_1 et G_2 d'après la proposition 2.43. D'autre part, quelque soient $h_1 \in H_1$ et $h_2 \in H_2$, il existe $x_1 \in G_1$ et $x_2 \in G_2$ tels que $h_1 = (x_1, 1_{G_2})$ et $h_2 = (1_{G_1}, x_2)$ d'où $h_1h_2 = (x_1, x_2) = h_2h_1$ par définition de la loi sur le produit direct. On vérifie directement que $H_1 \cap H_2 = \{1_G\}$ et que tout élément (x_1, x_2) de G s'écrit $(x_1, 1_{G_2})(1_{G_1}, x_2) \in H_1H_2$ d'où $G = H_1H_2$. Les quatre conditions sont satisfaites.

Inversement supposons les conditions satisfaites par deux sous-groupes H_1 et H_2 de G . Montrons que l'application

$$\begin{aligned} f : H_1 \times H_2 &\longrightarrow G \\ (h_1, h_2) &\longmapsto h_1h_2 \end{aligned}$$

est un isomorphisme de groupes, ce qui permettra de conclure, en utilisant $H_1 \simeq G_1$ et $H_2 \simeq G_2$, que $G \simeq G_1 \times G_2$. D'abord f est un morphisme car si (h_1, h_2) et (h'_1, h'_2) sont dans $H_1 \times H_2$ alors par la deuxième condition,

$$\begin{aligned} f((h_1, h_2)(h'_1, h'_2)) &= f(h_1h'_1, h_2h'_2) = h_1h'_1h_2h'_2 = h_1h_2h'_1h'_2 \\ &= f(h_1, h_2)f(h'_1, h'_2). \end{aligned}$$

L'application f est surjective car $G = H_1H_2$ (quatrième condition). Enfin si $(h_1, h_2) \in \text{Ker } f$ alors $h_1h_2 = 1_G$ d'où $h_1 = h_2^{-1} \in H_1 \cap H_2$ ce qui entraîne $h_1 = h_2 = 1_G$ par la troisième condition. Ainsi $\text{Ker } f = \{1_G\}$ d'où l'injectivité de f . Cela prouve que f est un isomorphisme de groupes.

L'unicité de l'écriture dans H_1H_2 vient enfin de l'injectivité de l'application f . □

Ce théorème sera souvent appliqué dans la situation où $G_1 = H_1$ et $G_2 = H_2$ sont eux-mêmes des sous-groupes de G . Dans ce cas, on dit que G est le *produit direct interne* des sous-groupes H_1 et H_2 . Le groupe G est alors isomorphe à $H_1 \times H_2$, l'isomorphisme étant donné d'après le théorème par :

$$\begin{aligned} H_1 \times H_2 &\longrightarrow G \\ (h_1, h_2) &\longmapsto h_1h_2. \end{aligned}$$

☞ *Exercices pouvant être traités :*

- exercice 2.14 
- exercice 2.15  

Chapitre 3

Ordre d'un élément, classes modulo un sous-groupe

Introduction

Ce chapitre introduit des notions fondamentales ayant trait aux groupes : ordre d'un élément, classification des groupes monogènes et cycliques, classes à gauche et à droite modulo un sous-groupe, théorème de Lagrange. Un peu d'arithmétique élémentaire sera utilisée : divisibilité, division euclidienne, pgcd, ppcm. Les exercices pourront faire appel à d'autres résultats classiques d'arithmétique, pour lesquels on renvoie au chapitre 6 en cas de besoin.

3.1 Ordre d'un élément

Définition 3.1

Soit x un élément d'un groupe G . On dit que x est *d'ordre fini* si le sous-groupe $\langle x \rangle$ est fini. Dans ce cas on appelle l'*ordre de x* le cardinal du sous-groupe $\langle x \rangle$, et on le note $\text{ord}(x)$.

Exemple 3.2. Tout groupe a un unique élément d'ordre 1 : l'élément neutre 1_G .

Commençons par un résultat préliminaire, élémentaire mais d'usage constant.

Lemme 3.3

Soient G un groupe et x un élément de G . Supposons qu'il existe un entier $n \geq 1$ tel que $x^n = 1_G$. Alors

$$\forall a \in \mathbb{Z}, \quad x^a = x^r$$

où $r \in \{0, \dots, n-1\}$ est le reste de la division euclidienne de a par n .

Démonstration. Cette division euclidienne est $a = nq + r$ avec $q \in \mathbb{Z}$ et $r \in \{0, \dots, n-1\}$ le reste. On a alors $x^a = x^{nq+r} = (x^n)^q x^r = 1_G x^r = x^r$. \square

L'énoncé qui suit rassemble des propriétés importantes de l'ordre d'un élément et une caractérisation essentielle de celui-ci par l'étude de puissances successives.

Théorème 3.4

Soient G un groupe et x un élément de G .

1. L'élément x est d'ordre fini si et seulement s'il existe un entier $n \geq 1$ tel que $x^n = 1_G$.
2. Soit x d'ordre fini. Son ordre est le plus petit entier $\ell \geq 1$ satisfaisant $x^\ell = 1_G$. Il est donc caractérisé par

$$x^\ell = 1_G \quad \text{et} \quad \forall k \in \{1, \dots, \ell - 1\}, \quad x^k \neq 1_G.$$

Les éléments $1_G, x, x^2, \dots, x^{\ell-1}$ sont alors deux à deux distincts et

$$\langle x \rangle = \{1_G, x, x^2, \dots, x^{\ell-1}\}$$

Démonstration. 1. Supposons $x^n = 1_G$. On sait que $\langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$. Or par le lemme 3.3, les puissances entières de x ne prennent qu'au plus n valeurs distinctes : $1_G, x, \dots, x^{n-1}$. Donc $\langle x \rangle$ est de cardinal fini et ainsi, x est d'ordre fini. Réciproquement supposons x d'ordre fini. Considérons l'ensemble $\{m \in \mathbb{N}^* \mid x^m = 1_G\}$. Il est non vide : en effet, comme le sous-groupe $\langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$ est fini, il existe deux entiers distincts $n_1 > n_2$ tels que $x^{n_1} = x^{n_2}$; on a donc $x^{n_1 - n_2} = 1_G$. On pose alors $n = n_1 - n_2$, et x^n vaut 1_G .

2. Comme x est d'ordre fini, il existe un plus petit entier $\ell \geq 1$ tel que $x^\ell = 1_G$ d'après le point 1 de l'énoncé. Montrons que les éléments $1_G, x, x^2, \dots, x^{\ell-1}$ sont deux à deux distincts. Supposons $x^{n_1} = x^{n_2}$ avec $0 \leq n_1 \leq n_2 \leq \ell - 1$. On a $x^{n_1 - n_2} = 1_G$ avec $0 \leq n_1 - n_2 \leq \ell - 1$. Par minimalité de ℓ , on en déduit $n_1 - n_2 = 0$ d'où $n_1 = n_2$, ce qui prouve l'assertion. De plus, on a $\{1_G, x, x^2, \dots, x^{\ell-1}\} \subset \langle x \rangle$. L'inclusion réciproque est fournie par le fait que $x^\ell = 1_G$ et le lemme 3.3. □

Exemple 3.5. 1. Dans le groupe multiplicatif $\text{GL}_2(\mathbb{C})$, la matrice $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est d'ordre 4. En effet on a

$$A \neq \text{id}, \quad A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq \text{id}, \quad A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \neq \text{id}, \quad A^4 = \text{id}$$

où id désigne la matrice identité de $\text{GL}_2(\mathbb{C})$.

2. Les ordres des éléments de \mathcal{S}_3 sont les suivants :

- (a) id est d'ordre 1 ;
- (b) les transpositions $(1, 2), (1, 3)$ et $(2, 3)$ sont d'ordre 2 ;

(c) les 3-cycles $(1, 2, 3)$ et $(1, 3, 2)$ sont d'ordre 3.

Plus généralement tout k -cycle de \mathcal{S}_n est d'ordre k (voir le chapitre 1).

3. Dans le groupe multiplicatif U_n des racines n -èmes de l'unité, l'élément $e^{2i\pi/n}$ est d'ordre n . Plus généralement si k et n sont premiers entre eux, l'élément $e^{2i\pi k/n}$ est d'ordre n dans U_n (démonstration laissée en exercice – voir par exemple l'exercice 6.5 pour une version additive de cette affirmation).

Voyons une caractérisation de l'ordre d'un élément en termes de divisibilité.

Théorème 3.6

Soient G un groupe et x un élément d'ordre fini. L'ordre de x est l'unique entier $\ell \geq 1$ satisfaisant la propriété

$$\forall k \in \mathbb{Z} : (x^k = 1_G \iff \ell \text{ divise } k).$$

En particulier si $x^k = 1_G$ alors ℓ divise k .

Démonstration. Notons $\ell = \text{ord}(x)$ et montrons que ℓ satisfait la propriété annoncée. Soit $k \in \mathbb{Z}$. La division euclidienne de k par ℓ s'écrit $k = q\ell + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < \ell$. Comme $x^\ell = 1_G$ d'après le théorème 3.4, le lemme 3.3 entraîne : $x^k = 1_G \iff x^r = 1_G$. De plus, par la propriété de minimalité vérifiée par ℓ (théorème 3.4.2), $x^r = 1_G$ équivaut à $r = 0$, c'est-à-dire à ℓ divise k .

Montrons maintenant qu'il existe au plus un entier ≥ 1 vérifiant la propriété de l'énoncé. Si $\ell \geq 1$ est un entier qui la satisfait, cela signifie les égalités d'ensembles suivantes :

$$\{k \in \mathbb{Z} \mid x^k = 1_G\} = \{k \in \mathbb{Z} \mid \ell \text{ divise } k\} = \ell\mathbb{Z}.$$

Ainsi ℓ est le plus petit entier naturel non nul de l'ensemble $\{k \in \mathbb{Z} \mid x^k = 1_G\}$. Cela caractérise ℓ de manière unique à partir de x . \square

Remarque 3.7. L'ordre ℓ de x est ainsi le plus petit entier $\ell \geq 1$ satisfaisant $x^\ell = 1_G$, « plus petit » pouvant être compris dans l'un ou l'autre des sens suivants :

- pour la relation d'ordre usuelle \leq sur \mathbb{N}^* (cf. théorème 3.4) ;
- pour la relation d'ordre donnée par la divisibilité sur \mathbb{N}^* (cf. théorème 3.6).

Une erreur fréquente est de croire que $x^n = 1_G$ signifie que x est d'ordre n . Or cela assure uniquement que $\text{ord}(x)$ divise n . Par exemple, si x est un élément d'ordre 2, il satisfait $x^2 = 1_G$ mais aussi $x^4 = (x^2)^2 = (1_G)^2 = 1_G$, $x^8 = (x^2)^4 = (1_G)^4 = 1_G$, etc. Pour conclure que l'ordre est n , il reste à montrer que si un entier $m \geq 1$ vérifie $x^m = 1_G$ alors $n \leq m$ (ou n divise m).

Dans le groupe symétrique, décomposer une permutation en cycles permet de calculer aisément son ordre.

Proposition 3.8

Soit σ une permutation dans \mathcal{S}_n distincte de l'identité, de décomposition

en cycles à supports deux à deux disjoints $\sigma = c_1 \cdots c_s$. Alors on a

$$\text{ord}(\sigma) = \text{ppcm}(\ell(c_1), \dots, \ell(c_s))$$

où $\ell(c_i)$ désigne la longueur du cycle c_i .

Démonstration. Notons m ce ppcm. Pour tout i , $\ell(c_i)$ divise m donc $c_i^m = \text{id}$ par la caractérisation de l'ordre en termes de divisibilité (théorème 3.6). Comme les cycles sont à supports deux à deux disjoints, ils commutent deux à deux (proposition 1.9). On en déduit $\sigma^m = c_1^m \cdots c_s^m = \text{id}$. Ainsi σ est d'ordre fini d'après le théorème 3.4.

Pour conclure que l'ordre de σ est m , il nous reste d'après le théorème 3.6 à montrer que pour tout entier $k \geq 1$, on a

$$\sigma^k = \text{id} \implies m \mid k$$

(l'autre implication est immédiate). Supposons $\sigma^k = \text{id}$ et soit x dans le support d'un cycle c_i . Alors $\sigma^k(x) = c_i^k(x)$ car x est fixe par tous les cycles c_j avec $j \neq i$. On en déduit, par hypothèse, $c_i^k(x) = \text{id}(x) = x$. Ceci étant valable pour tout x dans le support de c_i , et comme c_i^k est l'identité en-dehors de son support, on a $c_i^k = \text{id}$. Donc $\ell(c_i) \mid k$ par le théorème 3.6. Ainsi le ppcm m divise k . \square

 Exercices pouvant être traités :

- exercice 3.1 
- exercice 3.2  
- exercice 3.3   
- exercice 3.4 
- exercice 3.5   

3.2 Le groupe additif $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier naturel. On renvoie à l'annexe page 99 pour des rappels sur les relations d'équivalence, ensembles quotients et systèmes de représentants.

Définition 3.9

Soient a et b deux entiers relatifs. On dit que a est congru à b modulo n lorsque n divise $a - b$. On écrit alors $a \equiv b \pmod{n}$, ou encore $a \equiv b [n]$.

Proposition 3.10

La congruence modulo n est une relation d'équivalence sur \mathbb{Z} .

Démonstration. Soient a, b et c dans \mathbb{Z} . Alors n divise $a - a$ d'où la réflexivité. Si $a \equiv b \pmod{n}$ alors n divise $a - b$ donc n divise $b - a$, ce qui signifie $b \equiv a \pmod{n}$: la relation est symétrique. Enfin si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ alors n divise simultanément $a - b$ et $b - c$ donc n divise leur somme $a - c$. Cela prouve la transitivité. \square

Pour tout $a \in \mathbb{Z}$, la classe d'équivalence de a modulo n est :

$$\{a + nk \mid k \in \mathbb{Z}\}.$$

On la note $a + n\mathbb{Z}$, ou $a \bmod n$, ou encore \bar{a} lorsque l'entier n est sous-entendu (on lit alors « a barre » ou « classe de a »).

Définition 3.11

L'ensemble des classes d'équivalence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ (on lit « \mathbb{Z} sur $n\mathbb{Z}$ » ou encore « \mathbb{Z} modulo $n\mathbb{Z}$ »).

- Exemple 3.12.**
1. Si $n = 0$, on a $a \equiv b \pmod{0}$ si et seulement si $a = b$. Donc $\bar{a} = \{a\}$ et $\mathbb{Z}/0\mathbb{Z} = \{\{a\} \mid a \in \mathbb{Z}\}$, ensemble qu'on identifie à \mathbb{Z} .
 2. Si $n = 1$, on a toujours $a \equiv b \pmod{1}$. Tous les éléments sont dans la même classe et il n'y a qu'une seule classe modulo 1 : $\bar{0} = 0 + 1\mathbb{Z} = \mathbb{Z}$. Donc $\mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\}$, ensemble à un élément.
 3. Si $n = 2$, deux entiers relatifs sont congrus modulo 2 si et seulement s'ils ont même parité. Donc $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\} = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\}$.

Proposition 3.13

On a $a \equiv b \pmod{n}$ si et seulement si les divisions euclidiennes de a et b par n ont le même reste.

Démonstration. Soient $a = nq_a + r_a$ (resp. $b = nq_b + r_b$) la division euclidienne de a (resp. b) par n , avec r_a (resp. r_b) le reste, qui appartient à $\{0, \dots, n-1\}$. On a alors

$$\begin{aligned} a \equiv b \pmod{n} &\iff n \mid (a - b) \iff n \mid n(q_a - q_b) + r_a - r_b \\ &\iff n \mid (r_a - r_b). \end{aligned}$$

Or $0 \leq |r_a - r_b| \leq n - 1$. Donc $n \mid (r_a - r_b)$ équivaut à $r_a - r_b = 0$ c'est-à-dire à $r_a = r_b$. \square

Théorème 3.14

Supposons $n \geq 1$.

1. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n et

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Plus généralement tout $k \in \mathbb{Z}$ on a

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{k}, \overline{k+1}, \dots, \overline{k+n-1}\}.$$

2. Si a, b, a', b' sont des entiers relatifs avec $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors $a + b \equiv a' + b' \pmod{n}$. Autrement dit on a :

$$(\bar{a} = \bar{a'} \quad \text{et} \quad \bar{b} = \bar{b'}) \implies \overline{a+b} = \overline{a'+b'}.$$

3. Posons, pour a, b dans \mathbb{Z} de classes \bar{a}, \bar{b} dans $\mathbb{Z}/n\mathbb{Z}$,

$$\bar{a} + \bar{b} = \overline{a + b}.$$

Muni de cette loi d'addition interne $+$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien, de neutre $\bar{0}$. L'inverse de \bar{a} pour cette loi est l'élément $\overline{-a}$, qu'on notera $-\bar{a}$.

4. L'application π (lettre grecque pi) :

$$\begin{array}{ccc} \pi : (\mathbb{Z}, +) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z}, +) \\ a & \longmapsto & \bar{a} \end{array}$$

est un morphisme de groupes surjectif et de noyau $n\mathbb{Z}$. On l'appelle la *surjection canonique*.

5. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique et engendré par $\bar{1}$.

Démonstration. 1. D'après la proposition 3.13, a et son reste dans la division euclidienne par n ont même classe modulo n . Comme les restes possibles de ces divisions euclidienne sont $0, 1, \dots, n-1$, la première assertion est démontrée. Fixons maintenant $k \in \mathbb{Z}$. Les classes $\bar{k}, \dots, \bar{k} + n - 1$ sont deux à deux distinctes : en effet si $\bar{k} + \bar{i} = \bar{k} + \bar{j}$ avec $0 \leq i, j \leq n-1$ alors n divise $k + j - k - i = j - i$ d'où $j = i$ puisque $0 \leq j - i \leq n-1$. Par égalité de cardinaux, on conclut $\mathbb{Z}/n\mathbb{Z} = \{\bar{k}, \bar{k} + 1, \dots, \bar{k} + n - 1\}$.

2. Supposons que $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ c'est-à-dire n divise à la fois $a - a'$ et $b - b'$. Comme $(a + b) - (a' + b') = (a - a') + (b - b')$, alors n divise $(a + b) - (a' + b')$ donc $a + b \equiv a' + b' \pmod{n}$.
3. Il faut s'assurer que la formule $\bar{a} + \bar{b} = \overline{a + b}$ définit sans ambiguïté une application $+: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ c'est-à-dire que pour tout $x \in \bar{a}$ et $y \in \bar{b}$ on a $\overline{x + y} = \overline{a + b}$. Or c'est précisément le point précédent du théorème.

Pour montrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien, on prouve que les axiomes de groupe sont satisfaits. Ils se déduisent des propriétés de l'addition sur \mathbb{Z} par réduction modulo n . Par exemple pour l'associativité, si a, b, c sont des entiers dont les classes modulo n sont respectivement $\bar{a}, \bar{b}, \bar{c}$, alors

$$\begin{aligned} (\bar{a} + \bar{b}) + \bar{c} &= \overline{a + b} + \bar{c} = \overline{(a + b) + c} = \overline{a + (b + c)} \\ &= \bar{a} + \overline{b + c} = \bar{a} + (\bar{b} + \bar{c}). \end{aligned}$$

Les autres vérifications sont similaires et laissées aux lecteurs.

4. L'application π est un morphisme de groupes car l'addition a été définie de manière à satisfaire $\pi(a + b) = \overline{a + b} = \bar{a} + \bar{b} = \pi(a) + \pi(b)$ pour tous a, b dans \mathbb{Z} . L'application est clairement surjective. Son noyau est l'ensemble des entiers relatifs congrus à 0 modulo n , c'est-à-dire divisibles par n : c'est le sous-groupe $n\mathbb{Z}$ de $(\mathbb{Z}, +)$.

5. On sait que le groupe $(\mathbb{Z}, +)$ est engendré par 1 : tout entier $a \in \mathbb{Z}$ s'écrit $a = a \cdot 1$. Modulo n , on en déduit $\bar{a} = a\bar{1}$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$. En particulier le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est engendré par $\bar{1}$. Comme il est fini, il est cyclique. \square

Exemple 3.15. Prenons $n = 10$. Alors $\bar{1}$ et $\overline{11}$ sont dans la même classe : on a $1 \equiv 11 \pmod{10}$, ce que l'on note $\bar{1} = \overline{11}$ dans $\mathbb{Z}/10\mathbb{Z}$. D'après le théorème on a :

$$\mathbb{Z}/10\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}.$$

Pour l'addition, on a par exemple $\bar{7} + \bar{8} = \overline{7+8} = \overline{15} = \bar{5}$.

Exemple 3.16. Voici la table de Cayley du groupe $(\mathbb{Z}/5\mathbb{Z}, +)$:

$(\mathbb{Z}/5\mathbb{Z}, +)$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

En particulier $\bar{2}$ est d'ordre 5 dans $(\mathbb{Z}/5\mathbb{Z}, +)$ car

$$\begin{aligned} \bar{2} &\neq \bar{0} \\ \bar{2} + \bar{2} &= \bar{4} \neq \bar{0} \\ \bar{2} + \bar{2} + \bar{2} &= \bar{1} \neq \bar{0} \\ \bar{2} + \bar{2} + \bar{2} + \bar{2} &= \bar{3} \neq \bar{0} \\ \bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2} &= \bar{0}. \end{aligned}$$

Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est un exemple typique de groupe quotient. Nous retrouverons cette construction dans un cadre plus général au chapitre 4.

 *Exercices pouvant être traités :*

- exercice 3.6 
- exercice 3.7 

3.3 Classification des groupes monogènes et des groupes cycliques

Commençons par un critère simple, dont la démonstration est à retenir, pour montrer qu'un groupe fini est cyclique.

Proposition 3.17

Soit G un groupe fini d'ordre n . Alors G est cyclique si et seulement s'il possède un élément d'ordre n .

Démonstration. Pour le sens direct, prenons un générateur x de G : cet élément vérifie $\langle x \rangle = G$, il est donc d'ordre n . Pour le sens réciproque, supposons qu'il existe $x \in G$ d'ordre n . Alors le sous-groupe $\langle x \rangle$ est contenu dans G . Ces ensembles ayant même cardinal n , ils sont égaux. \square

Exemple 3.18. Le groupe symétrique \mathcal{S}_3 est d'ordre 6. Il n'est pas cyclique car il ne contient aucun élément d'ordre 6 (voir l'exemple 3.5).

Théorème 3.19

Soit G un groupe monogène.

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

En particulier tout groupe monogène est abélien.

Démonstration. Cette démonstration est à retenir.

1. Supposons $G = \langle g \rangle$ avec $g \in G$, et G infini. L'application

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow G \\ m &\longmapsto g^m \end{aligned}$$

est un morphisme surjectif de groupes (vérifiez-le). Il est injectif : en effet si $g^m = 1_G$ avec $m \neq 0$ alors g est d'ordre fini donc $G = \langle g \rangle$ l'est aussi, ce qui est impossible ; ainsi $m = 0$, ce qui donne $\text{Ker } f = \{0\}$ et l'injectivité. On conclut que f est un isomorphisme de $(\mathbb{Z}, +)$ dans G d'où $G \simeq (\mathbb{Z}, +)$.

2. Supposons $G = \langle g \rangle$ avec $g \in G$, et G fini d'ordre n . Par le théorème 3.4 on a $G = \{1_G, g, \dots, g^{n-1}\}$ où $n = \text{ord}(g) = \text{ord}(G)$. Si $k \equiv k' \pmod n$ alors $g^{k'} = g^k$ du fait que $g^n = 1_G$ et grâce au lemme 3.3. On définit ainsi une application

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\longrightarrow G \\ \bar{k} &\longmapsto g^k. \end{aligned}$$

On vérifie facilement que f est un morphisme surjectif de groupes. Comme $\mathbb{Z}/n\mathbb{Z}$ et G sont finis de même cardinal, f est donc un isomorphisme de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans G . \square

Exemple 3.20. Nous avons vu que le groupe (U_n, \cdot) des racines n -èmes de l'unité est cyclique d'ordre n . Il est donc isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. D'après la démonstration du théorème, un tel isomorphisme correspond au choix d'un générateur de U_n , c'est-à-dire d'une racine primitive n -ème de l'unité. Par exemple

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z}, +) &\longrightarrow (U_n, \cdot) \\ \bar{k} &\longmapsto (e^{2i\pi/n})^k \end{aligned}$$

est un isomorphisme.

 Exercices pouvant être traités :

- exercice 3.8  
- exercice 3.12  
- exercice 3.14   

3.4 Classes à gauche et à droite modulo un sous-groupe

En nous inspirant de la construction de $\mathbb{Z}/n\mathbb{Z}$, on construit deux relations d'équivalence sur un groupe G à partir d'un sous-groupe donné.

Définition 3.21

Soit H un sous-groupe d'un groupe G . On définit sur G les relations suivantes : pour x, y dans G ,

$$x \sim_g y \iff x^{-1}y \in H$$

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

La relation \sim_g (resp. \sim_d) est appelée *congruence à gauche* (resp. *à droite*) modulo H .

Proposition 3.22

Les relations \sim_g et \sim_d sont des relations d'équivalence sur G .

Démonstration. Faisons la démonstration pour \sim_g , celle pour \sim_d étant similaire. La relation \sim_g est réflexive car $x \sim_g x$ puisque $x^{-1}x = 1_G$ appartient à H . Elle est symétrique car si $x^{-1}y \in H$ alors $(x^{-1}y)^{-1} = y^{-1}x$ appartient à H donc $y \sim_g x$. Enfin elle est transitive : si $x \sim_g y$ et $y \sim_g z$ alors $x^{-1}y \in H$ et $y^{-1}z \in H$ d'où $x^{-1}z = x^{-1}yy^{-1}z$ appartient à H , donc $x \sim_g z$. \square

Définition 3.23

L'ensemble des classes d'équivalence de \sim_g est noté G/H . L'ensemble de ses classes d'équivalence de \sim_d est noté $H \setminus G$.

On lit « G modulo H à gauche » pour G/H , et « G modulo H à droite » pour $H \setminus G$.

Dans certains cas, les ensembles quotients G/H et $H \setminus G$ sont munis d'une structure de groupe héritée de G , tout comme l'ensemble $\mathbb{Z}/n\mathbb{Z}$ hérite de l'addition de $(\mathbb{Z}, +)$: nous verrons au chapitre 4 à quelle condition sur le sous-groupe H c'est possible.

Le résultat suivant décrit les classes d'équivalence et justifie les terminologies « gauche » et « droite ».

Proposition 3.24

Soit $x \in G$. La classe de congruence à gauche modulo H de x est l'ensemble $xH = \{xy \mid y \in H\}$. La classe de congruence à droite modulo H de x est l'ensemble $Hx = \{yx \mid y \in H\}$.

Démonstration. On a

$$x \sim_g y \iff x^{-1}y \in H \iff y \in xH \quad \text{et}$$

$$x \sim_d y \iff y \sim_d x \iff yx^{-1} \in H \iff y \in Hx.$$

\square

- Exemple 3.25.**
1. La classe à gauche modulo H de l'élément neutre est $1_G H = \{1_G y \mid y \in H\} = \{y \mid y \in H\} = H$. De même on a $H 1_G = H$.
 2. Si $H = G$ alors $x \sim_g y$ pour tous x, y dans G . Il n'y a donc qu'une classe de congruence à gauche modulo H : $G/H = \{1_G G\} = \{G\}$, ensemble à un élément. De même on a $H \setminus G = \{G 1_G\} = \{G\}$.
 3. Si $H = \{1_G\}$ alors $x \sim_g y$ si et seulement si $x = y$. Donc $G/H = \{x\{1_G\} \mid x \in G\} = \{\{x\} \mid x \in G\}$, ensemble qui s'identifie à G . Même chose pour les classes à droite.
 4. Si G est abélien, les relations \sim_g et \sim_d sont les mêmes et les ensembles G/H et $H \setminus G$ égaux. C'est le cas pour $G = (\mathbb{Z}, +)$ et $H = n\mathbb{Z}$: on retrouve alors l'ensemble $\mathbb{Z}/n\mathbb{Z}$.
 5. Dans \mathcal{S}_3 , soit H le sous-groupe engendré par $t = (1, 2)$ c'est-à-dire $H = \{\text{id}, t\}$. On note $c = (1, 2, 3)$. Il y a trois classes à gauche qui sont :

$$\begin{aligned} \text{id}H &= H = \{\text{id}, t\} = \{\text{id}, (1, 2)\}, \\ cH &= \{c, ct\} = \{(1, 2, 3), (1, 3)\}, \\ c^2H &= \{c^2, c^2t\} = \{(1, 3, 2), (2, 3)\} \end{aligned}$$

et trois classes à droite qui sont :

$$\begin{aligned} H\text{id} &= H = \{\text{id}, (1, 2)\}, \\ Hc &= \{c, tc\} = \{(1, 2, 3), (2, 3)\}, \\ Hc^2 &= \{c^2, tc^2\} = \{(1, 3, 2), (1, 3)\}. \end{aligned}$$

Dans cet exemple, les classes Hc et cH ne sont pas les mêmes, de même pour c^2H et Hc^2 .

Soit $(x_i)_{i \in I}$ un système de représentants de G pour la relation d'équivalence \sim_g (c'est-à-dire $\{x_i \mid i \in I\}$ est une partie de G contenant un élément, et un seul, dans chaque classe d'équivalence pour \sim_g). On a alors la partition :

$$G = \bigsqcup_{i \in I} x_i H$$

où \bigsqcup désigne une réunion disjointe. De même si $(y_j)_{j \in J}$ est un système de représentants pour la relation \sim_d , on a :

$$G = \bigsqcup_{j \in J} H y_j.$$

On remarque que n'importe quelle classe d'équivalence xH ou Hy est en bijection avec H . De plus l'ensemble quotient G/H est en bijection avec l'ensemble quotient $H \setminus G$, la bijection étant donnée par $xH \mapsto Hx$.

Définition 3.26

Lorsque l'ensemble G/H est fini, son cardinal est appelé l'*indice de H*

— dans G . On le note $[G : H]$. C'est le nombre de classes à gauche modulo H .

Par les constatations précédentes, il y a autant de classes à droite que de classes à gauche : ainsi il revient au même de définir l'indice comme le nombre de classes à droite.

Nous en venons au résultat suivant, qui relie l'ordre d'un groupe à celui de ses sous-groupes, et qui est d'un usage constant en théorie des groupes.

Théorème 3.27 (Lagrange)

— Soit G un groupe fini et H un sous-groupe de G . Alors on a

$$\text{ord}(G) = [G : H] \text{ord}(H).$$

— En particulier :

1. l'ordre de H divise l'ordre de G ;
2. l'ordre de tout élément $x \in G$ divise l'ordre de G ; de plus $x^{\text{ord}(G)} = 1_G$.

Démonstration. Dans la partition $G = \bigsqcup_{i \in I} x_i H$, prenons les cardinaux de part et d'autre :

$$\text{ord}(G) = \sum_{i \in I} \text{Card}(x_i H) = \sum_{i \in I} \text{Card}(H) = \text{Card}(I) \cdot \text{ord}(H) = [G : H] \text{ord}(H).$$

Cette égalité d'entiers naturels entraîne que $\text{ord}(H)$ divise $\text{ord}(G)$. Si x est un élément de G , le sous-groupe $\langle x \rangle$, qui est d'ordre $\text{ord}(x)$, divise donc $\text{ord}(G)$. Pour la dernière affirmation, il reste à invoquer le fait que $\text{ord}(x) \mid \text{ord}(G)$ et le théorème 3.6. \square

- Exemple 3.28.**
1. L'indice de \mathcal{A}_n dans \mathcal{S}_n est $\frac{n!}{n!/2} = 2$, d'après la proposition 1.31.
 2. Dans l'exemple 3.25.5, H est d'indice 3 dans \mathcal{S}_3 .
 3. Si d divise l'ordre du groupe G , il n'existe pas toujours un élément d'ordre d dans G . Par exemple le groupe additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est d'ordre 4 mais ne possède aucun élément d'ordre 4 (voir l'exercice 3.11).

Le résultat suivant, dont la démonstration est élémentaire et à retenir, constitue un résultat de classification et témoigne de la force du théorème de Lagrange.

Corollaire 3.29

— Tout groupe fini d'ordre un nombre premier est cyclique.

Démonstration. Soit G un groupe d'ordre un nombre premier p . Comme $p > 1$, il existe un élément $x \in G$, $x \neq 1_G$. Étant donné que $x \neq 1_G$, l'ordre de x est > 1 . Or d'après le théorème de Lagrange, cet ordre divise p . Comme p est premier, cela entraîne que $\text{ord}(x) \in \{1, p\}$ d'où $\text{ord}(x) = p$. Par la proposition 3.17, on en déduit que G est cyclique. \square

Ainsi un groupe d'ordre premier p est toujours abélien et isomorphe à $(\mathbb{Z}/p\mathbb{Z}, +)$.

- Remarque 3.30.**
1. Sans hypothèse de primalité, le résultat est faux car il existe des groupes finis non cycliques, par exemple \mathcal{S}_3 .
 2. La réciproque du théorème est aussi fausse : le groupe $(\mathbb{Z}/4\mathbb{Z}, +)$ est cyclique (théorème 3.14) mais d'ordre 4, non premier.

☞ *Exercices pouvant être traités :*

- exercice 3.9 
- exercice 3.10 
- exercice 3.11 
- exercice 3.13  

Chapitre 4

Groupes quotients, théorème d'isomorphisme

Introduction

La notion de quotient existe pour les structures algébriques usuelles : espaces vectoriels, groupes, anneaux,... Ce chapitre aborde celle de groupe quotient : si H est un sous-groupe d'un groupe G , il s'agit de définir sur l'ensemble quotient G/H (ou $H\backslash G$) une structure de groupe héritée de G . Cela généralise la construction du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ à partir de $(\mathbb{Z}, +)$. La condition pour que cela soit possible, qui sera introduite, est que le sous-groupe H soit normal dans G . Ces concepts pouvant paraître un peu abstraits dans un premier temps, il est important de bien étudier les exemples et exercices proposés. Nous verrons le théorème de factorisation (aussi appelé passage au quotient) des morphismes, et le théorème d'isomorphisme. Nous terminerons par la notion de produit semi-direct, qui généralise celle de produit direct. Un exemple important issu de la géométrie sera donné avec le groupe diédral.

4.1 Sous-groupes normaux

On s'intéresse aux sous-groupes H d'un groupe G pour lesquels chaque classe à gauche xH coïncide avec la classe à droite Hx . On rappelle que xHx^{-1} désigne l'ensemble $\{xhx^{-1} \mid h \in H\}$.

Proposition 4.1

Soit H un sous-groupe d'un groupe G . Les assertions suivantes sont équivalentes :

1. pour tout $x \in G$, on a $xHx^{-1} = H$;
2. pour tout $x \in G$, on a $xHx^{-1} \subset H$;
3. pour tout $x \in G$, on a $xH = Hx$.

Démonstration. L'implication $1 \Rightarrow 2$ est immédiate.

Supposons 2 et soit $x \in G$: on a donc $xhx^{-1} \subset H$. Montrons l'autre inclusion. Pour tout $h \in H$, on peut écrire $h = x(x^{-1}hx)x^{-1}$. Or $x^{-1}hx$ appartient à $x^{-1}Hx$. D'après 2 appliqué à l'élément x^{-1} , $x^{-1}Hx$ est contenu dans H donc $x^{-1}hx \in H$. On conclut que $h \in xHx^{-1}$, d'où le point 1. On a ainsi prouvé $1 \iff 2$.

Constatons que l'associativité de la loi de G permet de modifier les parenthèses de la manière suivante : pour tous x, y dans G et A partie de G , on a

$$x(yA) = (xy)A, \quad A(xy) = (Ax)y, \quad \text{et} \quad (xA)y = x(Ay).$$

Si $xH = Hx$ on a alors $xHx^{-1} = (xH)x^{-1} = (Hx)x^{-1} = H(x^{-1}) = H1_G = H$. Enfin si $xHx^{-1} = H$ alors

$$xH = (xH)1_G = xH(x^{-1}x) = (xHx^{-1})x = Hx.$$

Cela prouve $1 \iff 3$. □

Définition 4.2

Un sous-groupe H est dit *normal dans G* (ou *distingué dans G*) s'il vérifie l'une des conditions équivalentes de la proposition 4.1. On note alors $H \triangleleft G$.

Remarque 4.3. D'après la proposition, H est normal dans G si et seulement si les relations \sim_g et \sim_d sont les mêmes. On parle alors de *congruence modulo H* (sans distinguer gauche ou droite) et on note $x \sim y$ pour signifier que x et y sont congrus modulo H .

Exemple 4.4. 1. Si G est un groupe, ses sous-groupes triviaux $\{1_G\}$ et G sont normaux dans G .

2. Le centre $Z(G)$ est normal dans G (démontrez-le).
3. Si G est un groupe abélien, tout sous-groupe de G est normal dans G .
4. Montrons que $\text{SL}_n(K)$ est normal dans $\text{GL}_n(K)$ en utilisant la condition 2. Pour toutes matrices $M \in \text{GL}_n(K)$ et $N \in \text{SL}_n(K)$, on a :

$$\det(MNM^{-1}) = \det(M) \det(N) \det(M)^{-1} = \det(N) = 1$$

d'où $MNM^{-1} \in \text{SL}_n(K)$: cela prouve que $M\text{SL}_n(K)M^{-1} \subset \text{SL}_n(K)$.

5. On considère $K = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\}$. On montre facilement que K est

un sous-groupe de $\text{GL}_2(\mathbb{R})$. Posons $x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R})$. Alors on a

$$x^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}. \text{ Pour } a \in \mathbb{R} \text{ on a } x \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} x^{-1} = \begin{pmatrix} 1-a & a \\ -a & a+1 \end{pmatrix}. \text{ Cet}$$

élément n'appartenant pas à K en général, K n'est pas normal dans $\text{GL}_2(\mathbb{R})$.

6. Si H est un sous-groupe de G alors H est un sous-groupe normal de son normalisateur $N_G(H)$ (revoir l'exemple 2.30 pour sa définition). On peut montrer que $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal.

Attention, *être normal n'est pas une relation transitive* : si K est un sous-groupe normal de H et H un sous-groupe normal de G , on n'a pas forcément K normal dans G . Un contre-exemple sera donné dans l'exercice 4.7.

Le résultat suivant est classique et sa démonstration est à retenir.

Proposition 4.5

Si H est un sous-groupe d'indice 2 d'un groupe G alors H est normal dans G .

Démonstration. Si H est d'indice 2, on a une partition de G en deux classes à gauche : $G = H \sqcup xH$ quelque soit x élément de G n'appartenant pas à H . De même on a une partition de G en deux classes à droite : $G = H \sqcup Hx$ pour ce même x . On en déduit $xH = Hx$. L'autre classe à gauche $H = 1_G H$ coïncidant aussi avec la classe à droite $H = H1_G$, le sous-groupe H est normal dans G . \square

Proposition 4.6

Soient G et G' deux groupes et soit $f : G \rightarrow G'$ un morphisme de groupes.

1. Si $H' \triangleleft G'$, alors $f^{-1}(H') \triangleleft G$. En particulier $\text{Ker } f \triangleleft G$.
2. Si $H \triangleleft G$ et si f est surjective alors $f(H) \triangleleft G'$.

Démonstration. 1. Soit $H' \triangleleft G'$. On sait déjà que $f^{-1}(H')$ est un sous-groupe de G . Montrons qu'il est normal dans G . Soit $x \in G$, on veut montrer que $xf^{-1}(H')x^{-1} \subset f^{-1}(H')$. Soit $y \in f^{-1}(H')$. Il faut montrer que $xyx^{-1} \in f^{-1}(H')$ c'est à dire que $f(xyx^{-1}) \in H'$. Or comme f est un morphisme de groupes, on a $f(xyx^{-1}) = f(x)f(y)f(x)^{-1}$. Comme $f(y) \in H'$ et que H' est normal dans G' , on conclut que $f(x)f(y)f(x)^{-1} \in H'$. Donc $f^{-1}(H')$ est un sous-groupe normal de G .

2. Soit $H \triangleleft G$ et supposons f surjective. On sait déjà que $f(H)$ est un sous-groupe de G' . Montrons qu'il est normal dans G' . Soit $x \in G'$. On veut montrer $xf(H)x^{-1} \subset f(H)$. Comme f est surjective, il existe $z \in G$ tel que $f(z) = x$. Alors on a $f(z^{-1}) = f(z)^{-1} = x^{-1}$. Soit $y \in H$, on a $xf(y)x^{-1} = f(zyz^{-1})$ car f est un morphisme de groupes. Comme H est normal dans G , on sait que $zyz^{-1} \in H$. Il suit $xf(y)x^{-1} \in f(H)$. Donc $f(H)$ est un sous-groupe normal de G' . \square

Exemple 4.7. 1. On retrouve le fait que le sous-groupe $\text{SL}_n(K)$ est normal dans $\text{GL}_n(K)$, comme noyau du morphisme de groupes $\det : \text{GL}_n(K) \rightarrow K^*$.

2. Le sous-groupe alterné \mathcal{A}_n est normal dans \mathcal{S}_n car c'est le noyau du morphisme signature $\varepsilon : \mathcal{S}_n \rightarrow \{\pm 1\}$.

 Exercices pouvant être traités :

- exercice 4.1 
- exercice 4.2 
- exercice 4.3  

4.2 Groupe quotient, théorème d'isomorphisme

Soit H un sous-groupe d'un groupe G . On se demande à quelle condition l'ensemble quotient G/H peut être muni d'une loi de groupe héritée de G . Précisons ce que cela signifie. Considérons la surjection canonique

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ x &\longmapsto xH. \end{aligned}$$

qui à x associe sa classe à gauche $\bar{x} = xH$. Le groupe G étant noté multiplicativement, on voudrait pouvoir définir une loi $*$ sur G/H telle que $xH * yH = xyH$ i.e.

$$\forall (x, y) \in G \times G, \quad \bar{x} * \bar{y} = \overline{xy}$$

c'est-à-dire telle que l'application π soit un morphisme de groupes.

Théorème 4.8

Soient G un groupe et H un sous-groupe *normal* dans G . Pour tous $(x, y) \in G \times G$, posons

$$\forall (x, y) \in G \times G, \quad \bar{x} * \bar{y} = \overline{xy}.$$

Alors $*$ est une loi interne sur G/H . De plus $(G/H, *)$ est un groupe, appelé le *groupe quotient* de G par H . L'application $\pi : G \rightarrow G/H$ est un morphisme de groupes surjectif et de noyau H .

Le groupe quotient G/H se lit « G sur H » ou « G modulo H ».

Remarque 4.9. Rappelons que comme H est normal dans G , les ensembles quotients G/H et $G \setminus H$ sont identiques et donc tous deux munis de la loi de groupe $*$.

Démonstration. Pour $(x, y) \in G \times G$, notons $\bar{x} = xH$ et $\bar{y} = yH$ leurs classes respectives dans G/H . Montrons que la formule $\bar{x} * \bar{y} = \overline{xy}$ définit sans ambiguïté une application

$$\begin{aligned} * : G/H \times G/H &\longrightarrow G/H \\ (\bar{x}, \bar{y}) &\longmapsto \overline{xy}. \end{aligned}$$

Il s'agit de montrer que si $x' \in \bar{x}$ et $y' \in \bar{y}$ alors $\overline{x'y'} = \overline{xy}$ c'est-à-dire que le résultat ne dépend pas des choix de représentants faits dans chaque classe modulo H . Écrivons $x'y'(xy)^{-1} = x'y'y^{-1}x^{-1}$. Or on a $y'y^{-1} \in H$ car $y \sim y'$; de plus $x'H = xH$ car $x' \sim x$. On en déduit $x'y'y^{-1}x^{-1} \in x'Hx^{-1} = xHx^{-1} = H$ par normalité de H . Ainsi la loi $*$ est définie et interne sur G/H .

Cette loi est associative car elle hérite cette propriété de la loi de G . Elle a un élément neutre, qui est $\overline{1_G} = H$, car $\overline{1_G} * \bar{x} = \overline{1_G x} = \bar{x} = \bar{x} \overline{1_G}$ pour tout \bar{x} dans G/H . L'inverse de $\bar{x} = xH$ est $\overline{x^{-1}} = x^{-1}H$, qu'on note aussi \bar{x}^{-1} , car

$$\bar{x} * \overline{x^{-1}} = \overline{xx^{-1}} = \overline{1_G} = \overline{x^{-1}} * \bar{x}.$$

Ainsi G/H muni de la loi $*$ est un groupe.

L'application $\pi : G \rightarrow G/H$ est un morphisme, par définition de la loi $*$; elle est surjective et de noyau H car pour tout $x \in G$, on a $\bar{x} = \overline{1_G} \iff x \sim 1_G \iff x \in H$. \square

Remarque 4.10. 1. Si le groupe G est abélien, le sous-groupe H est toujours normal dans G et de plus le groupe quotient $(G/H, *)$ est abélien.
2. Lorsque H est normal dans G , on peut montrer que la structure de groupe $(G/H, *)$ du théorème est la seule à faire de l'application $\pi : G \rightarrow G/H$ un morphisme de groupes. Inversement, on peut montrer que si G/H possède une structure de groupe faisant de π un morphisme de groupes, alors nécessairement H est normal dans G .

Pour simplifier les notations, on notera encore multiplicativement la loi de groupe sur G/H , autrement dit on écrira :

$$\bar{x} * \bar{y} = \overline{x \cdot y}.$$

Exemple 4.11. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ étudié au chapitre 3 est le groupe quotient du groupe abélien $(\mathbb{Z}, +)$ par son sous-groupe (normal) $n\mathbb{Z}$.

Rappelons que, lorsque S est un ensemble, afin de définir une application $f : G/H \rightarrow S$, on doit associer à chaque élément de G/H un élément de S défini sans ambiguïté : si $\bar{x} = \bar{y}$ dans G/H on doit s'assurer que $f(x) = f(y)$, autrement dit que f est constante sur chaque classe de congruence. Le théorème suivant donne un critère pratique pour définir une telle application à partir d'un morphisme de groupes, sans avoir à écrire cette vérification.

Théorème 4.12

Soient G et G' deux groupes et $f : G \rightarrow G'$ un morphisme de groupes. Soit $H \triangleleft G$ un sous-groupe *normal* de G tel que $H \subset \text{Ker } f$. Alors il existe un unique morphisme de groupes $\bar{f} : G/H \rightarrow G'$ tel que $\bar{f} \circ \pi = f$ où $\pi : G \rightarrow G/H$ est la surjection canonique.

On représente la conclusion en disant que le diagramme suivant est commutatif :

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \downarrow & \nearrow \bar{f} & \\ G/H & & \end{array}$$

et on dit que le morphisme f *passse au quotient*, ou *se factorise*, par H . Noter que la condition $\bar{f} \circ \pi = f$ signifie simplement que

$$\forall x \in G, \quad \bar{f}(\bar{x}) = f(x). \quad (4.1)$$

En particulier les morphismes f et \bar{f} ont même image dans G' .

Remarque 4.13. Ce théorème est une « machine » qui prend en entrée un morphisme de groupes $f : G \rightarrow G'$ et, sous les bonnes hypothèses, et retourne un morphisme de groupes $G/H \rightarrow G'$ induit par f . Dès qu'on vous demande de construire un tel morphisme dans un exercice, il faut systématiquement penser à utiliser le théorème de factorisation !

Démonstration. L'unicité vient du fait que la relation (4.1) détermine de manière unique l'application \bar{f} à partir de la donnée de f .

Passons à l'existence. Si $\bar{x} = \bar{y}$ dans G/H alors $xy^{-1} \in H$. Comme $H \subset \text{Ker } f$, on en déduit $f(x)f(y)^{-1} = f(xy^{-1}) = 1_{G'}$ donc $f(x) = f(y)$. On peut ainsi définir l'application suivante :

$$\begin{aligned} \bar{f} : G/H &\longrightarrow G' \\ \bar{x} &\longmapsto f(x). \end{aligned}$$

Elle vérifie par construction $f(x) = \bar{f}(\bar{x})$ pour tout $x \in G$, c'est-à-dire $\bar{f} \circ \pi = f$. Il reste à montrer que \bar{f} est un morphisme de groupes : si $x, y \in G$ on veut montrer que $\bar{f}(\bar{x} \cdot \bar{y}) = \bar{f}(\bar{x})\bar{f}(\bar{y})$. Par définition on a $\bar{x} \cdot \bar{y} = \overline{xy}$ donc $\bar{f}(\bar{x} \cdot \bar{y}) = f(xy) = f(x)f(y) = \bar{f}(\bar{x})\bar{f}(\bar{y})$. Ainsi \bar{f} est bien un morphisme de groupes. \square

Corollaire 4.14 (Théorème d'isomorphisme)

Plaçons-nous dans la situation du théorème 4.12 : soient $f : G \rightarrow G'$ un morphisme de groupes, H un sous-groupe normal de G tel que $H \subset \text{Ker } f$ et $\bar{f} : G/H \rightarrow G'$ le morphisme de groupes obtenu par passage au quotient de f . Alors :

1. le morphisme \bar{f} est surjectif si et seulement si f est surjectif ;
2. le morphisme \bar{f} est injectif si et seulement si $H = \text{Ker } f$.

En particulier, tout morphisme de groupes $f : G \rightarrow G'$ induit un isomorphisme de groupes $G/\text{Ker } f \simeq \text{Im } f$.

Démonstration. 1. Cela vient du fait que f et \bar{f} ont même image dans G' .
2. Le noyau de $\bar{f} : G/H \rightarrow G'$ est

$$\text{Ker } \bar{f} = \{\bar{x} \in G/H \mid f(x) = 1_{G'}\} = \{\bar{x} \in G/H \mid x \in \text{Ker } f\} = \pi(\text{Ker } f).$$

Supposons \bar{f} injectif. Soit $x \in \text{Ker } f$. Alors par ce qui précède, $\bar{x} \in \text{Ker } \bar{f}$ donc $\bar{x} = 1_{G/H}$ c'est-à-dire $x \in H$. Cela prouve que $\text{Ker } f \subset H$. Comme H est supposé contenu dans $\text{Ker } f$, on conclut que $H = \text{Ker } f$. Réciproquement, supposons que $H = \text{Ker } f$. Alors $\text{Ker } \bar{f} = \{\bar{x} \in G/H \mid x \in H\} = \{1_{G/H}\}$, donc \bar{f} est injectif.

Soit maintenant $f : G \rightarrow G'$ un morphisme de groupes. Sa corestriction à $\text{Im } f$ donne un morphisme de groupes, encore noté f , de G dans $\text{Im } f$. On applique ce qui précède au sous-groupe $H = \text{Ker } f$, qui est normal dans G : f induit un morphisme de groupes $\bar{f} : G/\text{Ker } f \rightarrow \text{Im } f$ qui est à la fois injectif et surjectif, donc un isomorphisme. \square

Exemple 4.15. 1. Nous savons que le morphisme de groupes $\det : \text{GL}_n(K) \rightarrow K^*$ est de noyau $\text{SL}_n(K)$ et surjectif. Par factorisation, on en déduit un isomorphisme de groupes $\text{GL}_n(K)/\text{SL}_n(K) \simeq (K^*, \cdot)$.
2. Lorsque $n \geq 2$, le morphisme signature $\varepsilon : \mathcal{S}_n \rightarrow \{\pm 1\}$ est surjectif (voir corollaire 1.28) et de noyau le sous-groupe alterné \mathcal{A}_n . Par factorisation, on en déduit un isomorphisme de groupes $\mathcal{S}_n/\mathcal{A}_n \simeq \{\pm 1, \cdot\}$.

3. Soit $U = \{z \in \mathbb{C}, |z| = 1\}$ l'ensemble des nombres complexes de module 1. Alors (U, \cdot) est un groupe, et même un sous-groupe de (\mathbb{C}^*, \cdot) . L'application module

$$\begin{aligned} (\mathbb{C}^*, \cdot) &\longrightarrow (\mathbb{R}^{+*}, \cdot) \\ z &\longmapsto |z| \end{aligned}$$

est un morphisme de groupes car pour tous z_1, z_2 dans \mathbb{C}^* on a $|z_1 z_2| = |z_1| |z_2|$. Il est surjectif et de noyau $\{z \in \mathbb{C}^*, |z| = 1\} = U$. Par factorisation, on en déduit un isomorphisme de groupes $\mathbb{C}^*/U \simeq (\mathbb{R}^{+*}, \cdot)$.

Définition 4.16

Un groupe G est dit *simple* s'il n'a pas de sous-groupe normal non trivial, c'est-à-dire distinct de $\{1_G\}$ et de G .

Remarque 4.17. Une erreur fréquente est d'oublier *normal* dans la définition précédente. Sans cette condition, la notion dégagée ne serait pas nouvelle (voir l'exercice 3.12).

Exemple 4.18. 1. Tout groupe fini d'ordre premier p est simple. En effet par le théorème de Lagrange, ses sous-groupes sont d'ordre 1 ou p , c'est-à-dire $\{1_G\}$ ou le groupe tout entier.

2. On peut démontrer que le groupe alterné \mathcal{A}_n est simple si $n \geq 5$. Voir l'exercice 4.5 pour un autre cas.

Les groupes simples jouent un rôle important dans l'étude générale des groupes. Étant donné un groupe fini G , si on dispose d'un sous-groupe normal H non trivial, on espère pouvoir ramener l'étude de G à celles de H et de G/H , qui sont de plus petit cardinal que G (cette philosophie porte le nom de *dévisage des groupes*). Si G/H n'est pas simple, il possède un sous-groupe normal non trivial et on peut alors former un autre groupe quotient. On continue ainsi jusqu'à trouver un groupe simple G' et espérer récupérer des propriétés de G à partir de G' . Pour cette raison, les groupes finis simples peuvent être perçus comme les composantes élémentaires de tous les groupes finis, de la même façon que tous les nombres entiers peuvent être factorisés en produit de nombres premiers.

La classification des groupes finis simples a été achevée en 1982 et constitue un travail colossal mené par une centaine de chercheurs dans la deuxième moitié du vingtième siècle. Cette classification comporte : les groupes d'ordre premier, les groupes alternés \mathcal{A}_n avec $n \geq 5$, les groupes simples dits de Lie, et 26 groupes simples dits sporadiques qui échappent aux familles précédentes. Le plus grand groupe simple sporadique est appelé le Monstre et il est d'ordre $2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$ (environ 8×10^{53}).

☞ *Exercices pouvant être traités :*

- exercice 4.4 
- exercice 4.5  
- exercice 4.8  

4.3 Sous-groupes d'un groupe quotient

Lorsque H est normal dans G , nous avons muni l'ensemble G/H d'une structure de groupe. Nous cherchons maintenant à en décrire ses sous-groupes à partir ceux de G .

Théorème 4.19

Soient G un groupe et H un sous-groupe normal dans G . Notons $\pi : G \rightarrow G/H$ la surjection canonique. L'application φ (lettre grecque phi) définie par :

$$\varphi : \left\{ \begin{array}{l} \text{Sous-groupes de } G \text{ contenant } H \\ K \end{array} \right\} \begin{array}{l} \longrightarrow \\ \longmapsto \end{array} \left\{ \begin{array}{l} \text{Sous-groupes de } G/H \\ \pi(K) \end{array} \right\}$$

est une bijection.

Démonstration. Comme K est un sous-groupe de G et π est un morphisme de groupes, $\pi(K)$ est un sous-groupe de G/H d'après la proposition 2.26. L'application φ est donc définie.

Montrons l'injectivité de φ . Soient K, K' deux sous-groupes de G contenant H tels que $\pi(K) = \pi(K')$. Montrons que $K = K'$. Soit $x \in K$. Alors $\pi(x)$ appartient à $\pi(K)$ et à $\pi(K')$. Il existe donc $x' \in K'$ tel que $\pi(x) = \pi(x')$ c'est-à-dire $x \equiv x' \pmod{H}$ c'est-à-dire $xx'^{-1} \in H$. Puisque $H \subset K'$, on a $xx'^{-1} \in K'$ d'où $x \in K'$ puisque $x' \in K'$. Ainsi on a $K \subset K'$. Par symétrie on obtient $K' \subset K$ d'où l'injectivité de φ .

Il reste à montrer que φ est surjective. Soit J un sous-groupe de G/H . Notons $K = \pi^{-1}(J)$, l'image réciproque de J par π , et montrons que K est un sous-groupe de G contenant H et qui satisfait $\pi(K) = J$. On sait déjà que K est un sous-groupe de G par la proposition 2.26. Puisque l'élément neutre de G/H est la classe H , on a $H \subset K$. Enfin comme π est surjective, on a $\pi(\pi^{-1}(B)) = B$ pour toute partie B de G/H . En particulier, $\pi(K)$ est égal à J . L'application est surjective, donc bijective. \square

Si K est un sous-groupe de G contenant H , le sous-groupe $\pi(K)$ de G/H est souvent noté K/H .

Remarque 4.20. 1. La bijection réciproque de φ est $J \mapsto \pi^{-1}(J)$, qui associe à tout sous-groupe J de G/H son image réciproque par π .

2. L'application φ n'est pas un isomorphisme de groupes, ni même un morphisme : ses ensembles de départ et d'arrivée ne sont pas munis d'une structure naturelle de groupe.

Exemple 4.21. Rappelons que les sous-groupes de $(\mathbb{Z}, +)$ sont les $m\mathbb{Z}$ où $m \in \mathbb{N}$ (exercice 2.12). D'après la bijection φ , les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont donc les $m\mathbb{Z}/n\mathbb{Z}$ où $m \in \mathbb{N}$ est tel que $n\mathbb{Z} \subset m\mathbb{Z}$ c'est-à-dire tel que m divise n . Par exemple les sous-groupes de $(\mathbb{Z}/8\mathbb{Z}, +)$ sont

$$\mathbb{Z}/8\mathbb{Z}, \quad 2\mathbb{Z}/8\mathbb{Z}, \quad 4\mathbb{Z}/8\mathbb{Z}, \quad 8\mathbb{Z}/8\mathbb{Z}(= \{0\}).$$

L'énoncé suivant donne une condition nécessaire et suffisante pour qu'un sous-groupe de G/H soit normal.

Proposition 4.22

Soient G un groupe et H un sous-groupe normal de G . Soit K un sous-groupe de G contenant H . Alors le sous-groupe K/H est normal dans G/H si et seulement si K est normal dans G .

Démonstration. Soit K un sous-groupe de G qui contient H . Supposons que le sous-groupe K/H est normal dans G/H . Du fait que $H \subset K$, l'image réciproque $\pi^{-1}(K/H)$ est K . Donc K est normal dans G d'après la proposition 4.6. Réciproquement supposons K normal dans G . Alors comme π est surjectif, $\pi(K)$ est normal dans G/H d'après la proposition 4.6. \square

En combinant le théorème 4.19 et la proposition 4.22, on obtient une bijection entre d'une part l'ensemble des sous-groupes de G qui contiennent H et qui sont normaux dans G , et d'autre part l'ensemble des sous-groupes normaux de G/H .

☞ *Exercices pouvant être traités :*

- exercice 4.9 
- exercice 4.10 

4.4 Produit semi-direct

4.4.1 Retour sur le produit direct

Avec la notion de sous-groupe normal, le critère du théorème 2.44 se réécrit de la manière suivante dans le cas de deux sous-groupes.

Théorème 4.23

Soient G un groupe et H_1, H_2 deux sous-groupes de G vérifiant les conditions suivantes :

1. $H_1 \triangleleft G$ et $H_2 \triangleleft G$;
2. $H_1 \cap H_2 = \{1_G\}$;
3. $G = H_1 H_2$.

Alors $G \simeq H_1 \times H_2$.

Démonstration. Pour montrer l'équivalence de cet énoncé avec le théorème 2.44, il suffit de montrer que si les conditions $H_1 \cap H_2 = \{1_G\}$ et $G = H_1 H_2$ sont satisfaites, alors

$$(\forall h_1 \in H_1, \forall h_2 \in H_2, h_1 h_2 = h_2 h_1) \iff (H_1 \triangleleft G \text{ et } H_2 \triangleleft G).$$

(\Rightarrow) Supposons que pour tous $h_1 \in H_1$ et $h_2 \in H_2$ on a $h_1 h_2 = h_2 h_1$. Alors H_1 est un sous-groupe normal de G . En effet, si $g \in G$ alors il existe $h'_1 \in H_1$ et $h'_2 \in H_2$ tels que $g = h'_1 h'_2$. On obtient pour tout $h_1 \in H_1$,

$$gh_1 g^{-1} = h'_1 h'_2 h_1 h'_2{}^{-1} h_1{}^{-1} = h'_1 h'_2 h_2{}^{-1} h_1 h_1{}^{-1} = h'_1 h_1 h_1{}^{-1}.$$

Ce dernier élément appartient à H_1 . On a donc $gH_1g^{-1} \subset H_1$. Ainsi H_1 est un sous-groupe normal de G . On procède de même pour H_2 .

(\Leftarrow) Supposons que H_1 et H_2 soient normaux dans G . Soient $h_1 \in H_1$ et $h_2 \in H_2$. Considérons l'élément $h_1^{-1}h_2^{-1}h_1h_2$ de G . On a :

- d'une part, $h_2 \in H_2$ et $h_1^{-1}h_2^{-1}h_1 \in H_2$ car $H_2 \triangleleft G$ donc $h_1^{-1}h_2^{-1}h_1h_2 \in H_2$;
- d'autre part, $h_1^{-1} \in H_1$ et $h_2^{-1}h_1h_2 \in H_1$ car $H_1 \triangleleft G$ donc $h_1^{-1}h_2^{-1}h_1h_2 \in H_1$.

Ainsi on $h_1^{-1}h_2^{-1}h_1h_2 \in H_1 \cap H_2$. Comme $H_1 \cap H_2 = \{1_G\}$, on obtient $h_1h_2 = h_2h_1$. \square

4.4.2 Produit semi-direct de deux sous-groupes

La notion de produit semi-direct généralise celle de produit direct, en ne demandant qu'au premier sous-groupe d'être normal.

Définition 4.24

Soient G un groupe et H_1, H_2 deux sous-groupes de G . On dit que G est *produit semi-direct de H_1 par H_2* si les conditions suivantes sont vérifiées :

1. $H_1 \triangleleft G$;
2. $H_1 \cap H_2 = \{1_G\}$;
3. $G = H_1H_2$.

Dans ce cas on note $G = H_1 \rtimes H_2$.

On prendra garde à ce que H_1 et H_2 ne jouent pas des rôles symétriques. On parle aussi de *produit semi-direct interne* de H_1 par H_2 .

En particulier, le produit semi-direct $G = H_1 \rtimes H_2$ est direct ($G \simeq H_1 \times H_2$) si et seulement si $H_2 \triangleleft G$.

Exemple 4.25. Si $n \geq 2$, montrons que le groupe symétrique \mathcal{S}_n est produit semi-direct de \mathcal{A}_n par H où $H = \langle \tau \rangle$ désigne le sous-groupe engendré par une transposition τ de \mathcal{S}_n .

- On a déjà vu que le sous-groupe \mathcal{A}_n est normal dans \mathcal{S}_n .
- On a $\mathcal{A}_n \cap H = \{\text{id}\}$ car $\tau \notin \mathcal{A}_n$ (sa signature est -1).
- Montrons que $\mathcal{S}_n = \mathcal{A}_nH$. En effet, toute permutation σ de \mathcal{S}_n s'écrit :

$$\sigma = \begin{cases} \sigma \cdot \text{id} \in \mathcal{A}_nH & \text{si } \sigma \text{ est paire ;} \\ (\sigma\tau) \cdot \tau \in \mathcal{A}_nH & \text{si } \sigma \text{ est impaire.} \end{cases}$$

Ainsi $\mathcal{S}_n = \mathcal{A}_n \rtimes H$.

Proposition 4.26

Supposons que $G = H_1 \rtimes H_2$ avec H_1, H_2 sous-groupes de G .

1. Pour tout $g \in G$ il existe un unique couple $(h_1, h_2) \in H_1 \times H_2$ tel que $g = h_1h_2$.
2. L'effet de la loi de G sur cette décomposition est comme suit : si

$g = h_1 h_2$ et $g' = h'_1 h'_2$ alors la décomposition de gg' est

$$gg' = (h_1 h_2 h'_1 h_2^{-1})(h_2 h'_2)$$

avec $h_1 h_2 h'_1 h_2^{-1} \in H_1$ et $h_2 h'_2 \in H_2$.

Démonstration. 1. Cela résulte des conditions $H_1 \cap H_2 = \{1_G\}$ et $G = H_1 H_2$, comme dans la preuve du théorème 2.44.

2. L'égalité entre les deux membres de la formule est claire. De plus comme $H_1 \triangleleft G$, on a $h_2 h'_1 h_2^{-1} \in H_1$ d'où $h_1 h_2 h'_1 h_2^{-1} \in H_1$. Par ailleurs $h_2 h'_2$ appartient à H_2 . Donc la formule donne la décomposition en produit d'un élément de H_1 et d'un élément de H_2 . □

D'après ces constatations, et en suivant le principe de la démonstration du théorème 2.44, on peut montrer que le produit semi-direct interne $G = H_1 \rtimes H_2$ est isomorphe à une structure de groupe particulière sur le produit cartésien $H_1 \times H_2$: la loi n'y est pas généralement celle du produit direct mais une variante « tordue » de celle-ci, énoncée dans le théorème suivant. Cela justifie l'appellation de produit semi-direct.

Proposition 4.27

Soit $G = H_1 \rtimes H_2$ avec H_1, H_2 sous-groupes de G . Notons G' le produit cartésien $H_1 \times H_2$. Il est muni de la loi interne suivante :

$$(h_1, h_2) * (h'_1, h'_2) = (h_1 h_2 h'_1 h_2^{-1}, h_2 h'_2).$$

Alors $(G', *)$ est un groupe, qui est isomorphe au produit semi-direct G par

$$\begin{aligned} G' &\longrightarrow G \\ (h_1, h_2) &\longmapsto h_1 h_2. \end{aligned}$$

Démonstration. Laissez en exercice : vérifier que la loi $*$ muni G' d'une structure de groupe puis, pour l'isomorphisme, s'inspirer de la démonstration du théorème 2.44. □

Le groupe $(G', *)$ de ce dernier énoncé est un cas particulier de produit semi-direct externe, que nous n'aborderons pas dans ce cours.

☞ *Exercices pouvant être traités :*

- exercice 4.6 
- exercice 4.13 

4.5 Groupe diédral

Bien qu'il puisse être défini de manière abstraite, ce groupe a une origine géométrique. Il constitue un nouvel exemple de produit semi-direct.

Proposition 4.28

Soit n un entier naturel ≥ 3 . Soit G un groupe possédant deux éléments a et b qui satisfont les conditions suivantes :

1. $G = \langle a, b \rangle$;
2. a est d'ordre n ;
3. b est d'ordre 2 ;
4. $baba = 1_G$.

Alors

1. $G = \langle a \rangle \rtimes \langle b \rangle$;
2. G est d'ordre $2n$;
3. Tout groupe qui possède deux éléments satisfaisant les mêmes conditions que a et b est isomorphe à G .

Démonstration. Commençons par montrer que $b \notin \langle a \rangle$. En effet si $b \in \langle a \rangle$ alors b commute à a donc $1_G = baba = b^2a^2 = 1_Ga^2 = a^2$, ce que contredit le fait que $\text{ord}(a) = n \geq 3$.

1. Une récurrence directe donne $ba^k = a^{-k}b$ pour tout $k \in \mathbb{Z}$. On en déduit que tout élément de $G = \langle a, b \rangle$ s'écrit $a^i b^j$ avec $i \in \mathbb{Z}$ et $j \in \mathbb{Z}$. Grâce aux ordres de a et b , on peut même supposer que $i \in \{0, \dots, n-1\}$ et $j \in \{0, 1\}$. En particulier on a $G = \langle a \rangle \langle b \rangle$. De plus $\langle a \rangle \cap \langle b \rangle = \{1_G\}$ car $b \notin \langle a \rangle$. Enfin comme $ba^k b^{-1} = a^{-k}$ et G est engendré par a et b , on peut vérifier par un calcul que $\langle a \rangle$ est normal dans G . Ainsi $G = \langle a \rangle \rtimes \langle b \rangle$.
2. En utilisant la relation $ba^k = a^{-k}b$, on voit que tout élément de G est l'un des éléments

$$1_G, a, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}$$

et qu'ils sont distincts deux à deux. Cela prouve que G est d'ordre $2n$.

3. Les raisonnements précédents montrent que la donnée de a et b vérifiant les quatre conditions détermine de manière unique la loi sur le groupe c'est-à-dire sa table de Cayley. Donc tout groupe qui possède deux éléments satisfaisant les mêmes conditions que a et b est isomorphe à G .

□

Définition 4.29

Un groupe G vérifiant les conditions de la proposition 4.28 est appelé un *groupe diédral d'ordre $2n$* .

À n fixé, tous les groupes diédraux d'ordre $2n$ sont donc isomorphes. Par abus, on dit souvent « le » groupe diédral, au lieu d'un groupe diédral, et on le note D_n (attention, certains auteurs le notent D_{2n}).

On retiendra la relation suivante dans D_n :

$$\forall k \in \mathbb{Z}, \quad ba^k = a^{-k}b$$

qui permet d'en manipuler les éléments.

Exemple 4.30. Le groupe symétrique \mathcal{S}_3 est diédral d'ordre 6 : prendre $a = (1, 2, 3)$ et $b = (1, 2)$ (voir l'exercice 4.11).

Proposition 4.31

Dans le plan affine euclidien \mathcal{E} , on considère un polygone régulier \mathcal{P}_n à n côtés avec $n \geq 3$. Le groupe des isométries de \mathcal{E} laissant \mathcal{P}_n invariant est un groupe diédral d'ordre $2n$.

Précisons ce que cet énoncé entend par « invariant » : il s'agit des isométries f de \mathcal{E} satisfaisant $f(\mathcal{P}_n) = \mathcal{P}_n$.

Démonstration. Nous avons besoin de quelques connaissances de géométrie affine, pour lesquelles nous renvoyons à l'unité *Structures affines*. Notons O le centre du polygone \mathcal{P}_n et r la rotation de centre O et de mesure d'angle $2\pi/n$. Soit $\{A_1, \dots, A_n\}$ l'ensemble des sommets de \mathcal{P}_n avec la convention que $A_{j+1} = r(A_j)$ pour tout $j \in \{1, \dots, n-1\}$ et $A_1 = r(A_n)$. Notons G l'ensemble des isométries u de \mathcal{E} telles que $u(\mathcal{P}_n) = \mathcal{P}_n$. On vérifie facilement que G est un sous-groupe de celui des isométries du plan. Soit s la symétrie orthogonale par rapport à la droite (OA_1) . Il est clair que r est d'ordre n et s d'ordre 2 dans G . D'après l'unité *Structures affines*, sr est une symétrie donc elle est d'ordre 2 d'où $sr sr = \text{id}$. Montrons enfin que G est engendré par r et s . Soit $g \in G$. Si $g(A_1) = A_1$ alors g fixe la droite (OA_1) : on en déduit que g est l'identité ou la symétrie orthogonale s . Si $g(A_1) = A_k$ pour un certain $k \neq 1$ on a $(r^{1-k} \circ g)(A_1) = A_1$ d'où $g = r^{k-1} \circ s$ ou bien $g = r^{k-1}$. Ainsi $G = \langle r, s \rangle$. On en déduit que G est un groupe diédral d'ordre $2n$ d'après la proposition 4.28. \square

Notons r la rotation de centre O et de mesure d'angle $2\pi/n$ (elle est d'ordre n dans D_n) et s la symétrie orthogonale s d'axe la droite (OA_1) (elle est d'ordre 2 dans D_n). Les éléments du groupe géométrique diédral D_n sont les suivants :

- les n rotations r^k de centre O et de mesure d'angle $2k\pi/n$ pour $k \in \{0, \dots, n-1\}$;
- les n symétries orthogonales d'axe la droite passant par O et par un sommet ou un milieu d'arête ; ce sont les $sr^k (= r^{-k}s)$ pour $k \in \{0, \dots, n-1\}$.

De plus, d'après la proposition 4.28, D_n est le produit semi-direct $\langle r \rangle \rtimes \langle s \rangle$.

Exemple 4.32. Les illustrations suivantes représentent les polygones réguliers avec les axes des symétries orthogonales pour $n = 4$ (carré) et $n = 5$ (pentagone régulier). Si n est pair, les axes relient deux sommets ou deux milieux d'arêtes opposé(e)s, tandis que pour n impair ce sont les médiatrices des côtés.



Soit s la symétrie orthogonale par rapport à la droite (OI) . Si r désigne la rotation de centre O et de mesure d'angle $2\pi/4$, on a

$$D_4 = \{\text{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}.$$

Si r désigne la rotation de centre O et de mesure d'angle $2\pi/5$, on a

$$D_5 = \{\text{id}, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}.$$

Les lecteurs sont invités à identifier ces éléments comme isométries des figures précédentes.

☞ *Exercices pouvant être traités :*

- exercice 4.7 
- exercice 4.11 
- exercice 4.12   

Chapitre 5

Actions de groupes, théorèmes de Sylow

Introduction

Les actions fournissent un point de vue très fructueux pour l'étude des groupes. De nombreux groupes apparaissent naturellement en agissant sur certains ensembles, par exemple le groupe symétrique en combinatoire et le groupe diédral en géométrie. Historiquement la notion même de groupe a été dégagée par Évariste Galois à partir de son action comme permutations des racines d'un polynôme. Connaître une action du groupe permet d'obtenir des renseignements aussi bien sur l'ensemble sur lequel le groupe agit, que sur le groupe lui-même. Le champ d'application des actions dépasse ainsi largement la théorie des groupes.

Comme conséquence, nous verrons en fin de chapitre les théorèmes de Sylow qui jouent un rôle important dans l'étude générale des groupes finis : ils donnent des renseignements qu'on peut tirer d'un tel groupe en ne connaissant que son ordre.

5.1 Action d'un groupe sur un ensemble

Définition 5.1

Une *action* d'un groupe G sur un ensemble X est une application

$$\begin{aligned} \star : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \star x \end{aligned}$$

qui satisfait les conditions suivantes :

1. pour tout $x \in X$: $1_G \star x = x$;
2. pour tous $(g, g') \in G \times G$ et $x \in X$: $g \star (g' \star x) = (gg') \star x$.

On dit que G agit (ou opère) sur X .

En particulier, afin d'avoir une action de groupe il faut s'assurer que l'application \star est bien à valeurs dans X .

Remarque 5.2. On prendra garde aux écueils suivants :

- \star n'est pas la loi interne du groupe G ;
- l'application $\star : G \times X \rightarrow X$ n'est pas un morphisme de groupes, car ni X ni $G \times X$ ne sont munis d'une structure de groupes dans ce contexte.

Remarque 5.3. Cette action est aussi appelée *action à gauche*. Il est parfois utile de considérer une *action à droite* qui, si elle est notée $x \bullet g$, est définie pour tous x de X et (g, g') de $G \times G$ par : $x \bullet 1_G = x$ et $(x \bullet g) \bullet g' = x \bullet (gg')$. Si \bullet est une action à droite, elle définit une action à gauche \star de la manière suivante : $g \star x = x \bullet g^{-1}$ (exercice : vérifier que c'est bien une action à gauche). Inversement, toute action à gauche \star définit une action à droite \bullet par cette même formule. Dans ce cours et pour simplifier, nous ne considérerons que des actions à gauche.

Les exemples d'action que nous passons en revue devraient vous convaincre que vous avez déjà rencontré cette notion.

Exemple 5.4. 1. Le groupe \mathcal{S}_X des permutations d'un ensemble X agit sur X par $\sigma \star x = \sigma(x)$ pour $\sigma \in \mathcal{S}_X$ et $x \in X$. En effet pour tous $x \in X$ et $(\sigma, \sigma') \in \mathcal{S}_X \times \mathcal{S}_X$ on a :

$$\begin{aligned} \text{id} \star x &= \text{id}(x) = x, \\ \sigma \star (\sigma' \star x) &= \sigma \star (\sigma'(x)) = \sigma(\sigma'(x)) = (\sigma \circ \sigma') \star x. \end{aligned}$$

En particulier le groupe symétrique \mathcal{S}_n agit de cette manière sur $\{1, \dots, n\}$.

2. Le groupe multiplicatif $\text{GL}_n(K)$ agit sur K^n via la multiplication d'une matrice avec un vecteur colonne : $M \star x = Mx$ pour $M \in \text{GL}_n(K)$ et $x \in K^n$ (vérification immédiate, laissée en exercice).
3. Le groupe orthogonal $\text{O}_n(\mathbb{R})$ agit sur la sphère unité \mathbb{S} de l'espace euclidien \mathbb{R}^n par $u \star x = u(x)$ pour $u \in \text{O}_n(\mathbb{R})$ et $x \in \mathbb{S}$. En effet toute isométrie envoie un point de la sphère sur un point de la sphère donc $u \star x = u(x) \in \mathbb{S}$. On laisse les lecteurs vérifier que \star est une action.
4. Soit \mathcal{A} un espace affine de direction $\vec{\mathcal{A}}$ (c'est-à-dire que $\vec{\mathcal{A}}$ est l'espace vectoriel sous-jacent – voir l'unité *Structures affines*). Alors $(\vec{\mathcal{A}}, +)$ est un groupe qui agit sur \mathcal{A} par $\vec{v} \star A = A + \vec{v}$ pour $v \in \vec{\mathcal{A}}$ et $A \in \mathcal{A}$.

Il est possible de faire agir un groupe sur lui-même, c'est-à-dire sur son ensemble sous-jacent. Il y a plusieurs manières usuelles de le faire.

Définition 5.5

L'action du groupe G par *translation* (à gauche) sur lui-même est définie par

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto gh. \end{aligned}$$

L'action du groupe G par *conjugaison* sur lui-même est définie par

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto ghg^{-1}. \end{aligned}$$

L'action du groupe G par *conjugaison* sur l'ensemble \mathcal{S} de ses sous-groupes est définie par

$$\begin{aligned} G \times \mathcal{S} &\longrightarrow \mathcal{S} \\ (g, H) &\longmapsto gHg^{-1}. \end{aligned}$$

(voir l'exercice 5.4 pour le fait que ce sont des actions). Ces actions apportent souvent des renseignements pertinents sur la structure du groupe lui-même.

L'énoncé suivant donne un point de vue complémentaire et fécond sur les actions de groupes.

Proposition 5.6

Se donner une action d'un groupe G sur un ensemble X équivaut à se donner un morphisme de groupes de G dans le groupe symétrique \mathcal{S}_X . Plus précisément :

- une action \star étant donnée, elle définit un morphisme de groupes $\varphi_\star : G \rightarrow \mathcal{S}_X$ donné par $\varphi_\star(g) : x \mapsto g \star x$;
- un morphisme de groupes $\varphi : G \rightarrow \mathcal{S}_X$ étant donné, il définit une action \star_φ de G sur X donnée par $g \star_\varphi x = (\varphi(g))(x)$;
- ces opérations sont réciproques : pour toute action \star de G sur X on a,

$$\star_{(\varphi_\star)} = \star$$

et tout morphisme de groupes $\varphi : G \rightarrow \mathcal{S}_X$, on a

$$\varphi_{(\star_\varphi)} = \varphi.$$

Démonstration. Voir l'exercice 5.6. □

Pour simplifier les notations du cours, on écrira $\varphi : G \rightarrow \mathcal{S}_X$ le morphisme associé à une action.

Exemple 5.7. Si G agit sur lui-même par conjugaison, le morphisme correspondant est

$$\begin{aligned} \varphi : G &\longrightarrow \mathcal{S}_G \\ g &\longmapsto (x \mapsto gxg^{-1}). \end{aligned}$$

L'application $\varphi(g) : x \mapsto gxg^{-1}$ est un automorphisme de G , appelé l'*automorphisme intérieur* associé à g . Pour cette raison, l'action d'un groupe par conjugaison sur lui-même est aussi appelée *action par automorphismes intérieurs*.

Nous pouvons ainsi recourir aux techniques usuelles des morphismes de groupes (restriction à un sous-groupe, étude du noyau, passage au quotient,...) pour comprendre une action du groupe. Par exemple si H est un sous-groupe de G , toute action de G sur X induit une action de H sur X : il suffit de considérer la restriction du morphisme φ à H . Nous verrons aussi comment le théorème de Cayley (théorème 2.31) s'interprète dans ce contexte.

☞ *Exercices pouvant être traités :*

- exercice 5.1 
- exercice 5.6   
- exercice 5.3, question 1  
- exercice 5.7, question 1  

5.2 Stabilisateurs, orbites, équation des classes

5.2.1 Stabilisateurs et orbites

Soit G un groupe agissant sur un ensemble X . L'étude de cette action passe par celle des stabilisateurs et des orbites.

Définition 5.8

Soit $x \in X$. Le *stabilisateur* de x (aussi appelé *sous-groupe d'isotropie* de x) est le sous-ensemble suivant de G :

$$G_x = \{g \in G \mid g \star x = x\}.$$

Le stabilisateur est parfois noté $\text{Stab}(x)$.

L'*orbite* de x est le sous-ensemble suivant de X :

$$G \star x = \{g \star x \mid g \in G\}.$$

L'orbite est parfois notée $\text{Orb}(x)$.

Proposition 5.9

Le stabilisateur G_x est un sous-groupe de G .

Démonstration. En effet le stabilisateur contient 1_G car $1_G \star x = x$; s'il contient g et g' on a $(gg') \star x = g \star (g' \star x) = g \star x = x$ i.e. $gg' \in G_x$; enfin si $g \in G_x$ alors $g^{-1} \star x = g^{-1} \star (g \star x) = (g^{-1}g) \star x = 1_G \star x = x$ d'où $g^{-1} \in G_x$. \square

Ainsi le stabilisateur d'un élément est muni d'une structure algébrique mais ce n'est pas le cas de l'orbite.

Définition 5.10

Un élément $x \in X$ est dit *fixe (par G)* ou *un point fixe (de G)* lorsque pour tout $g \in G$ on a $g \star x = x$.

De manière équivalente, x est fixe par G si $G \star x = \{x\}$, c'est-à-dire $G_x = G$.

Exemple 5.11. Soit $\sigma \in \mathcal{S}_n$ et faisons agir le sous-groupe $\langle \sigma \rangle$ par permutations sur $\{1, \dots, n\}$: on retrouve alors les notions de point fixe pour σ et de σ -orbites vues au chapitre 1.

Définition 5.12

L'action de G sur X est dite *transitive* si elle ne possède qu'une seule

orbite : il existe $x \in X$ tel que $X = G \star x$.

L'action est dite *libre* si tous les stabilisateurs sont réduits au neutre, i.e. pour tout $x \in X$, on a $G_x = \{1_G\}$.

L'action est dite *fidèle* si l'intersection de tous les stabilisateurs est réduite au neutre.

L'action est dite *simplement transitive* si elle est à la fois libre et transitive.

On a : simplement transitif \Rightarrow libre \Rightarrow fidèle.

Proposition 5.13

Soit G un groupe agissant sur un ensemble X .

1. L'action est transitive si et seulement si elle satisfait l'une des propriétés équivalentes suivantes :

(a) pour tout $x \in X$, on a $G \star x = X$;

(b) pour tous (x, y) de $X \times X$, il existe $g \in G$ tel que $y = g \star x$.

2. L'action est libre si et seulement si, pour tout $g \in G$,

$$(\exists x \in X, g \star x = x) \implies g = 1_G.$$

3. L'action est simplement transitive si et seulement si pour tous x, y dans X il existe un unique élément $g \in G$ tel que $y = g \star x$.

4. L'action est fidèle si et seulement si le morphisme $\varphi : G \rightarrow \mathcal{S}_X$ est injectif.

Démonstration. Les vérifications sont élémentaires et laissées en exercice. Pour le point 4, remarquer que le noyau du morphisme φ est $\bigcap_{x \in X} G_x$. \square

Exemple 5.14. 1. Faisons agir \mathcal{S}_n sur $\{1, \dots, n\}$ comme dans l'exemple 5.4.

— Le stabilisateur de $i \in \{1, \dots, n\}$ est $\{\sigma \in \mathcal{S}_n \mid \sigma(i) = i\}$: c'est un sous-groupe de \mathcal{S}_n qui est isomorphe à \mathcal{S}_{n-1} , donc d'ordre $(n-1)!$. L'action n'est pas libre dès que $n \geq 3$. Par contre elle est fidèle.

— L'orbite de $i \in \{1, \dots, n\}$ est $\{\sigma(i) \mid \sigma \in \mathcal{S}_n\}$. Tout élément $j \in \{1, \dots, n\}$ est dans cette orbite : en effet, il suffit d'utiliser la transposition qui échange i et j . Donc il n'y a qu'une seule orbite. L'action est transitive.

2. Faisons agir le groupe multiplicatif $\text{GL}_n(K)$ sur K^n comme dans l'exemple 5.4.

— Le stabilisateur d'un vecteur non nul x de K^n est $\{M \in \text{GL}_n(K) \mid Mx = x\}$: ce sont les matrices inversibles ayant 1 pour valeur propre et x pour vecteur propre associé. Le stabilisateur du vecteur nul est $\text{GL}_n(K)$ tout entier. En particulier l'action n'est pas libre.

— L'action est fidèle : si $M \in \text{GL}_n(K)$ vérifie $Mx = x$ pour tout vecteur $x \in K^n$ alors M est la matrice identité (prendre successivement pour x les vecteurs de la base canonique de K^n).

— L'orbite de x est $\{Mx \mid M \in \text{GL}_n(K)\}$. L'action n'est pas transitive : en effet, si $x \neq 0$, aucune matrice inversible $M \in \text{GL}_n(K)$ ne vérifie $Mx = 0$, donc x et le vecteur nul sont dans des orbites distinctes.

3. Faisons agir le groupe orthogonal $O_2(\mathbb{R})$ sur le cercle unité \mathbb{S} comme dans l'exemple 5.4 avec $n = 2$.
 - Le stabilisateur de $x \in \mathbb{S}$ est $\{u \in O_2(\mathbb{R}) \mid u(x) = x\}$. C'est le sous-groupe d'ordre 2 engendré par la symétrie orthogonale d'axe la droite $\mathbb{R}x$. En particulier l'action n'est pas libre. Elle est fidèle car si $u \in O_2(\mathbb{R})$ vérifie $u(x) = x$ pour tout $x \in \mathbb{S}$ alors u est l'identité (à nouveau, prendre pour x les vecteurs de la base canonique, qui sont de norme 1).
 - L'orbite de x est $\{u(x) \mid u \in O_2(\mathbb{R})\}$. Or étant donnés deux vecteurs x et y de norme 1 de \mathbb{R}^2 , il existe une rotation vectorielle du plan qui envoie x sur y . Donc l'orbite de tout élément x est la sphère unité \mathbb{S} . L'action est transitive.
4. Un espace affine peut être défini comme un ensemble \mathcal{A} muni d'une action simplement transitive de $(\vec{\mathcal{A}}, +)$ où $\vec{\mathcal{A}}$ est un espace vectoriel. On dit aussi que \mathcal{A} est un *espace homogène principal* sous le groupe additif de $\vec{\mathcal{A}}$ (voir l'unité *Structures affines*).
5. Pour l'action d'un groupe G sur lui-même par translation, le stabilisateur de $x \in G$ est $G_x = \{g \in G \mid gx = x\} = \{1_G\}$ puisque x est inversible dans G . Cette action est donc libre. En particulier l'action est fidèle et le morphisme de groupes induit $\varphi : G \rightarrow \mathcal{S}_G$ est injectif : c'est une démonstration très succincte du théorème de Cayley (théorème 2.31) avec le langage des actions de groupes.

On pourra aussi démontrer que l'action par translation à gauche de G sur lui-même est transitive (voir l'exercice 5.4).

Proposition 5.15 (Lien entre stabilisateur et orbite)

Soit un groupe G opérant sur un ensemble X et soit $x \in X$. L'application

$$\begin{aligned} G/G_x &\longrightarrow G \star x \\ gG_x &\longmapsto g \star x \end{aligned}$$

est une bijection entre l'ensemble des classes à gauche modulo le stabilisateur G_x et l'orbite $G \star x$. En particulier si G_x est d'indice fini dans G , l'orbite $G \star x$ est finie et de cardinal $[G : G_x]$.

On prendra garde au fait que l'application de l'énoncé n'est pas un morphisme de groupes : en effet $G \star x$ n'est pas muni d'une structure algébrique dans ce contexte et par ailleurs le sous-groupe G_x n'est pas supposé normal dans G .

Démonstration. C'est une démonstration classique : il est conseillé de bien la travailler et de la retenir. Commençons par voir que $gG_x \mapsto g \star x$ définit une application de G/G_x dans $G \star x$ c'est-à-dire que si $gG_x = g'G_x$ alors $g \star x = g' \star x$. Supposons $gG_x = g'G_x$. Il existe $h \in G_x$ tel que $g' = gh$. On en déduit $g' \star x = (gh) \star x = g \star (h \star x)$. Or h est dans le stabilisateur de x d'où $h \star x = x$ ce qui entraîne $g' \star x = g \star x$. L'application de l'énoncé est donc bien définie. Il s'agit d'établir sa bijectivité. Par définition de l'orbite $G \star x$, l'application est

surjective. Pour l'injectivité, prenons deux classes à gauche gG_x et $g'G_x$ telles que $g \star x = g' \star x$. Alors d'après la définition d'une action, on a

$$(g'^{-1}g) \star x = g'^{-1} \star (g \star x) = g'^{-1} \star (g' \star x) = (g'^{-1}g') \star x = 1_G \star x = x$$

donc $g'^{-1}g$ appartient au stabilisateur G_x . On en déduit $g \in g'G_x$ d'où $gG_x \subset g'G_x$. Enfin par symétrie on a $gG_x = g'G_x$, ce qui démontre l'injectivité. \square

5.2.2 Conjugaison

Nous donnons une simple relecture des notions de centralisateur, normalisateur, et sous-groupe normal avec le langage des actions de groupe (revoir page 27 pour les définitions de $C_G(A)$ et $N_G(A)$).

Définition 5.16

Deux éléments x et y de G sont dit *conjugués* dans G s'il existe $g \in G$ tel que $y = gxg^{-1}$. Deux sous-groupes H et H' de G sont dits *conjugués* dans G s'il existe $g \in G$ tel que $H' = gHg^{-1}$.

Deux éléments (resp. sous-groupes) sont conjugués s'ils sont dans la même orbite pour l'action de G sur lui-même (resp. sur l'ensemble de ses sous-groupes) par conjugaison.

On constate que pour l'action de G sur lui-même par conjugaison :

- le centralisateur $C_G(A)$ d'une partie A de G est l'intersection des stabilisateurs de tous les éléments de A ;
- le centre $Z(G)$ est l'intersection de tous les stabilisateurs des éléments de G i.e. l'ensemble des points fixes de G ;
- le nombre de conjugués de x , c'est-à-dire le cardinal de l'orbite de x , est donc l'indice $[G : C_G(x)]$ d'après la proposition 5.15.

De plus pour l'action de G par conjugaison sur l'ensemble de ses sous-groupes :

- le normalisateur $N_G(H)$ d'un sous-groupe H est le stabilisateur de H ;
- le nombre de conjugués de H est l'indice $[G : N_G(H)]$;
- le sous-groupe H est normal dans G si et seulement si H est un point fixe de G c'est-à-dire $N_G(H) = G$.

Ces résultats ne sont pas à apprendre par cœur mais à savoir éventuellement retrouver.

Remarque 5.17. Une caractérisation des classes de conjugaison des éléments de \mathcal{S}_n est obtenue dans l'exercice 1.8 : deux permutations sont conjuguées si et seulement si elles ont même type.

5.2.3 Équation des classes

Étant donné un groupe G agissant sur un ensemble X , on définit sur X une relation d'équivalence \sim en posant :

$$x \sim y \iff \exists g \in G, y = g \star x.$$

En effet pour tous $(x, y, z) \in X \times X \times X$, on a $x \star 1_G = x$ d'où $x \sim x$; si $x \sim y$ alors il existe $g \in G$ tel que $y = g \star x$ d'où $x = 1_G \star x = g^{-1} \star (g \star x) = g^{-1} \star y$ et $y \sim x$; enfin si $x \sim y$ et $y \sim z$, il existe $g_1, g_2 \in G$ avec $y = g_1 \star x$ et $z = g_2 \star y$ d'où $z = g_2 \star (g_1 \star x) = (g_2 g_1) \star x$ donc $x \sim z$. La relation \sim étant réflexive, symétrique et transitive, c'est bien une relation d'équivalence sur X .

La classe d'équivalence de x est son orbite $G \star x$. Cette relation d'équivalence donne alors une partition de X en orbites sous l'action de G . Plus précisément, si on fixe un système de représentants S des orbites, on a :

$$X = \coprod_{x \in S} G \star x. \quad (5.1)$$

Cette partition est indépendante du choix du système de représentants S .

Exemple 5.18. La démonstration de la décomposition d'une permutation en cycles (théorème 1.21) s'interprète naturellement avec le langage des actions de groupe. Soit σ une permutation. Le sous-groupe $G = \langle \sigma \rangle$ agit sur $\{1, \dots, n\}$ par permutations. La relation \sim qui lui correspond est la σ -équivalence (définition 1.18) et les orbites sont les σ -orbites (définition 1.19). L'argument-clé de la démonstration du théorème repose sur l'écriture $\{1, \dots, n\} = C_1 \sqcup \dots \sqcup C_r$, qui n'est autre que la partition en orbites (5.1) pour cette action.

Ainsi dans l'exemple 1.16, cette partition est :

$$\{1, \dots, 9\} = \{1, 3, 6\} \sqcup \{2, 4\} \sqcup \{5\} \sqcup \{7, 8, 9\}.$$

La formule (5.1) entraîne une relation fondamentale entre les cardinaux : c'est l'équation des classes, aussi appelée formule des classes, qui intervient dans de nombreux problèmes de dénombrement.

Théorème 5.19 (Équation des classes)

Soit G un groupe agissant sur un ensemble *fini* X et soit S un système de représentants des orbites de X sous l'action de G . On a

$$\text{Card}(X) = \sum_{x \in S} \text{Card}(G \star x) = \sum_{x \in S} [G : G_x] = \sum_{x \in S} \frac{\text{ord}(G)}{\text{ord}(G_x)},$$

la dernière égalité étant valable uniquement si G est fini.

Démonstration. La première égalité s'obtient en prenant les cardinaux dans (5.1), qui sont finis par hypothèse. La seconde s'en déduit à l'aide de la proposition 5.15. La dernière provient de $[G : G_x] = \text{Card}(G/G_x) = \text{ord}(G)/\text{ord}(G_x)$, qui est le théorème de Lagrange. \square

 *Exercices pouvant être traités :*

- exercice 5.2 
- exercice 5.3  
- exercice 5.4 
- exercice 5.5  
- exercice 5.7  
- exercice 5.8 

5.3 p -groupes et théorèmes de Sylow

5.3.1 Le centre des p -groupes

Définition 5.20

Soit p un nombre premier. Un p -groupe est un groupe fini dont l'ordre est une puissance de p .

- Exemple 5.21.**
1. Le groupe trivial $\{1\}$ est un p -groupe (il est d'ordre p^0).
 2. Le groupe $(\mathbb{Z}/8\mathbb{Z}, +)$ est un 2-groupe ; $(\mathbb{Z}/6\mathbb{Z}, +)$ n'est pas un p -groupe.
 3. Si G est un p -groupe, tout sous-groupe de G est aussi un p -groupe (conséquence du théorème de Lagrange).

Lorsqu'un p -groupe agit sur un ensemble fini, l'équation des classes donne une congruence entre le cardinal de cet ensemble et celui de ses points fixes.

Proposition 5.22 (Équation des classes pour un p -groupe)

Soit G un p -groupe agissant sur un ensemble fini X . Notons X^G l'ensemble des points fixes sous l'action de G : $X^G = \{x \in X \mid \forall g \in G, g \star x = x\}$. Alors on a

$$\text{Card}(X^G) \equiv \text{Card}(X) \pmod{p}.$$

Démonstration. Le stabilisateur G_x est un sous-groupe de G , donc un p -groupe. Par le théorème de Lagrange, deux cas se présentent :

- ou bien $\text{ord}(G_x) = \text{ord}(G)$: ceci se produit si et seulement si $G_x = G$ c'est-à-dire $x \in X^G$;
- ou bien $\text{ord}(G_x)$ divise strictement $\text{ord}(G)$; alors, comme G est un p -groupe, p divise $\text{ord}(G)/\text{ord}(G_x) = [G : G_x]$; donc $[G : G_x] \equiv 0 \pmod{p}$.

Puisque G et X sont finis, on déduit alors du théorème 5.19 les congruences :

$$\text{Card}(X) \equiv \sum_{x \in S \cap X^G} 1 \equiv \sum_{x \in X^G} 1 \equiv \text{Card}(X^G) \pmod{p}.$$

En effet on a $S \cap X^G = X^G$: tout élément $x \in X^G$ a son orbite réduite à $\{x\}$, donc x appartient au système de représentants S . \square

Cette équation des classes renseigne sur le centre des p -groupes.

Proposition 5.23

Si G est un p -groupe distinct de $\{1_G\}$, son centre $Z(G)$ est distinct de $\{1_G\}$.

Démonstration. Considérons l'action de G sur lui-même par conjugaison. On a vu que l'ensemble des points fixes est le centre $Z(G)$. Par la proposition 5.22 et comme $\text{ord}(G) \equiv 0 \pmod{p}$, on a $\text{ord}(Z(G)) \equiv 0 \pmod{p}$. Donc $Z(G)$ ne peut être réduit à $\{1_G\}$. \square

5.3.2 Théorèmes de Sylow

Définition 5.24

Soient G un groupe fini d'ordre n et p un nombre premier divisant n . Écrivons $n = p^r m$ avec $r \geq 1$ et p ne divisant pas m . Un p -sous-groupe de Sylow de G est un sous-groupe d'ordre p^r de G .

Autrement dit un p -sous-groupe de Sylow de G est un p -sous-groupe d'ordre maximal dans G . Pour abrégé on parlera souvent de p -Sylow.

Exemple 5.25. Un groupe d'ordre $40 = 2^3 \times 5$ a comme sous-groupes de Sylow ses sous-groupes d'ordre 8 (c'est-à-dire ses 2-Sylow) et ses sous-groupes d'ordre 5 (c'est-à-dire ses 5-Sylow), s'il en existe.

Tout p -sous-groupe de Sylow est donc un p -groupe mais la réciproque est fautive (dans l'exemple précédent, un sous-groupe d'ordre 4 n'est pas un 2-Sylow du groupe).

Dans un groupe donné, on peut se demander s'il existe des sous-groupes de Sylow et combien sont-ils. Leur existence est assurée par le théorème suivant qui renseigne aussi sur le nombre de ces sous-groupes et certaines de leurs propriétés.

Théorème 5.26 (Sylow)

Soient G un groupe fini d'ordre n et p un nombre premier divisant n . Écrivons $n = p^r m$ avec $r \geq 1$ et p ne divisant pas m .

1. (Existence) Il existe au moins un p -sous-groupe de Sylow de G .
2. (Conjugaison) Soit H un p -sous-groupe de G et soit P un p -sous-groupe de Sylow de G . Alors il existe $g \in G$ tel que $H \subset gPg^{-1}$. En particulier :
 - (a) H est contenu dans un p -sous-groupe de Sylow de G ;
 - (b) deux p -sous-groupes de Sylow de G sont toujours conjugués : si P, P' sont des p -sous-groupes de Sylow de G , il existe $g \in G$ tel que $P' = gPg^{-1}$.
3. (Dénombrement) Soit n_p le nombre de p -sous-groupes de Sylow de G . Alors $n_p \equiv 1 \pmod{p}$ et n_p divise m .

Remarque 5.27. Ce théorème renseigne sur les p -Sylow à p fixé. Dans les exercices 5.11 et 5.12, nous apprendrons à tirer des informations de l'étude simultanée des p -Sylow et q -Sylow pour $p \neq q$.

Démonstration. Celle que nous proposons utilise une panoplie d'actions du groupe G et les équations des classes correspondantes.

1. (Existence) On fait agir G par translation à gauche sur l'ensemble X de ses parties à p^r éléments. Pour $g \in G$ et $A \in X$, posons $g \star A = gA = \{ga \mid a \in A\}$. On laisse les lecteurs vérifier que c'est bien une action. L'équation des classes (théorème 5.19) donne

$$\binom{n}{p^r} = \binom{mp^r}{p^r} = \text{Card}(X) = \sum_{A \in S} [G : G_A] \quad (5.2)$$

où S est un système de représentants des orbites de X sous l'action de G . Admettons provisoirement le lemme combinatoire suivant.

Lemme 5.28

Soient p un nombre premier et m un entier tels que $p \nmid m$. Alors on a

$$\binom{mp^r}{p^r} \equiv m \pmod{p}.$$

Ce lemme, combiné à l'équation (5.2) assure que $\sum_{A \in S} [G : G_A] \not\equiv 0 \pmod{p}$. Donc il existe $A \in S$ dont le stabilisateur G_A est d'indice premier à p . Montrons que G_A est un p -sous-groupe de Sylow de G . En effet, d'une part son ordre est $\text{ord}(G_A) = \text{Card}(G)/[G : G_A]$, donc divisible par p^r . D'autre part, si on fixe $a \in A$ on a $G_A a \subset A$ car G_A est le stabilisateur de A . Or G_A est en bijection avec G_{Aa} (via $x \mapsto xa$) et donc $\text{ord}(G_A) \leq \text{Card}(A) = p^r$. Cela prouve que G_A est d'ordre p^r , donc un p -sous-groupe de Sylow de G , sous réserve du lemme. Prouvons-le maintenant.

Démonstration du lemme. Le coefficient binomial vérifie :

$$\begin{aligned} \binom{mp^r}{p^r} &= \frac{(mp^r)!}{(p^r)!(mp^r - p^r)!} \\ &= \frac{(mp^r)(mp^r - 1) \cdots (mp^r - (p^r - 1))(mp^r - p^r)!}{p^r(p^r - 1)!(mp^r - p^r)!} \\ &= m \prod_{i=1}^{p^r-1} \frac{mp^r - i}{p^r - i}. \end{aligned}$$

Comme $0 \leq i < p^r$ on peut écrire $i = p^s l$ avec $s < r$ et $p \nmid l$. On a ainsi

$$\binom{mp^r}{p^r} = m \prod_{p^s l = 1}^{p^r-1} \frac{mp^{r-s} - l}{p^{r-s} - l}.$$

Or on a les congruences modulo p : $mp^{r-s} - l \equiv -l$, $p^{r-s} - l \equiv -l$ et $l \not\equiv 0$. Donc les termes $(mp^{r-s} - l)/(p^{r-s} - l)$ sont tous congrus à 1. Finalement $\binom{mp^r}{p^r} \equiv m \pmod{p}$. \square

2. (Conjugaison) Soit P un p -sous-groupe de Sylow, dont l'existence est maintenant garantie. Soit H un p -sous-groupe de G . Faisons agir H sur G/P en posant $h \star gP = (hg)P$. On laisse les lecteurs vérifier que c'est bien une action. L'équation des classes pour H donne que le nombre de points fixes pour cette action est congru à $\text{Card}(G/P) = [G : P] = m$ modulo p , donc $\not\equiv 0 \pmod{p}$. Ainsi il existe un point fixe g_0P c'est-à-dire tel que $hg_0P = g_0P$ pour tout $h \in H$. Pour tout $h \in H$, cela entraîne $hg_0 \in g_0P$ c'est-à-dire $h \in g_0Pg_0^{-1}$. On a donc $H \subset g_0Pg_0^{-1}$.

De plus $g_0Pg_0^{-1}$ est un sous-groupe de G (le vérifier) et il est en bijection avec P (vérifier que l'application $P \rightarrow g_0Pg_0^{-1}$, $x \mapsto g_0xg_0^{-1}$, est bijective). C'est donc un p -sous-groupe de Sylow de G et on a prouvé 2a.

Enfin si H est un p -sous-groupe de Sylow, l'inclusion $H \subset g_0Pg_0^{-1}$ est une égalité car les deux ensembles ont même cardinal p^r , d'où 2b.

3. (Dénombrement) Notons Syl l'ensemble des p -sous-groupes de Sylow de G . Son cardinal est n_p . Faisons agir G sur Syl par conjugaison en posant $g \star P = gPg^{-1}$. On laisse les lecteurs vérifier que c'est bien une action. Deux p -sous-groupes de Sylow étant conjugués par le point 2b, cette action n'a qu'une seule orbite. L'équation des classes donne $n_p = [G : G_P] = \text{Card}(G)/\text{Card}(G_P)$ (pour P quelconque dans Syl). Or P est un sous-groupe de G_P (le vérifier) d'où $\text{Card}(P)$ divise $\text{Card}(G_P)$, qui divise $\text{Card}(G)$. Donc il existe un diviseur d de m , premier à p , tel que $\text{Card}(G_P) = p^r d$. On en déduit $n_p = m/d$, ce qui donne bien $n_p \mid m$.

Enfin faisons agir un p -sous-groupe de Sylow P sur Syl par conjugaison. L'équation des classes pour le p -groupe P dit que le nombre de points fixes est congru à $n_p \pmod p$. Montrons qu'il n'y a qu'un point fixe. On a déjà $gPg^{-1} = P$ pour tout $g \in P$ donc P est fixe pour cette action. Soit Q un p -Sylow fixe i.e. pour tout $g \in P$, $gQg^{-1} = Q$. Considérons le normalisateur de Q dans G i.e. le sous-groupe $N_G(Q) = \{g \in G \mid gQg^{-1} = Q\}$ de G . Il contient P et Q . En particulier P et Q sont des p -sous-groupes de Sylow de $N_G(Q)$. Par le point 2, ils sont conjugués par un élément $g \in N_G(Q)$ i.e. $gQg^{-1} = P$. Or par définition du normalisateur, on a $gQg^{-1} = Q$ d'où $P = Q$. Cela prouve que P est le seul point fixe d'où $n_p \equiv 1 \pmod p$.

□

5.3.3 Applications

Les conséquences des théorèmes de Sylow sont nombreuses. En voici deux classiques et à retenir.

Théorème 5.29 (Cauchy)

Soit G un groupe fini et soit p un nombre premier divisant l'ordre de G . Alors G possède au moins un élément d'ordre p .

Démonstration. Soit P un p -sous-groupe de Sylow de G (il en existe et il est distinct de $\{1_G\}$ car $p \mid \text{ord}(G)$). Soit x un élément de P distinct de 1_G . Par le théorème de Lagrange dans P , x est d'ordre p^α avec $\alpha > 0$. Alors $y = x^{p^{\alpha-1}}$ est d'ordre p : en effet on a d'une part $y^p = x^{p^\alpha} = 1_G$, ce qui montre que $\text{ord}(y) \mid p$ et d'autre part y n'est pas d'ordre 1 car $y \neq 1_G$. □

Remarque 5.30. Ce théorème fournit une réciproque au théorème de Lagrange pour les diviseurs premiers : tout groupe fini d'ordre divisible par un nombre premier p possède un sous-groupe d'ordre p (celui engendré par un élément d'ordre p).

Proposition 5.31

Un p -sous-groupe de Sylow de G est normal dans G si et seulement si $n_p = 1$.

Démonstration. Soit H un p -sous-groupe de Sylow de G . Il est normal si et seulement si, pour tout $g \in G$, $gHg^{-1} = H$, autrement dit si H est égal à tous ses conjugués. Comme tous les p -Sylow sont conjugués entre eux par les théorèmes de Sylow, cela revient à dire qu'il n'y a qu'un seul p -Sylow c'est-à-dire $n_p = 1$. \square

Exemple 5.32. Soit G un groupe d'ordre $15 = 3 \times 5$. D'après les théorèmes de Sylow, le nombre n_3 de ses 3-sous-groupes de Sylow divise 5 (d'où $n_3 \in \{1, 5\}$) et $n_3 \equiv 1 \pmod{3}$. La seule valeur possible est $n_3 = 1$. Il n'y a donc qu'un seul 3-Sylow, qui est normal dans G par la proposition 5.31. Par ailleurs, ce sous-groupe n'est ni $\{1_G\}$ ni G (car il est d'ordre 3). Donc le groupe G n'est pas simple. Les lecteurs vérifieront qu'on obtient le même résultat en regardant les 5-Sylow de G .

 *Exercices pouvant être traités :*

- exercice 5.9  
- exercice 5.10 
- exercice 5.11  
- exercice 5.12  
- exercice 5.13 

Chapitre 6

Arithmétique dans \mathbb{Z}

Introduction

Ce dernier chapitre commence par passer en revue les propriétés de \mathbb{Z} , notamment de nature arithmétique, sous l'angle de sa structure d'anneau. Il s'agit d'une introduction à cette nouvelle structure algébrique qui sera développée en détail dans l'unité *Anneaux*. Nous verrons aussi que le groupe quotient $(\mathbb{Z}/n\mathbb{Z}, +)$ est muni d'une structure d'anneau héritée de celle de \mathbb{Z} , ce qui en fait un exemple d'anneau quotient. Enfin nous serons amenés à étudier le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ qui intervient souvent en arithmétique. Ce chapitre, plus long que les précédents, contient certains résultats avec lesquels vous êtes déjà familiers. La section 6.3 reprend la construction de \mathbb{N} via l'axiomatique de Peano puis de \mathbb{Z} par le procédé de symétrisation : elle est donnée à titre culturel et n'est pas exigible pour l'examen.

6.1 L'anneau \mathbb{Z} et son arithmétique

Soient \mathbb{N} l'ensemble des entiers naturels et \mathbb{Z} l'ensemble des entiers relatifs. Nous renvoyons à la section 6.3 pour des constructions de ces ensembles (elles sont instructives mais un peu longues à mettre en place).

Théorème 6.1

L'ensemble \mathbb{Z} est muni de deux lois $+$ et \times qui en font un *anneau commutatif unitaire intègre*. Cela signifie qu'il vérifie les propriétés suivantes :

1. $(\mathbb{Z}, +)$ est un groupe abélien d'élément neutre 0 ;
2. la loi \times est associative, commutative, et possède un élément neutre qui est 1 ;
3. la loi \times est distributive par rapport à la loi $+$: $a \times (b + c) = a \times b + a \times c$ pour tous a, b, c dans \mathbb{Z} ;
4. si $ab = 0$ pour a et b dans \mathbb{Z} alors $a = 0$ ou $b = 0$.

On note $-x$ l'inverse de x pour l'addition. L'ensemble \mathbb{N} est vu comme un sous-ensemble de \mathbb{Z} et on a $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ où $-\mathbb{N} = \{-a \mid a \in \mathbb{N}\}$. Sur \mathbb{N} on

dispose du principe de récurrence (voir la section 6.3).

L'anneau \mathbb{Z} est muni d'une relation d'ordre total \leq définie par

$$x \leq y \iff y - x \in \mathbb{N}.$$

Sa restriction définit aussi une relation d'ordre total \leq sur \mathbb{N} . L'ordre \leq vérifie les propriétés fondamentales suivantes.

Théorème 6.2

1. Toute partie non vide de \mathbb{N} admet un plus petit élément pour \leq (on dit que \leq est un *bon ordre* sur \mathbb{N}).
2. Toute partie finie non vide de \mathbb{N} admet un plus grand élément pour \leq .
3. La relation d'ordre \leq sur \mathbb{N} est *archimédienne* : pour tout $x \in \mathbb{N}$ et pour tout $n \in \mathbb{N} - \{0\}$, il existe $k \in \mathbb{N}$ tel que $kn \geq x$.

Les propriétés 2 et 3 restent vraies pour (\mathbb{Z}, \leq) mais 1 est fausse si on remplace \mathbb{N} par \mathbb{Z} .

6.1.1 Division euclidienne

Nous commençons par étudier les propriétés de divisibilité dans l'anneau \mathbb{Z} , qui fondent l'arithmétique des entiers.

Définition 6.3

Soient a et b dans \mathbb{Z} . On dit que b *divise* a s'il existe $c \in \mathbb{Z}$ tel que $a = bc$.

On écrit alors $b \mid a$. On dit aussi que b est un *diviseur* de a ou que a est un *multiple* de b . Par exemple 1 et -1 divisent tous les entiers relatifs, et tous les entiers relatifs divisent 0. La divisibilité est une relation d'ordre sur \mathbb{Z} .

Théorème 6.4 (Division euclidienne)

Soit $a \in \mathbb{Z}$ et soit $b \in \mathbb{Z}$, $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ avec $0 \leq r < |b|$ tel que

$$a = bq + r.$$

L'entier q (resp. r) est appelé le *quotient* (resp. le *reste*) de la division euclidienne de a par b .

Démonstration. Lorsque a et b sont dans \mathbb{N} , montrons le résultat comme conséquence de la propriété archimédienne de \mathbb{N} . L'ensemble des $k \in \mathbb{N}$ tels que $bk > a$ est non vide. Soit donc q' le plus petit entier naturel tel que $bq' > a$. On pose alors $q = q' - 1 \in \mathbb{Z}$. Alors on vérifie qu'on a $0 \leq a - bq < b$. Il suffit de poser $r = a - bq$. Pour l'unicité, si $bq_1 + r_1 = bq_2 + r_2$ avec $0 \leq r_1, r_2 < b$ alors on peut supposer que $q_1 \geq q_2$ et on a $b(q_1 - q_2) = r_2 - r_1$ avec $0 \leq r_2 - r_1 < b$. Si $q_1 - q_2 \neq 0$ alors $b(q_1 - q_2) \geq b$, ce qui est impossible. On en déduit $q_1 = q_2$ puis $r_1 = r_2$. Lorsque a ou b est de signe quelconque, le théorème se démontre par une analyse de cas en se ramenant à la situation précédente. \square

Corollaire 6.5

Soit $a \in \mathbb{Z}$ et soit $b \in \mathbb{Z}$, $b \neq 0$. Alors b divise a si et seulement si le reste r de la division euclidienne de a par b est nul.

Démonstration. Le sens \Leftarrow est immédiat. Pour \Rightarrow , supposons que b divise a . Écrivons la division euclidienne de a par b : $a = bq + r$ avec $q \in \mathbb{Z}$, $r \in \mathbb{N}$ et $0 < r < |b|$. Comme b divise à la fois bq et a , il divise donc r . Si $r \neq 0$ on aurait alors $|b| \leq r$, ce qui contredit $0 < r < |b|$. Donc $r = 0$. \square

Rappelons le résultat important suivant, démontré en utilisant la division euclidienne (voir l'exercice 2.12).

Théorème 6.6

Pour tout sous-groupe H de $(\mathbb{Z}, +)$ il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Remarquons que $a\mathbb{Z} \subset b\mathbb{Z}$ si et seulement si b divise a . De plus pour tout $n \in \mathbb{N}$, on a $n\mathbb{Z} = (-n)\mathbb{Z} = -n\mathbb{Z}$.

6.1.2 Pgcd, ppcm**Définition 6.7**

Soient $a\mathbb{Z}$ et $b\mathbb{Z}$ deux sous-groupes de $(\mathbb{Z}, +)$. L'ensemble

$$a\mathbb{Z} + b\mathbb{Z} = \{an + bm \mid n \in \mathbb{Z}, m \in \mathbb{Z}\}$$

est un sous-groupe de $(\mathbb{Z}, +)$. Il est donc de la forme $d\mathbb{Z}$ pour un unique $d \in \mathbb{N}$. L'entier d s'appelle le *plus grand diviseur commun de a et b* et on note $d = \text{pgcd}(a, b)$.

On vérifie aisément que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe car c'est celui engendré par la partie $\{a, b\}$. Pour simplifier, on écrit pgcd au lieu de plus grand diviseur commun.

Proposition 6.8

Pour tous a, b, c dans \mathbb{Z} on a :

1. $\text{pgcd}(a, b) = \text{pgcd}(b, a)$;
2. $\text{pgcd}(1, a) = 1$;
3. $\text{pgcd}(0, a) = a$;
4. $a \cdot \text{pgcd}(b, c) = \text{pgcd}(ab, ac)$.

Démonstration. Vérifications directes laissées aux lecteurs. \square

Définition 6.9

Deux entiers relatifs a et b sont *premiers entre eux* lorsque $\text{pgcd}(a, b) = 1$.

Théorème 6.10

1. (Relation de Bézout) Soient a, b dans \mathbb{Z} . Il existe u et v dans \mathbb{Z} tels que $\text{pgcd}(a, b) = au + bv$.
2. (Théorème de Bézout) Soient a, b dans \mathbb{Z} . Alors a et b sont premiers entre eux si et seulement s'il existe u et v dans \mathbb{Z} tels que $1 = au + bv$.

Démonstration. Les démonstrations de ces énoncés, à partir de la définition du pgcd donnée dans ce cours, sont à connaître.

1. C'est immédiat puisque $\text{pgcd}(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ et que $\text{pgcd}(a, b) \in \text{pgcd}(a, b)\mathbb{Z}$.
2. Le sens direct est conséquence du premier point. Inversement s'il existe u, v tels que $au + bv = 1$ alors tout élément $n \in \mathbb{Z}$ s'écrit $n = aun + bvn \in a\mathbb{Z} + b\mathbb{Z}$, ce qui prouve $\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$. L'autre inclusion étant immédiate, on a $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. On en déduit $\text{pgcd}(a, b) = 1$.

□

- Remarque 6.11.**
1. Dans le théorème 6.10/1, on prendra garde à une erreur courante : l'existence de u, v tels que $d = au + bv$ n'entraîne pas $d = \text{pgcd}(a, b)$. Par exemple on a $2 \times 2 + 4 \times 1 = 8$ et pourtant 8 n'est pas le pgcd de 2 et 4.
 2. Le couple d'entiers (u, v) d'une relation de Bézout n'est pas unique. À ce sujet, voir l'exercice 6.3.

Théorème 6.12 (Lemme de Gauss)

Soient a, b, c dans \mathbb{Z} . Si a divise bc et si a et b sont premiers entre eux alors a divise c .

Démonstration. Cette démonstration est à connaître. Puisque a et b sont premiers entre eux, il existe u, v dans \mathbb{Z} tels que $1 = au + bv$ par le théorème de Bézout. On a alors $c = acu + bcv$. Comme a divise bc et a divise évidemment acu , on en déduit que a divise c . □

L'énoncé suivant justifie l'appellation de plus grand diviseur commun : c'est le plus grand, au sens de la divisibilité, diviseur commun à a et b .

Proposition 6.13

Soit $d \in \mathbb{N}$. Alors d est le pgcd de a et b si et seulement s'il satisfait les deux propriétés suivantes :

1. d divise a et b ;
2. si un entier naturel d' divise a et b , alors d' divise d .

Démonstration. Commençons par montrer que $\text{pgcd}(a, b)$ vérifie les deux propriétés énoncées. On a $a\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$ donc $\text{pgcd}(a, b) \mid a$ et de même,

$\text{pgcd}(a, b) \mid b$. De plus, si d' divise a et b alors $a\mathbb{Z} \subset d'\mathbb{Z}$ et $b\mathbb{Z} \subset d'\mathbb{Z}$ et on en déduit facilement que $\text{pgcd}(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset d'\mathbb{Z}$, ce qui entraîne $d' \mid \text{pgcd}(a, b)$.

Inversement, soit d un entier naturel satisfaisant ces deux propriétés. Comme d divise a et b on a $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$ donc $\text{pgcd}(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$. On en déduit que d divise $\text{pgcd}(a, b)$. Par ailleurs, comme $\text{pgcd}(a, b)$ divise a et b (voir la première partie de la démonstration), on a $\text{pgcd}(a, b)$ divise d par la seconde propriété. Donc $d = \text{pgcd}(a, b)$. □

Corollaire 6.14

1. Soient a, b dans \mathbb{Z} et $d = \text{pgcd}(a, b)$. Il existe des entiers a' et b' uniques et premiers entre eux tels que $a = da'$ et $b = db'$.
2. Soient a et b dans \mathbb{Z} . Pour tout $q \in \mathbb{N}$ on a

$$\text{pgcd}(a, b) = \text{pgcd}(b, a - bq).$$

Démonstration. 1. Comme d divise a , il existe $a' \in \mathbb{Z}$ tel que $a = da'$. De même il existe $b' \in \mathbb{Z}$ tel que $b = db'$. De plus il existe $u, v \in \mathbb{Z}$ tels qu'on ait la relation de Bézout $d = au + bv = da'u + db'v$. En simplifiant par d , on obtient $1 = a'u + b'v$. Le théorème de Bézout entraîne que a' et b' sont premiers entre eux.

2. Notons $d = \text{pgcd}(b, a - bq)$. Alors d divise à la fois b et $a - bq$, donc d divise a . Par ailleurs si d' divise a et b alors d' divise $a - bq$ donc d' divise leur pgcd d . La proposition 6.13 entraîne $d = \text{pgcd}(a, b)$. □

La deuxième partie du corollaire est le principe fondateur de l'algorithme d'Euclide pour le calcul du pgcd . On écrit la succession de divisions euclidiennes :

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0q_1 + r_1 \\ r_0 &= r_1q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1} + 0 \end{aligned}$$

où r_n désigne le dernier reste non nul. Justifions qu'un tel entier n existe. Si $r_j \neq 0$ alors les restes satisfont $0 \leq r_{j+1} < r_j$. Or il n'existe pas de suite strictement décroissante d'entiers naturels car \leq est un bon ordre sur \mathbb{N} . Il existe donc un plus petit rang, noté $n + 1$, tel que $r_{n+1} = 0$. Par le corollaire, on a

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = \text{pgcd}(r_0, r_1) = \cdots = \text{pgcd}(r_{n-1}, r_n) = r_n.$$

L'algorithme d'Euclide étendu, dans lequel on « remonte » les lignes de l'algorithme, permet de trouver un couple d'entiers $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $\text{pgcd}(a, b) = au + bv$ c'est-à-dire une relation de Bézout entre a et b .

D'une manière similaire on définit le ppcm de deux entiers.

Définition 6.15

Soient $a\mathbb{Z}$ et $b\mathbb{Z}$ deux sous-groupes de $(\mathbb{Z}, +)$. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Il est donc de la forme $m\mathbb{Z}$ pour un unique $m \in \mathbb{N}$. L'entier m s'appelle le *plus petit multiple commun* de a et b et on note $m = \text{ppcm}(a, b)$.

L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe puisque c'est une intersection de sous-groupes. Pour simplifier on écrit ppcm au lieu de plus petit multiple commun.

Proposition 6.16

Pour tous a, b, c dans \mathbb{Z} on a :

1. $\text{ppcm}(a, b) = \text{ppcm}(b, a)$;
2. $\text{ppcm}(1, a) = a$;
3. $\text{ppcm}(0, a) = 0$;
4. $a \cdot \text{ppcm}(b, c) = \text{ppcm}(ab, ac)$.

Démonstration. Vérifications directes laissées aux lecteurs. □

Proposition 6.17

Soit $m \in \mathbb{N}$. Alors m est le ppcm de a et b si et seulement s'il vérifie les deux propriétés suivantes :

1. m est un multiple de a et b ;
2. si un entier naturel m' est un multiple de a et b , alors m' est un multiple de m .

Démonstration. Similaire à celle de la proposition 6.13 et laissée aux lecteurs. □

Proposition 6.18

Pour tous a et b dans \mathbb{Z} , on a $\text{pgcd}(a, b) \cdot \text{ppcm}(a, b) = |ab|$.

Démonstration. Pour simplifier supposons a et b positifs (on peut toujours se ramener à cette situation). Notons $d = \text{pgcd}(a, b)$, $m = \text{ppcm}(a, b)$. Par la proposition 6.14, il existe a' et b' premiers entre eux tels que $a = da'$ et $b = db'$. Montrons que $m = da'b'$, ce qui entraînera $dm = ab$. Il est clair que $da'b' = ab' = a'b$ est un multiple de a et de b . Soit m' un multiple de a et de b . Il existe k, l dans \mathbb{Z} tels que $m' = ka$ et $m' = lb$. On a alors $ka = lb$ d'où $kda' = ldb'$ d'où $ka' = lb'$. En particulier a' divise lb' et comme a' et b' sont premiers entre eux, le lemme de Gauss implique que a' divise l . On en déduit $a'b$ divise lb c'est-à-dire m divise m' . La proposition 6.17 affirme alors que $m = \text{ppcm}(a, b) = da'b'$ ce qui conclut. □

6.1.3 Écriture d'un entier dans une base

Le théorème suivant permet de représenter tous les entiers relativement à une base donnée.

Proposition 6.19

Fixons un entier b supérieur ou égal à 2. Soit $E = \{0, \dots, b-1\}$. Pour tout $n \in \mathbb{Z} - \{0\}$, il existe un unique signe $\varepsilon \in \{\pm 1\}$, un unique entier $k \in \mathbb{N}$, et des entiers n_0, \dots, n_k dans E uniques avec $n_k \neq 0$ tels que

$$n = \varepsilon(n_0 + n_1b + \dots + n_{k-1}b^{k-1} + n_k b^k) = \varepsilon \sum_{i=0}^k n_i b^i.$$

Il s'agit de l'écriture de n en base b . Les nombres n_0, \dots, n_k sont appelés les *chiffres de n en base b* (si on parle de chiffre sans mentionner la base, il s'agit généralement de la base 10 c'est-à-dire de l'écriture décimale). On note aussi cette écriture comme suit :

$$n = \overline{n_k n_{k-1} \dots n_1 n_0}^b.$$

Par exemple $101 = \overline{101}^{10} = \overline{203}^7$.

Des exemples de bases sont la base décimale ($b = 10$), la base binaire ($b = 2$) et la base hexadécimale ($b = 16$), ces deux dernières étant utilisées en informatique. Pour la base hexadécimale, on adopte la convention suivante pour les chiffres utilisés : $0, 1, \dots, 9, A, B, C, D, E, F$.

Remarque 6.20. La proposition s'étend au cas où $n = 0$ pour l'existence de l'écriture (à condition de ne plus supposer $n_k \neq 0$) mais pas pour l'unicité.

Démonstration. Supposons que $n > 0$ i. e $\varepsilon = +1$ (on peut toujours se ramener à cette situation). On démontre l'existence par récurrence sur n . Le résultat est clair si n vaut 1. Supposons l'existence de l'écriture vérifiée pour tout entier $< n$. La division euclidienne de n par b est $n = bq + n_0$ avec $n_0 \in E$ et $0 \leq \frac{n - n_0}{b} < n$. Par hypothèse de récurrence, on a

$$\frac{n - n_0}{b} = x_0 + x_1b + \dots + x_j b^j$$

avec $x_j \neq 0$ et x_0, \dots, x_j dans E . On en déduit

$$n = n_0 + x_0b + x_1b^2 + \dots + x_j b^{j+1}$$

qui est une écriture de n en base b .

Pour l'unicité, supposons que

$$n = n_0 + n_1b + \dots + n_k b^k = n'_0 + n'_1b + \dots + n'_l b^l \quad (6.1)$$

avec $n_k \neq 0, n'_l \neq 0$, et les n_i, n'_i dans E . Comme $n_k \geq 1$, on a donc

$$n_0 + n_1b + \dots + n_k b^k \geq b^k$$

et

$$n'_0 + n'_1 b + \cdots + n'_l b^l \leq (b-1)(b^l + b^{l-1} + \cdots + b + 1) = b^{l+1} - 1.$$

On en déduit que $b^k < b^{l+1}$ d'où $k < l + 1$. De même on obtient $l < k + 1$ d'où $l = k$. Démontrons par récurrence sur n que $n_i = n'_i$ pour tout $i \in \{0, \dots, k\}$ dans l'égalité (6.1). On remarque d'abord que b divise $n_0 - n'_0$. Or n_0 et n'_0 appartiennent à E donc $|n_0 - n'_0| < b$ ce qui entraîne $n_0 = n'_0$. En simplifiant par n_0 et en divisant par b , l'égalité (6.1) devient :

$$\frac{n - n_0}{b} = n_k b^{k-1} + \cdots + n_1 = n'_k b^{k-1} + \cdots + n'_1.$$

Par récurrence on a $n_i = n'_i$ pour tout $i \leq k - 1$, d'où l'égalité $n_k = n'_k$. \square

Remarque 6.21. La démonstration fournit une méthode effective permettant d'écrire un entier donné dans une base. Voir l'exercice 6.6 à ce sujet.

6.1.4 Théorème fondamental de l'arithmétique

Définition 6.22

Un entier $p \in \mathbb{N}$ est un *nombre premier* si $p > 1$ et si ses seuls diviseurs dans \mathbb{N} sont 1 et p .

Exemple 6.23. Les dix premiers nombres premiers sont :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$$

Proposition 6.24

1. Tout nombre entier supérieur ou égal à 2 est divisible par au moins un nombre premier.
2. Soient p un nombre premier et $a \in \mathbb{N}$. Alors p divise a ou p est premier avec a .

Démonstration. 1. Raisonnons par récurrence sur $n \in \mathbb{N}$, $n > 1$. Si $n = 2$, le résultat est clair. Soit $n \geq 2$ et supposons la propriété satisfaite pour tout entier $< n$. Si n est premier, il n'y a rien à démontrer. Sinon, n n'étant pas premier, il est divisible par un entier $d \in \{2, \dots, n - 1\}$. Par hypothèse de récurrence, d est divisible par un nombre premier p . Donc p divise aussi n .

2. On pose $d = \text{pgcd}(a, p)$. Alors d divise p donc, par primalité de p , d vaut p ou 1. Si $d = p$ alors p divise a . Si $d = 1$ alors les entiers a et p sont premiers entre eux. \square

Remarque 6.25. De façon plus précise, on peut montrer que si n n'est pas premier alors il existe un nombre premier p divisant n tel que $p \leq \sqrt{n}$. Cette remarque est à l'origine du crible d'Ératosthène : pour trouver tous les nombres premiers compris entre 2 et N , on liste tous les entiers de $\{2, \dots, N\}$ puis on supprime tous ceux divisibles par 2, 3, \dots , $[\sqrt{N}]$ où $[\cdot]$ désigne la partie entière.

Corollaire 6.26

Il existe une infinité de nombres premiers.

Démonstration. Il s'agit de la démonstration d'Euclide. Raisonnons par l'absurde. Supposons qu'il n'existe qu'un nombre fini de nombre premiers, notés p_1, \dots, p_n . On pose :

$$N = p_1 p_2 \cdots p_n + 1$$

dans \mathbb{N} . Par le premier point de la proposition, il existe un nombre premier divisant N . Ce diviseur premier est p_j pour un certain $j \in \{1, \dots, n\}$. Mais p_j divisant aussi $p_1 \cdots p_n$, il divise 1, ce qui est impossible. \square

Proposition 6.27 (Lemme d'Euclide)

Soient p un nombre premier et a, b dans \mathbb{Z} . Si p divise ab alors p divise a ou p divise b .

Démonstration. Il s'agit d'un résultat classique d'arithmétique, dont la démonstration est à connaître. Supposons que p divise ab et p ne divise pas a . Comme p est premier, le second point de la proposition 6.24 assure que p et a sont premiers entre eux. D'après le lemme de Gauss, p divise donc b . \square

Théorème 6.28 (Théorème fondamental de l'arithmétique)

Soit n un entier relatif distinct de 0, 1 et -1 . Il existe un unique entier $\varepsilon \in \{\pm 1\}$, un unique entier naturel $r \geq 1$, une unique famille de nombres premiers $p_1 < p_2 < \cdots < p_r$, et une unique famille d'entiers $(k_i)_{1 \leq i \leq r}$ avec $k_i \geq 1$ tels que :

$$n = \varepsilon \prod_{i=1}^r p_i^{k_i}.$$

C'est la décomposition de n en facteurs premiers.

Remarque 6.29. Le cas où $n \in \{1, -1\}$ peut être inclus dans cet énoncé, quitte à autoriser la famille $(p_i)_i$ à être vide (le produit indexé par un ensemble vide est, par convention, égal à 1).

Démonstration. Le nombre ε est évidemment le signe de n . On se ramène facilement au cas où $n > 1$ c'est-à-dire $\varepsilon = +1$. En quelques mots, l'existence repose sur l'existence d'un diviseur premier (proposition 6.24) et l'unicité utilise le lemme d'Euclide.

Démontrons le théorème par récurrence sur n . Si $n = 2$, alors comme 2 est premier, sa décomposition en facteurs premiers est $n = 2$ et elle est évidemment unique. Soit $n > 1$. Supposons que tout entier strictement inférieur à n peut être décomposé de manière unique comme annoncé. Deux cas se présentent. Si n est premier, la décomposition de n est trouvée, et il n'y en a pas d'autre. Si n n'est pas premier, alors il existe un nombre premier p et un entier m tels que $n = pm$ d'après la proposition 6.24. Comme $m < n$, l'hypothèse de récurrence

assure l'existence d'une factorisation $m = p_1^{k_1} \cdots p_r^{k_r}$ avec r unique, $p_1 < \cdots < p_r$ uniques et $(k_i)_{1 \leq i \leq r}$ uniques avec $k_i \geq 1$. On en déduit :

$$n = pm = pp_1^{k_1} \cdots p_r^{k_r}$$

qui est une factorisation de p de la forme annoncée. Prouvons qu'elle est unique. Supposons $n = pp_1^{k_1} \cdots p_r^{k_r} = q_1^{\ell_1} \cdots q_s^{\ell_s}$ avec $s \geq 1$, $q_1 < \cdots < q_s$ premiers et $(\ell_j)_{1 \leq j \leq s}$ avec $\ell_j \geq 1$. Alors d'après le lemme d'Euclide, p appartient à $\{q_1, \dots, q_s\}$. Posons alors $p = q_j$. On en déduit :

$$m = \frac{n}{p} = p_1^{k_1} \cdots p_r^{k_r} = q_1^{\ell_1} \cdots q_j^{\ell_j-1} \cdots q_s^{\ell_s}.$$

Or par hypothèse de récurrence, la factorisation de m est unique. Donc $r = s$, $p_1 = q_1, \dots, p_s = q_s$, $k_1 = \ell_1, \dots, k_j = \ell_j - 1, \dots, k_r = \ell_r$. La factorisation de n est donc unique. \square

Définition 6.30

Soit p un nombre premier et soit $n \in \mathbb{Z}$, $n \neq 0$. L'ensemble d'entiers naturels $\{k \in \mathbb{N}, p^k \mid n\}$ est fini d'après le théorème fondamental de l'arithmétique. Il possède donc un plus grand élément, qui est l'entier naturel $v_p(n) = \max\{k \in \mathbb{N}, p^k \mid n\}$. On appelle $v_p(n)$ la *valuation p -adique de n* .

Si $v_p(n) = 0$ alors p ne divise pas n , et inversement. Si $v_p(n) > 0$, alors $v_p(n)$ est précisément la puissance de p dans la décomposition de n .

La décomposition de n s'écrit alors :

$$n = \text{sign}(n) \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

où sign est la fonction signe et \mathbb{P} désigne l'ensemble des nombres premiers. Le produit ci-dessus est fini car $v_p(n)$ est nul sauf pour un nombre fini de p (ceux intervenant dans la décomposition de n).

Exemple 6.31. 1. Comme $24 = 2^3 \times 3$, on a $v_2(24) = 3$, $v_3(24) = 1$ et $v_p(24) = 0$ pour tout premier p distinct de 2 et 3.

2. Dans un groupe d'ordre n , les p -sous-groupes de Sylow sont les sous-groupes d'ordre $p^{v_p(n)}$.

Voyons des propriétés de la valuation p -adique.

Proposition 6.32

Soient a et b deux entiers relatifs non nuls et p un nombre premier. On a :

1. $v_p(ab) = v_p(a) + v_p(b)$;
2. a divise b si et seulement si, pour tout $p \in \mathbb{P}$, $v_p(a) \leq v_p(b)$;
3. $v_p(\text{pgcd}(a, b)) = \min\{v_p(a), v_p(b)\}$;
4. $v_p(\text{ppcm}(a, b)) = \max\{v_p(a), v_p(b)\}$;
5. $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$.

Démonstration. 1. Notons $\alpha = v_p(a)$ et $\beta = v_p(b)$. On a $a = p^\alpha a'$ et $b = p^\beta b'$ avec $p \nmid a'$ et $p \nmid b'$. Alors on a $ab = p^{\alpha+\beta} a'b'$. Par le lemme d'Euclide, p ne divise pas $a'b'$. On en déduit $\alpha + \beta = v_p(ab)$.

2. Cela vient du fait que p premier divise a si et seulement si $v_p(a) \geq 1$, et alors $v_p(a)$ est la puissance de p dans la décomposition de a .
3. Posons $i_p = \min\{v_p(a), v_p(b)\}$. Il s'agit de montrer que $v_p(\text{pgcd}(a, b)) = i_p$ pour tout $p \in \mathbb{P}$. Par définition de i_p , l'entier $\prod_p p^{i_p}$ divise a et b donc il divise $\text{pgcd}(a, b)$. On en déduit, par le deuxième point de la proposition, que $i_p \leq v_p(\text{pgcd}(a, b))$ pour tout p . Inversement comme $\text{pgcd}(a, b)$ divise a et b on a aussi l'inégalité $v_p(\text{pgcd}(a, b)) \leq i_p$ d'où finalement l'égalité.
4. On peut procéder comme pour le pgcd , ou bien utiliser la relation $ab = \text{pgcd}(a, b) \cdot \text{ppcm}(a, b)$.
5. Posons $\alpha = v_p(a)$ et $\beta = v_p(b)$, puis $a' = p^{-\alpha}a$ et $b' = p^{-\beta}b$ dans \mathbb{Z} . Alors a' et b' sont de valuation p -adique nulle. Quitte à échanger les rôles de a et b , on peut supposer $\alpha \geq \beta$. Alors on a

$$a + b = p^\alpha a' + p^\beta b = p^\beta (p^{\alpha-\beta} a' + b').$$

C'est un produit de deux entiers relatifs. Par le premier point de la proposition, sa valuation est

$$v_p(a + b) = \beta + v_p(p^{\alpha-\beta} a' + b') \geq \beta = \min\{v_p(a), v_p(b)\}.$$

□

On déduit de cette proposition les décompositions suivantes du pgcd et du ppcm :

$$\text{pgcd}(a, b) = \prod_{p \in \mathbb{P}} p^{\min\{v_p(a), v_p(b)\}}, \quad \text{ppcm}(a, b) = \prod_{p \in \mathbb{P}} p^{\max\{v_p(a), v_p(b)\}}.$$

On retrouve ainsi la relation $\text{pgcd}(a, b) \cdot \text{ppcm}(a, b) = |ab|$ (proposition 6.18).

☞ *Exercices pouvant être traités :*

- exercice 6.1 
- exercice 6.2 
- exercice 6.3 
- exercice 6.4 
- exercice 6.6 
- exercice 6.8 
- exercice 6.15 

6.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$ et son arithmétique

6.2.1 Structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$

Dans le chapitre 3, nous avons défini le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$. Nous allons maintenant voir que ce groupe peut être muni d'une loi supplémentaire, la multiplication \times , qui est héritée de \mathbb{Z} , et que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Théorème 6.33

1. Si a, b, a', b' sont des entiers relatifs tels que $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors $ab \equiv a'b' \pmod{n}$. Autrement dit dans $\mathbb{Z}/n\mathbb{Z}$ on a :

$$(\bar{a} = \bar{a}' \quad \text{et} \quad \bar{b} = \bar{b}') \implies \overline{ab} = \overline{a'b'}.$$

2. Posons, pour \bar{a} et \bar{b} dans $\mathbb{Z}/n\mathbb{Z}$,

$$\bar{a} \times \bar{b} = \overline{ab}.$$

La loi \times est interne sur $\mathbb{Z}/n\mathbb{Z}$.

3. L'ensemble $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire, ce qui signifie :
- (a) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien, de neutre $\bar{0}$;
 - (b) la loi \times est associative, commutative, possède un élément neutre qui est $\bar{1}$;
 - (c) la loi \times est distributive par rapport à la loi $+$: $\bar{a} \times (\bar{b} + \bar{c}) = \bar{a} \times \bar{b} + \bar{a} \times \bar{c}$ pour tous $\bar{a}, \bar{b}, \bar{c}$ dans $\mathbb{Z}/n\mathbb{Z}$.
4. La surjection canonique $\pi : \mathbb{Z}/ \rightarrow \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \bar{a}$ est un morphisme d'anneaux unitaires, c'est-à-dire qu'elle satisfait : $\pi(1) = \bar{1}$ et pour tous a, b dans \mathbb{Z} ,

$$\pi(a + b) = \pi(a) + \pi(b), \quad \pi(ab) = \pi(a) \times \pi(b).$$

Démonstration. 1. Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors n divise à la fois $a - a'$ et $b - b'$. On écrit alors $a' = a + kn$ et $b' = b + ln$ avec k, l dans \mathbb{Z} et on a $a'b' = ab + (al + bk + kl)n$ d'où $a'b' \equiv ab \pmod{n}$.

2. Il faut s'assurer que la formule $\bar{a} \times \bar{b} = \overline{ab}$ définit sans ambiguïté une application $\times : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ c'est-à-dire que pour tout $x \in \bar{a}$ et $y \in \bar{b}$ on a $\overline{xy} = \overline{ab}$. Or c'est précisément le point précédent du théorème.
3. Montrons que $\bar{1}$ est l'élément neutre de \times : pour tout $a \in \mathbb{Z}$, on a $\bar{1} \times \bar{a} = \overline{1 \times a} = \bar{a}$ et de même, $\bar{a} \times \bar{1} = \bar{a}$. De plus il est clair que \times est associative, commutative et distributive par rapport à $+$: cela vient des propriétés analogues sur \mathbb{Z} par réduction modulo n .
4. On sait déjà que $\pi : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ est un morphisme de groupes. De plus on a évidemment $\pi(1) = \bar{1}$. Enfin par définition de \times , on a pour tous a, b dans \mathbb{Z} et par définition de la multiplication dans $\mathbb{Z}/n\mathbb{Z}$:

$$\pi(ab) = \overline{ab} = \bar{a} \times \bar{b} = \pi(a) \times \pi(b).$$

Donc π est un morphisme d'anneaux unitaires. □

Proposition 6.34

Soit $n \in \mathbb{N}$ d'écriture en base 10 :

$$n = n_0 + n_1 \times 10 + \cdots + n_k \times 10^k$$

avec n_0, \dots, n_k dans $\{0, \dots, 9\}$. Alors la somme $n_0 + \cdots + n_k$ des chiffres de n en base 10 est congrue à n modulo 9.

Démonstration. C'est un résultat classique, dont la démonstration est à connaître car le principe peut s'étendre à d'autres modulus. Il suffit de remarquer que $10 \equiv 1 \pmod{9}$ d'où $10^i \equiv 1^i \equiv 1 \pmod{9}$ pour tout entier $i \geq 0$. Ainsi on a :

$$\begin{aligned} n &\equiv n_0 + n_1 \times 10 + \cdots + n_k \times 10^k \pmod{9} \\ &\equiv n_0 + n_1 \times 1 + \cdots + n_k \times 1^k \pmod{9} \\ &\equiv n_0 + \cdots + n_k \pmod{9}. \end{aligned}$$

□

Il s'ensuit un critère bien connu des écoliers : un entier est divisible par 9 si et seulement si la somme de ses chiffres en base 10 est divisible par 9.

Remarque 6.35. La preuve par 9 s'étend à toutes les bases $b \geq 2$: il s'agit alors de regarder la somme des chiffres modulo $b - 1$.

6.2.2 Théorème des restes chinois

Ce théorème est aussi appelé simplement *théorème chinois*. Il apparaît dans un traité du mathématicien chinois Sun Tzu datant du troisième siècle de notre ère.

Théorème 6.36

Soient m et n deux entiers relatifs premiers entre eux. Pour tous x_1, x_2 dans \mathbb{Z} il existe un entier $x \in \mathbb{Z}$ tel que

$$\begin{cases} x \equiv x_1 \pmod{m} \\ x \equiv x_2 \pmod{n}. \end{cases}$$

De plus x est unique modulo mn : si y est une autre solution du système alors $y \equiv x \pmod{mn}$.

Ainsi si x est une solution particulière, l'ensemble des solutions du système est

$$\{x + mnk \mid k \in \mathbb{Z}\}.$$

Noter que cet ensemble de solutions est infini.

Démonstration. Comme m et n sont premiers entre eux, il existe u et v dans \mathbb{Z} tels que $mu + nv = 1$ (relation de Bézout). On en déduit $nv \equiv 1 \pmod{m}$ et $mu \equiv 1 \pmod{n}$. En posant $x = x_2mu + x_1nv$ on a donc

$$\begin{aligned}x &\equiv x_1nv \pmod{m} \\ &\equiv x_1 \pmod{m}\end{aligned}$$

et

$$\begin{aligned}x &\equiv x_2mu \pmod{n} \\ &\equiv x_2 \pmod{n}.\end{aligned}$$

Donc x est solution du système. Si y est une autre solution alors $x \equiv x_1 \equiv y \pmod{m}$ et $x \equiv x_2 \equiv y \pmod{n}$ d'où $x - y \equiv 0 \pmod{m}$ et $x - y \equiv 0 \pmod{n}$. On en déduit que m et n divisent $x - y$. Donc leur ppcm divise $x - y$. Or m et n étant premiers entre eux, leur ppcm est mn , ce qui termine la preuve. \square

La démonstration précédente est à connaître pour la raison suivante : pour résoudre un système donné, on peut procéder comme dans cette démonstration en commençant par établir une relation de Bézout entre m et n , puis en déduisant une solution particulière.

Remarque 6.37. 1. Le couple de Bézout (u, v) utilisé dans la démonstration n'est pas unique. Si (u', v') est un autre couple alors $x' = x_2mu' + x_1nv'$ est la solution particulière qui s'en déduit. Elle vérifie $x' \equiv x \pmod{mn}$. Cependant l'ensemble des solutions sera inchangé car :

$$\{x + mnk \mid k \in \mathbb{Z}\} = x + mn\mathbb{Z} = x' + mn\mathbb{Z} = \{x' + mnk' \mid k' \in \mathbb{Z}\}.$$

2. Le théorème signifie que le système à deux congruences se ramène à une unique congruence modulo mn . Par récurrence, l'énoncé se généralise facilement à un système de congruences modulo m_1, \dots, m_k , où ces entiers sont *premiers entre eux deux à deux*.

Le théorème chinois admet une reformulation en termes d'anneaux. Si A et B sont deux anneaux commutatifs unitaires, on peut munir le produit cartésien $A \times B$ d'une structure d'anneau héritée de celles sur A et B . L'addition et la multiplication sont définies en posant, pour tous a, a' dans A et b, b' dans B :

$$(a, b) + (a', b') = (a + a', b + b') \quad \text{et} \quad (a, b)(a', b') = (aa', bb').$$

L'élément neutre pour l'addition est $(0_A, 0_B)$ et l'élément neutre pour la multiplication est $(1_A, 1_B)$. On a ainsi une structure d'anneau commutatif unitaire sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proposition 6.38

Soient n et m deux entiers naturels et premiers entre eux. L'application

$$f : \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x \bmod mn & \longmapsto & (x \bmod m, x \bmod n) \end{array}$$

est un isomorphisme d'anneaux, c'est-à-dire que f est une application bijective vérifiant pour tous x, y dans \mathbb{Z} ,

$$\begin{aligned} f((x + y) \bmod mn) &= f(x \bmod mn) + f(y \bmod mn) \\ f(xy \bmod mn) &= f(x \bmod mn)f(y \bmod mn) \\ f(1 \bmod mn) &= (1_{\mathbb{Z}/m\mathbb{Z}}, 1_{\mathbb{Z}/n\mathbb{Z}}). \end{aligned}$$

Démonstration. Montrons que $x \bmod mn \mapsto (x \bmod m, x \bmod n)$ définit une application de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Si $x \equiv x' \pmod{mn}$ alors mn divise $x - x'$, donc m et n divisent $x - x'$, ce qui entraîne $x \equiv x' \pmod{m}$ et $x \equiv x' \pmod{n}$. Donc on a bien l'application f comme dans l'énoncé. Elle est surjective d'après le théorème chinois (existence d'une solution pour chaque système) et injective car deux solutions d'un système diffèrent d'un multiple de mn . Noter que la démonstration du théorème chinois (théorème 6.36) fournit l'application réciproque de f :

$$f^{-1} : \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/mn\mathbb{Z} \\ (x_1 \bmod m, x_2 \bmod n) & \longmapsto & x_2mu + x_1nv \end{array}$$

si $mu + nv = 1$ est une relation de Bézout entre u et v . Enfin on vérifie de manière directe que f est un morphisme d'anneaux. \square

Remarque 6.39. L'isomorphisme d'anneaux de cette proposition est en particulier un isomorphisme de groupes de $(\mathbb{Z}/mn\mathbb{Z}, +)$ dans $(\mathbb{Z}/m\mathbb{Z}, +) \times (\mathbb{Z}/n\mathbb{Z}, +)$.

 *Exercices pouvant être traités :*

- exercice 6.5  
- exercice 6.7  
- exercice 6.9 
- exercice 6.10 
- exercice 6.11 
- exercice 6.12 

6.2.3 Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/n\mathbb{Z}$ **Définition 6.40**

Soit n un entier naturel, $n \geq 1$. Un élément \bar{x} de $\mathbb{Z}/n\mathbb{Z}$ est dit *inversible* s'il existe $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{x}\bar{y} = \bar{1}$ dans $\mathbb{Z}/n\mathbb{Z}$. L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^\times$.

- Exemple 6.41.**
1. $\bar{0}$ n'est jamais inversible (ainsi $(\mathbb{Z}/n\mathbb{Z}, \times)$ n'est pas un groupe);
 2. $\bar{3} \in (\mathbb{Z}/5\mathbb{Z})^\times$ car $\bar{3} \times \bar{2} = \bar{6} = \bar{1}$ dans $\mathbb{Z}/5\mathbb{Z}$;
 3. $\bar{2} \notin (\mathbb{Z}/4\mathbb{Z})^\times$ car $\bar{0} \times \bar{2} = \bar{0} \neq \bar{1}$, $\bar{1} \times \bar{2} = \bar{2} \neq \bar{1}$, $\bar{2} \times \bar{2} = \bar{4} = \bar{0} \neq \bar{1}$ et $\bar{3} \times \bar{2} = \bar{6} = \bar{2} \neq \bar{1}$ dans $\mathbb{Z}/4\mathbb{Z}$.

Proposition 6.42

$((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est un groupe abélien, d'élément neutre $\bar{1}$.

Démonstration. Cet ensemble est non vide car il contient $\bar{1}$. Montrons que la multiplication est une loi interne sur $(\mathbb{Z}/n\mathbb{Z})^\times$ c'est-à-dire que si x_1 et x_2 sont inversibles alors x_1x_2 l'est aussi. Si x_1 et x_2 appartiennent à $(\mathbb{Z}/n\mathbb{Z})^\times$, il existe y_1 et y_2 dans $(\mathbb{Z}/n\mathbb{Z})^\times$ tels que $x_1y_1 = \bar{1}$ et $x_2y_2 = \bar{1}$. On en déduit $x_1x_2y_1y_2 = x_1y_1x_2y_2 = \bar{1} \times \bar{1} = \bar{1}$ d'où $x_1x_2 \in (\mathbb{Z}/n\mathbb{Z})^\times$. Enfin la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ étant associative, commutative, d'élément neutre $\bar{1}$ et tout élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ admettant un inverse dans $(\mathbb{Z}/n\mathbb{Z})^\times$, cela fait de $(\mathbb{Z}/n\mathbb{Z})^\times, \times$ un groupe abélien. \square

Le théorème suivant donne une description des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 6.43

On a

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{x} \in \mathbb{Z}/n\mathbb{Z} \mid 1 \leq x \leq n, \text{pgcd}(x, n) = 1\}.$$

Démonstration. Il faut d'abord se convaincre qu'on peut parler sans ambiguïté de $\text{pgcd}(x, n)$ si $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$, c'est-à-dire que ce pgcd ne dépend pas du choix du représentant choisi dans la classe \bar{x} . Si y est un entier dans la classe \bar{x} alors x et y sont congrus modulo n . Il existe donc $k \in \mathbb{Z}$ tel que $x = y + kn$, d'où $\text{pgcd}(x, n) = \text{pgcd}(y, n)$ par le corollaire 6.14. Cela prouve l'assertion voulue.

Maintenant pour x entier avec $1 \leq x \leq n$, on a

$$\begin{aligned} \text{pgcd}(x, n) = 1 &\stackrel{\text{Bézout}}{\iff} \exists(u, v) \in \mathbb{Z} \times \mathbb{Z}, xu + nv = 1 \\ &\iff \exists u \in \mathbb{Z}, xu \equiv 1 \pmod{n} \\ &\iff \exists u \in \mathbb{Z}, \bar{x}\bar{u} = \bar{1} \text{ dans } \mathbb{Z}/n\mathbb{Z} \\ &\iff \bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times. \end{aligned}$$

\square

Exemple 6.44. $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$; $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

Corollaire 6.45

Si p est premier alors $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\} = \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}$. C'est un groupe d'ordre $p - 1$.

En pratique, pour calculer l'inverse d'une classe inversible \bar{x} , on procède comme dans la démonstration du théorème : on établit une relation de Bézout $xu + nv = 1$ entre les entiers x et n (par exemple en utilisant l'algorithme d'Euclide étendu) puis on conclut que $\bar{x}^{-1} = \bar{u}$. Voir l'exercice 6.13.

Définition 6.46

Si $n \geq 1$, on pose

$$\varphi(n) = \text{Card}((\mathbb{Z}/n\mathbb{Z})^\times) = \text{Card}\{1 \leq x \leq n, \text{pgcd}(x, n) = 1\}.$$

La fonction $\varphi : \mathbb{N} - \{0\} \rightarrow \mathbb{N}$ est appelée l'*indicatrice d'Euler* ou *fonction phi d'Euler*.

Remarque 6.47. En vertu de l'exercice 6.5, $\varphi(n)$ est aussi le nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proposition 6.48

1. Si m et n sont premiers entre eux, on a $\varphi(mn) = \varphi(m)\varphi(n)$.
2. Si p est premier et $r \geq 1$, on a $\varphi(p^r) = p^{r-1}(p - 1)$.

Démonstration. Les démonstrations des deux assertions sont à connaître.

1. Comme m et n sont premiers entre eux, le théorème chinois (proposition 6.38) donne un isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. On peut montrer qu'il entraîne un isomorphisme de groupes multiplicatifs :

$$(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

donc une bijection entre ces ensembles. En passant aux cardinaux, l'égalité voulue en découle.

2. Comme p est premier, on a

$$\varphi(p^r) = \text{Card}\{1 \leq x \leq p^r \mid \text{pgcd}(x, p^r) = 1\} = \text{Card}\{1 \leq x \leq p^r, p \nmid x\}.$$

Or le nombre d'entiers entre 1 et p^r qui sont divisibles par p est p^{r-1} (ce sont les $p, 2p, 3p, \dots, p^{r-1}p$). On en déduit

$$\begin{aligned} \varphi(p^r) &= \text{Card}\{1 \leq x \leq p^r\} - \text{Card}\{1 \leq x \leq p^r, p \mid x\} \\ &= p^r - p^{r-1} = p^{r-1}(p - 1). \end{aligned}$$

□

Exemple 6.49. 1. On a $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2(2 - 1) = 2$, $\varphi(5) = 4$, $\varphi(6) = \varphi(2)\varphi(3) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = \varphi(2)\varphi(5) = 4$.

2. Si n est impair alors $\varphi(2n) = \varphi(n)$.

En combinant les deux énoncés de la proposition, on obtient la formule générale suivante. Si $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ est la décomposition en facteurs premiers :

$$\varphi(n) = \prod_{p \in \mathbb{P}, p|n} p^{v_p(n)-1}(p-1) = n \prod_{p \in \mathbb{P}, p|n} \left(1 - \frac{1}{p}\right).$$

Nous terminons par deux énoncés classiques d'arithmétique, qui peuvent être vus comme une conséquence de la théorie des groupes.

Théorème 6.50

1. (Théorème d'Euler) Soit $n \geq 1$ et soit a entier premier avec n alors on a

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

2. (Théorème de Fermat) Soit p un nombre premier et soit a un entier non divisible par p alors on a

$$a^{p-1} \equiv 1 \pmod{p}.$$

En particulier on a $a^p \equiv a \pmod{p}$ pour tout entier a .

Démonstration. Ces démonstrations sont à connaître.

1. Comme a est premier avec n , \bar{a} est inversible dans $\mathbb{Z}/n\mathbb{Z}$ donc $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Or le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est d'ordre $\varphi(n)$. On conclut grâce au théorème de Lagrange.
2. La première formule est le théorème d'Euler dans le cas où $n = p$ est premier, puisque $\varphi(p) = p - 1$. La seconde formule est immédiate si a est divisible par p (c'est $0 \equiv 0 \pmod{p}$); sinon elle s'obtient à partir de $a^{p-1} \equiv 1 \pmod{p}$ en multipliant par a de part et d'autre de la congruence.

□

Exemple 6.51. Calculons le dernier chiffre en base 10 de 17^{22} . Il s'agit de calculer $17^{22} \pmod{10}$ c'est-à-dire $7^{22} \pmod{10}$ puisque $17 \equiv 7 \pmod{10}$. Comme 7 et 10 sont premiers entre eux, le théorème d'Euler dit que $7^{\varphi(10)} \equiv 1 \pmod{10}$. Or $\varphi(10) = 4$. Donc pour tout $a \in \mathbb{Z}$, on a $7^a \equiv 7^r \pmod{10}$ où r désigne le reste de la division euclidienne de a par 4. On applique ce résultat à $a = 22$: son reste est 2. Donc $7^{22} \equiv 7^2 \equiv 49 \equiv 9 \pmod{10}$. Le dernier chiffre cherché est 9.

Remarque 6.52. Il existe plusieurs types de contre-exemples à une réciproque du théorème de Fermat. Par exemple on a $2^{340} \equiv 1 \pmod{341}$ mais $341 = 11 \times 31$ n'est pas premier. On peut aussi montrer que tout $a \in (\mathbb{Z}/561\mathbb{Z})^\times$ vérifie $a^{560} \equiv 1 \pmod{561}$ mais $561 = 3 \times 11 \times 17$ n'est pas premier. Le nombre 561 est un exemple de nombre de Carmichael.

☞ *Exercices pouvant être traités :*

— exercice 6.13 

- exercice 6.14 
- exercice 6.16  
- exercice 6.17 
- exercice 6.18  

6.3 Constructions de \mathbb{N} et de \mathbb{Z}

Cette partie présente des constructions possibles pour les ensembles \mathbb{N} et \mathbb{Z} ainsi que des démonstrations de la plupart de leurs propriétés.

6.3.1 Construction de \mathbb{N} par l'axiomatique de Peano

Nous choisissons une présentation basée sur l'axiomatique de Peano.

Axiome 6.1 (Axiomes de Peano). Il existe un ensemble \mathbb{N} , dont les éléments sont appelés les *entiers naturels*, qui a les propriétés suivantes :

1. il existe un élément 0 dans \mathbb{N} , appelé *zéro* ;
2. il existe une application *successeur* injective $s : \mathbb{N} \rightarrow \mathbb{N}$ telle que $0 \notin s(\mathbb{N})$;
3. si une partie A de \mathbb{N} vérifie $0 \in A$ et $s(A) \subset A$ alors $A = \mathbb{N}$.

La troisième propriété est connue sous le nom de *principe de récurrence* bien qu'il s'agisse, avec cette construction, d'un axiome et non d'un théorème.

On note $1 = s(0)$, $2 = s(1) = s(s(0))$, $3 = s(2)$, etc. Nous allons montrer à partir des axiomes de Peano, les propriétés de \mathbb{N} .

Proposition 6.53

Tout entier naturel non nul est le successeur d'un entier naturel c'est-à-dire $\mathbb{N} - \{0\} = s(\mathbb{N})$.

Démonstration. Il suffit de démontrer que $s(\mathbb{N}) \cup \{0\} = \mathbb{N}$, ce qu'on fait avec le principe de récurrence appliqué à $A = s(\mathbb{N}) \cup \{0\}$: on a $0 \in A$ et $s(A) = s(s(\mathbb{N})) \cup s(\{0\}) \subset s(\mathbb{N}) - \{0\}$ d'après l'axiome 2. Donc $s(A) \subset A$ d'où le résultat. \square

Remarque 6.54. D'autres constructions sont possibles, comme celle dite de von Neumann à partir des axiomes de la théorie des ensembles : les entiers sont alors définis comme des ensembles et plus précisément : $0 = \emptyset$, puis $1 = \{\emptyset\}$ (l'ensemble dont l'unique élément est l'ensemble vide), puis $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$, $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$, etc.

L'addition

Proposition 6.55

Il existe une application $+$: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ donnée par :

1. pour tout $n \in \mathbb{N}$, $n + 0 = n$;
2. pour tous n et m dans \mathbb{N} , $n + s(m) = s(n + m)$.

Démonstration. Montrons que ces formules définissent bien une application de $\mathbb{N} \times \mathbb{N}$ dans \mathbb{N} c'est-à-dire que l'ensemble $A = \{m \in \mathbb{N} \mid n + m \text{ est défini}\}$ satisfait $A = \mathbb{N}$. Comme A contient 0 (axiome 1) et est stable par successeur (axiome 2), cela résulte du principe de récurrence. \square

On a, par définition, $n + 1 = n + s(0) = s(n + 0) = s(n)$. L'application successeur est donc l'application qui consiste à ajouter 1. Par exemple on a $2 = s(1) = 1 + 1$.

Proposition 6.56

1. L'addition est associative : pour tous a, b, c dans \mathbb{N} , on a $a + (b + c) = (a + b) + c$.
2. Pour tout $a \in \mathbb{N}$, on a $a + 0 = a = 0 + a$.
3. L'addition est commutative : pour tous a, b dans \mathbb{N} on a $a + b = b + a$.
4. Pour tous a, b, c , dans \mathbb{N} , on a $a + b = a + c \implies b = c$ (règle de simplification).
5. Si $a + b = 0$ avec a et b dans \mathbb{N} alors $a = b = 0$.

Démonstration. 1. Fixons a et b . Soit $C = \{c \in \mathbb{N} \mid a + (b + c) = (a + b) + c\}$. Montrons que $C = \mathbb{N}$ en utilisant le principe de récurrence. On a $0 \in C$: en effet, on a $a + (b + 0) = a + b = (a + b) + 0$ par définition de $+$. Montrons maintenant que $s(C) \subset C$. Soit $c \in C$. On a $a + (b + s(c)) = a + s(b + c) = s(a + (b + c))$ par définition de $+$. Comme $c \in C$ et par définition de $+$, on a $s(a + (b + c)) = s((a + b) + c) = (a + b) + s(c)$. Donc $s(c) \in C$, ce qu'il fallait démontrer. Par le principe de récurrence on conclut $C = \mathbb{N}$.

2. On a $a + 0 = a$ par définition de $+$. Soit $A = \{a \in \mathbb{N} \mid 0 + a = a\}$. Montrons que $A = \mathbb{N}$ en utilisant le principe de récurrence. On a $0 \in A$: en effet, on a $0 = 0 + 0$ par définition de $+$. Montrons que $s(A) \subset A$. Soit $a \in A$. Alors on a $0 + s(a) = s(0 + a)$, par définition de $+$, puis $s(0 + a) = s(a)$ car $a \in A$. Cela prouve que $s(a) \in A$, ce qui conclut.

3. Lemme 6.57

┆ Pour tous a et b dans \mathbb{N} on a $s(a) + b = s(a + b)$.

Démonstration. Voir l'exercice 6.19. \square

Soit $B = \{b \in \mathbb{N} \mid \forall a \in \mathbb{N}, a + b = b + a\}$. Montrons que $B = \mathbb{N}$ en utilisant le principe de récurrence. On a $0 \in B$ par le deuxième point de la proposition. Montrons que si $b \in B$ alors $s(b) \in B$. Pour tout $a \in \mathbb{N}$, on a $a + s(b) = s(a + b)$ par définition de $+$, puis $s(a + b) = s(b + a)$ car $b \in B$, et enfin $s(b + a) = s(b) + a$ en utilisant le lemme, ce qui montre bien que $s(b) \in B$. On conclut que $B = \mathbb{N}$.

4. Voir l'exercice 6.19.

5. Raisonnons par l'absurde : si $a \neq 0$ et $b \neq 0$, il existe α et β dans \mathbb{N} tels que $a = s(\alpha)$ et $b = s(\beta)$ par la proposition 6.53. On a alors $a + b = s(\alpha) + s(\beta) = s(s(\alpha) + \beta)$ par définition de $+$, donc $0 = a + b$ est successeur d'un entier naturel. Cela contredit le premier axiome de Peano. \square

Exemple 6.58. En utilisant l'associativité, démontrons que $2 + 2 = 4$: en effet on a $4 = s(3) = 3 + 1 = (2 + 1) + 1 = 2 + (1 + 1) = 2 + 2$.

La multiplication

Proposition 6.59

Il existe une application $\times : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ donnée par :

1. pour tout $n \in \mathbb{N}$, $n \times 0 = 0$;
2. pour tous n et m dans \mathbb{N} , $n \times s(m) = n \times m + n$.

Démonstration. On démontre comme pour l'addition que ces formules définissent bien une application de $\mathbb{N} \times \mathbb{N}$ dans \mathbb{N} en utilisant le principe de récurrence. \square

Proposition 6.60

1. La multiplication est distributive par rapport à l'addition : pour tous a, b, c dans \mathbb{N} , on a $a \times (b + c) = a \times b + a \times c$ et $(a + b) \times c = a \times c + b \times c$.
2. La multiplication est associative : pour tous a, b, c dans \mathbb{N} , on a $a \times (b \times c) = (a \times b) \times c$.
3. Pour tout $a \in \mathbb{N}$, on a $a \times 1 = a = 1 \times a$.
4. La multiplication est commutative : pour tous a et b dans \mathbb{N} on a $a \times b = b \times a$.
5. Pour tous a et b dans \mathbb{N} on a $ab = 0 \implies a = 0$ ou $b = 0$.
6. Pour tous a, b, c dans \mathbb{N} avec $a \neq 0$, on a $ab = ac \implies b = c$ (règle de simplification).

Démonstration. On procède comme pour l'addition en utilisant le principe de récurrence. Les détails sont laissés aux lecteurs. \square

La relation d'ordre \leq

Définition 6.61

Pour a et b dans \mathbb{N} , on note $a \leq b$ s'il existe $c \in \mathbb{N}$ tel que $b = a + c$.

Proposition 6.62

La relation \leq est une relation d'ordre total sur \mathbb{N} .

Démonstration. La relation est réflexive : on a $a \leq a$ car $a = a + 0$. De plus elle est transitive : si $a \leq b$ et $b \leq c$ alors il existe d et e dans \mathbb{N} tels que $b = a + d$ et $c = b + e$, d'où $c = a + (d + e)$ c'est-à-dire $a \leq c$. Enfin elle est antisymétrique : si $a \leq b$ et $b \leq a$ alors il existe c et d dans \mathbb{N} tels que $b = a + c$ et $a = b + d$, d'où $b = b + (c + d)$ ce qui entraîne $c + d = 0$ par la règle de simplification de l'addition, puis $c = d = 0$ par propriété de l'addition. Donc on a $b = a$.

Montrons que l'ordre est total, c'est-à-dire que tous entiers a et b satisfont $a \leq b$ ou $b \leq a$. Fixons b et considérons l'ensemble $A = \{a \in \mathbb{N} \mid a \leq b \text{ ou } b \leq a\}$. Montrons que $A = \mathbb{N}$ en utilisant le principe de récurrence. On a $0 \in A$ car $0 \leq b$, par définition de \leq . Supposons maintenant $a \in A$. Distinguons deux cas.

- Si $a \leq b$ et $a \neq b$, alors il existe $c \in \mathbb{N}$, $c \neq 0$, tel que $b = a + c$. La proposition 6.53 assure l'existence de $d \in \mathbb{N}$ tel que $c = s(d) = d + 1$ d'où $b = a + 1 + d = s(a) + d$. Cela montre que $s(a) \leq b$.
- Supposons $b \leq a$, alors il existe $c \in \mathbb{N}$ tel que $a = b + c$ donc $s(a) = a + 1 = b + (1 + c)$, ce qui prouve que $b \leq s(a)$.

Dans tous les cas on a bien $s(a) \in A$, ce qui conclut. \square

Si $a \leq b$, on note $b - a$ l'unique entier $c \in \mathbb{N}$ tel que $b = a + c$. On écrit $a < b$ lorsque $a \leq b$ et $a \neq b$. De même on note $a \geq b$ pour dire $b \leq a$, et enfin $a > b$ pour dire $b < a$.

Théorème 6.63

L'ensemble ordonné (\mathbb{N}, \leq) est bien ordonné i.e. toute partie non vide de \mathbb{N} admet un plus petit élément. De plus toute partie non vide finie de \mathbb{N} a un plus grand élément.

Démonstration. Démontrons que si une partie A ne possède pas de plus petit élément alors A est vide i.e. son complémentaire est \mathbb{N} . Notons B ce complémentaire. On a $0 \in B$ (sinon 0 serait le plus petit élément de A). Soit $b \in B$ et montrons que $s(b) = b + 1 \in B$. On sait qu'aucun des entiers $0, 1, \dots, b$ n'est dans A , il s'agit de voir que $b + 1$ n'y est pas non plus. S'il y était alors $b + 1$ serait le plus petit élément de A , contrairement à l'hypothèse. Donc $b + 1 \in B$ et on conclut $B = \mathbb{N}$ par le principe de récurrence. Pour la démonstration de la deuxième assertion du théorème, voir l'exercice 6.20. \square

On peut établir d'autres propriétés usuelles de \leq , dont les démonstrations sont omises ici.

Proposition 6.64

1. Pour tous a, b, c dans \mathbb{N} , on a $a + b \leq a + c \iff b \leq c$.
2. Il n'existe aucun entier naturel a tel que $0 < a < 1$.
3. Il n'existe aucun entier naturel supérieur à tous les autres.
4. Si $a \leq b$ alors $ac \leq bc$ pour tout $c \in \mathbb{N}$.

Corollaire 6.65

Si a et b dans \mathbb{N} vérifient $ab = 1$ alors $a = 1$ et $b = 1$.

Démonstration. Si $ab = 1$ alors a et b sont non nuls donc $a \geq 1$ et $b \geq 1$. Si l'un deux, par exemple a , était supérieur ou égal à 2 alors ab serait supérieur ou égal à $2b$ donc $ab \geq 2$, ce qui contredit $ab = 1$. Donc $a = 1$ et $b = 1$. \square

On termine ce paragraphe avec la propriété achimédienne pour \leq .

Théorème 6.66

La relation d'ordre \leq sur \mathbb{N} est *archimédienne* : pour tout $x \in \mathbb{N}$ et pour tout $n \in \mathbb{N} - \{0\}$, il existe $k \in \mathbb{N}$ tel que $kn \geq x$.

Démonstration. Soient $x \in \mathbb{N}$ et $n \in \mathbb{N} - \{0\}$. Si $x \leq n$ alors $k = 1$ convient. Si $x > n$ considérons l'ensemble

$$B = \{cn \mid c \in \mathbb{N}, 1 \leq cn < x\}.$$

Il est non vide, car il contient $n = 1 \times n$, et fini car majoré par x . Donc il admet un plus grand élément, noté cn . Posons $k = s(c) = c + 1$. Alors on a $kn \geq x$ par maximalité de cn dans B . \square

Remarque 6.67. La multiplication permet de définir une autre relation d'ordre sur \mathbb{N} , celle de divisibilité : on écrit $a \mid b$ lorsqu'il existe $c \in \mathbb{N}$ tel que $b = c \times a$. Dans ce cas, l'entier naturel c est noté $\frac{b}{a}$. On vérifie que c'est une relation d'ordre partielle sur \mathbb{N} .

6.3.2 Construction de \mathbb{Z} par symétrisation

L'ensemble $(\mathbb{N}, +)$ n'est pas un groupe car les éléments $n \in \mathbb{N} - \{0\}$ n'ont pas d'opposé dans \mathbb{N} . On construit l'ensemble \mathbb{Z} pour palier ce manque. Pour cela on considère la relation suivante sur $\mathbb{N} \times \mathbb{N}$:

$$(m, n)\mathcal{R}(m', n') \iff m + n' = n + m'.$$

On vérifie sans difficulté que \mathcal{R} est une relation d'équivalence sur $\mathbb{N} \times \mathbb{N}$.

Définition 6.68

On définit \mathbb{Z} comme l'ensemble quotient $(\mathbb{N} \times \mathbb{N})/\mathcal{R}$. Ses éléments sont appelés les *entiers relatifs*.

On note $[m, n]$ la classe d'équivalence d'un élément $(m, n) \in \mathbb{N} \times \mathbb{N}$. Par exemple on a $[0, 4] = [1, 5] = [2, 6]$ et $[5, 2] = [4, 1] = [3, 0]$.

Proposition 6.69

Soit $z = [m, n]$ une classe d'équivalence dans \mathbb{Z} .

1. Si $m \leq n$ alors $z = [m - n, 0]$.
2. Si $n \leq m$ alors $z = [0, n - m]$.
3. On a $[m, 0] = [n, 0]$ si et seulement si $m = n$. De même on a $[0, m] = [0, n]$ si et seulement si $m = n$.

Démonstration. Immédiate à partir de la définition de \mathcal{R} . \square

Cette proposition entraîne que

$$\mathbb{Z} = \{[m, 0] \mid m \in \mathbb{N}\} \cup \{[0, n] \mid n \in \mathbb{N}\}.$$

On en déduit deux injections de \mathbb{N} dans \mathbb{Z} : $m \mapsto [m, 0]$ et $n \mapsto [0, n]$. On notera simplement m l'élément $[m, 0]$ et $-n$ l'élément $[0, n]$. Par exemple $[2, 6] = [0, 4] = -4$ et $[5, 2] = [3, 0] = 3$.

Proposition 6.70

Il existe une application $+$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ donnée par :

$$[m, n] + [p, q] = [m + p, n + q].$$

et une application \times : $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ donnée par :

$$[m, n] \times [p, q] = [mp + nq, mq + np].$$

Démonstration. On vérifie sans souci que ces applications sont bien définies c'est-à-dire que leur résultat ne dépend pas des représentants choisis dans les classes $[m, n]$ et $[p, q]$. \square

En notant comme auparavant m pour $[m, 0]$ et $-n$ pour $[0, n]$, on écrira simplement $m + n$ leur somme, $m \times n$ leur produit, et $m - n$ au lieu de $m + (-n)$. On démontre ensuite que toutes les propriétés classiques de \mathbb{Z} muni de $+$ et \times sont vérifiées. En particulier :

- l'élément neutre de $+$ est $[0, 0] = 0 = -0$ et l'opposé de m est $-m$. Ainsi $(\mathbb{Z}, +)$ est un groupe abélien.
- l'élément neutre de \times est $[1, 0] = 1$.

On étend la relation d'ordre \leq en une relation d'ordre total sur \mathbb{Z} , qui hérite de la propriété archimédienne.

 *Exercices pouvant être traités :*

- exercice 6.19   
- exercice 6.20   

Annexe 1 : relation d'équivalence, ensemble quotient

Définition. Soit E un ensemble. Une *relation binaire* sur E est une partie Γ de $E \times E$. On dit de deux éléments x et y de E qu'ils *satisfont la relation binaire* lorsque $(x, y) \in \Gamma$, ce qu'on note xRy .

Une relation binaire est donc décrite par l'ensemble des couples d'éléments satisfaisant cette relation.

Exemple. $\Gamma = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \text{ divise } y\}$ est une relation binaire sur \mathbb{Z} .

Définition. Soit E un ensemble. Une *relation d'équivalence* sur E est une relation binaire R sur E qui est

1. *réflexive* : pour tout $x \in E$ on a xRx ;
2. *symétrique* : xRy implique yRx ;
3. *transitive* : xRy et yRz impliquent xRz .

Exemple. 1. Soit E l'ensemble des parties finies de \mathbb{N} . La relation « avoir même cardinal » est une relation d'équivalence sur E .

2. Soit $E = M_{n,m}(K)$ l'ensemble des matrices à n lignes, m colonnes et coefficients dans un corps K . La relation définie par

$$A \sim B \iff \exists P \in \text{GL}_m(K), \exists Q \in \text{GL}_n(K), B = Q^{-1}AP$$

est une relation d'équivalence sur E . C'est la notion d'équivalence sur les matrices qui a été vue en algèbre linéaire.

Définition. Soit E un ensemble muni d'une relation d'équivalence R . Pour $x \in E$ on appelle *classe d'équivalence de x* le sous-ensemble de E défini par

$$\text{cl}(x) = \{y \in E \mid xRy\}.$$

Exemple. Reprenons $E = M_{n,m}(K)$ muni de la relation d'équivalence matricielle. Soit $A \in M_{n,m}(K)$ une matrice fixée. D'après le cours d'algèbre linéaire (pivot de Gauss, par exemple), la classe d'équivalence de A est formée des matrices de $M_{n,m}(K)$ ayant même rang que A .

Proposition. 1. On a $x \in \text{cl}(x)$.

2. Pour tous $x, y \in E$, on a

$$xRy \iff \text{cl}(x) = \text{cl}(y) \iff x \in \text{cl}(y).$$

3. Pour tous x, y dans E , on a l'alternative : $\text{cl}(x) = \text{cl}(y)$ ou $\text{cl}(x) \cap \text{cl}(y) = \emptyset$.

Définition. Soit E un ensemble muni d'une relation d'équivalence R . L'ensemble quotient de E par R est l'ensemble des classes d'équivalence d'éléments de E . On le note E/R .

L'application naturelle :

$$\begin{aligned} E &\longrightarrow E/R \\ x &\longmapsto \text{cl}(x) \end{aligned}$$

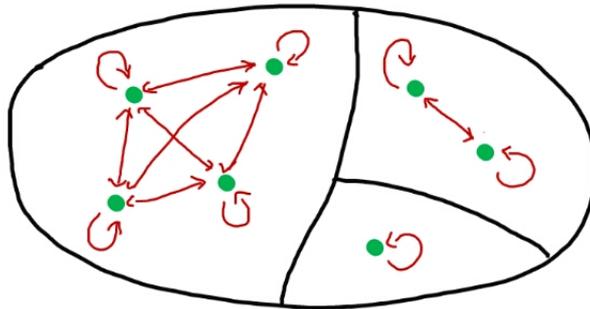
est surjective par définition de E/R et s'appelle la *surjection canonique* de E sur E/R .

D'après la proposition, les classes d'équivalence forment une partition de E :

$$E = \bigsqcup_{C \in E/R} C \quad (6.2)$$

où le symbole \bigsqcup signifie que la réunion est disjointe (les sous-ensembles considérés sont deux à deux disjoints).

Exemple 6.71. L'exemple suivant représente graphiquement un ensemble E à 7 éléments (points verts) muni d'une relation d'équivalence représentée par les doubles-flèches rouges. Elle comporte trois classes d'équivalence avec 1, 2 et 4 éléments respectivement, qui forment une partition de l'ensemble E . Ici on a $\text{Card}(E/R) = 3$.



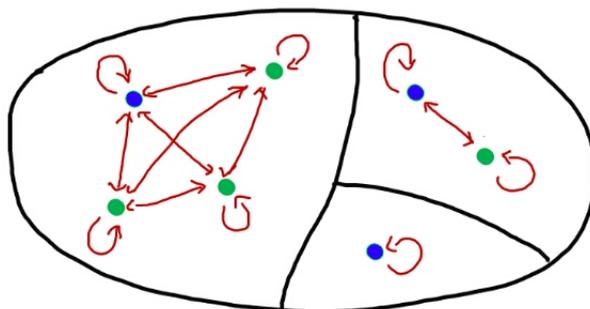
Pour rendre l'écriture (6.2) plus aisément manipulable, il peut être utile de passer par un système de représentants.

Définition. On appelle *représentant* d'une classe d'équivalence n'importe quel élément de cette classe d'équivalence. Un *système de représentants* des classes est toute partie de E qui contient exactement un représentant par classe d'équivalence.

Soit $(x_i)_{i \in I}$ un système de représentants des classes d'équivalence (selon la situation, son existence est avérée ou repose sur l'axiome du choix). La relation (6.2) se réécrit alors

$$E = \bigsqcup_{i \in I} \text{cl}(x_i).$$

Exemple. 1. Dans l'exemple graphique précédent, l'ensemble des points bleus constitue un système de représentants.



2. Reprenons $E = M_{n,m}(K)$ muni de la relation d'équivalence matricielle. Un système de représentants est fourni par la famille de matrices

$$J_r = \begin{pmatrix} I_r & 0_{r,m-r} \\ 0_{n-r,r} & 0_{n-r,m-r} \end{pmatrix}$$

pour $0 \leq r \leq \min(n, m)$. En effet d'après un théorème d'algèbre linéaire, toute matrice de E de rang $r \in \{0, \dots, \min(n, m)\}$ est équivalente à J_r ; de plus si $r \neq r'$ les matrices J_r et $J_{r'}$ ne sont pas équivalentes.

Annexe 2 : synthèse des groupes rencontrés

Le tableau suivant récapitule les principaux groupes rencontrés dans le cours : groupes particuliers puis procédés de constructions de groupes. La lettre K désigne un corps commutatif.

GROUPE	RÉFÉRENCE
Groupe symétrique \mathcal{S}_E d'un ensemble E	définition 1.1
Groupe symétrique \mathcal{S}_n	page 3
Groupe alterné \mathcal{A}_n	définition 1.30
$(\mathbb{Z}, +)$, $(K, +)$	exemple 2.3
$(K[X], +)$	exemple 2.3
(K^*, \cdot)	exemple 2.3
$(E, +)$ où E est un K -espace vectoriel	exemple 2.3
$(M_n(K), +)$	exemple 2.3
Groupe linéaire $(\mathrm{GL}_n(K), \cdot)$	exemple 2.3
Groupe spécial linéaire $(\mathrm{SL}_n(K), \cdot)$	exemple 2.21
$(\mathbb{Z}/n\mathbb{Z}, +)$	définition 3.11
Groupe (U_n, \cdot) des racines n -èmes complexes de l'unité	exemple 2.25
Groupe (U, \cdot) des nombres complexes de module 1	exemple 4.15
Groupe diédral D_n à $2n$ éléments	définition 4.29
Groupe $(\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ des inversibles modulo n	définition 6.40
Groupe des automorphismes $(\mathrm{Aut}(G), \circ)$ d'un groupe G	définition 2.11, prop. 2.16
Produit direct $\prod_{i \in I} G_i$ de groupes $(G_i)_{i \in I}$	définition 2.40
Groupe quotient G/H où H est un sous-groupe normal de G	théorème 4.8
Produit semi-direct $H_1 \rtimes H_2$ de deux sous-groupes	définition 4.24

Il est conseillé de faire le même exercice de recensement pour les procédés de construction de sous-groupes vus dans le cours (par exemple : intersection de sous-groupes, noyau d'un morphisme,...).

Deuxième partie

Algèbre 1
Les exercices

Exercices du chapitre 1

Exercice 1.1 (Manipulations élémentaires).

1. On considère les permutations suivantes dans \mathcal{S}_9 :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 6 & 5 & 4 & 8 & 9 & 3 & 1 \end{pmatrix},$$
$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 7 & 2 & 4 & 1 & 9 & 8 & 3 \end{pmatrix}.$$

- (a) Calculer $\sigma_1\sigma_2$, $\sigma_2\sigma_1$, σ_1^{-1} et σ_2^{-1} .
 - (b) Décomposer σ_1 et σ_2 en produit de cycles à supports deux à deux disjoints.
 - (c) Déterminer les signatures de σ_1 et σ_2 .
 - (d) Donner une factorisation de σ_1 en produit de transpositions. Même question pour σ_2 .
2. On considère les cycles suivants dans \mathcal{S}_7 :

$$c_1 = (1, 2, 7, 3, 6, 4), \quad c_2 = (5, 2, 6, 1).$$

- (a) Calculer c_1c_2 et c_2c_1 .
 - (b) Calculer le carré c_1^2 de c_1 . Est-ce un cycle ?
3. Soit $c = (a_1, \dots, a_k)$ un cycle de longueur k dans \mathcal{S}_n . Montrer que c^{-1} est un cycle et l'écrire.

Exercice 1.2 (Éléments de \mathcal{S}_4).

Établir la liste des éléments de \mathcal{S}_4 . Pour chacun d'eux, donner sa décomposition en cycles à supports deux à deux disjoints et sa signature. En déduire la liste des éléments du groupe alterné \mathcal{A}_4 .

Exercice 1.3 (Dénombrement des cycles de \mathcal{S}_n).

1. Si $n \geq 2$, compter le nombre de transpositions dans \mathcal{S}_n .
2. Si $n \geq 3$, compter le nombre de cycles de longueur 3 dans \mathcal{S}_n .
3. Généraliser : combien \mathcal{S}_n a-t-il de cycles de longueur k si $n \geq k$?

Exercice 1.4 (Supports disjoints et commutation).

Soient σ et σ' deux permutations dans \mathcal{S}_n telles que $\text{supp}(\sigma) \cap \text{supp}(\sigma') = \emptyset$. Montrer que $\sigma\sigma' = \sigma'\sigma$.

Exercice 1.5 (Générateurs de \mathcal{A}_n). 

Soient a, b, c, d des éléments deux à deux distincts de \mathbb{N}^* .

1. Montrer que $(a, b)(b, c)$ est un cycle de longueur 3.
2. Montrer que $(a, b)(c, d)$ est le produit de deux cycles de longueur 3.
3. Si $n \geq 3$, en déduire que tout élément de \mathcal{A}_n est un produit de cycles de longueur 3.
4. Calculer $(1, 2, a)(1, 2, b)(1, 2, a)^{-1}$ puis $(1, 2, a)(2, b, c)(1, 2, a)^{-1}$ pour $a, b, c \notin \{1, 2\}$. En déduire que tout élément de \mathcal{A}_n est un produit de cycles de longueur 3 de la forme $(1, 2, c)$ ou $(1, 2, c)^{-1}$ avec $c \geq 3$.

Exercice 1.6 (Centre de \mathcal{S}_n).  

On appelle *centre de \mathcal{S}_n* l'ensemble

$$Z(\mathcal{S}_n) = \{\sigma \in \mathcal{S}_n \mid \forall \sigma' \in \mathcal{S}_n, \sigma\sigma' = \sigma'\sigma\}.$$

L'objet de cet exercice est de montrer que $Z(\mathcal{S}_n) = \{\text{id}_n\}$ si $n \geq 3$. Supposons $n \geq 3$. Soit $\sigma \in Z(\mathcal{S}_n)$ et soient $i \neq j$ dans $\{1, \dots, n\}$. On pose τ la transposition (i, j) .

1. Montrer que $(\tau\sigma)(i) = \sigma(j)$.
2. En déduire que $\sigma(i) \in \{i, j\}$.
3. Montrer que $\sigma(i) = i$ (indication : on pourra faire intervenir un entier $k \notin \{i, j\}$ et la transposition (i, k)). Conclure.
4. Que se passe-t-il si $n = 2$?

Exercice 1.7 (Retour sur les transpositions).   

L'objet de cet exercice est de donner d'autres démonstrations de deux résultats du cours : les corollaires 1.28-1 et 1.22.

1. Soit $\tau = (i, j)$ une transposition de \mathcal{S}_n . Dénombrer les inversions de τ . En déduire la signature de τ .
2. Soit n un entier supérieur ou égal à 2. Par une récurrence descendante sur k , montrer que pour tout $k \in \{0, \dots, n\}$, toute permutation de \mathcal{S}_n ayant au moins k points fixes est un produit de transpositions.

Exercice 1.8 (Conjugaison dans \mathcal{S}_n).  

L'énoncé se place dans le groupe symétrique \mathcal{S}_n avec n supérieur ou égal à 2. Deux permutations σ et σ' sont dites *conjuguées* dans \mathcal{S}_n lorsqu'il existe $g \in \mathcal{S}_n$ tel que $\sigma' = g\sigma g^{-1}$.

1. Soit (a_1, \dots, a_k) un cycle de longueur k . Montrer que pour toute permutation σ on a

$$\sigma(a_1, \dots, a_k)\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

2. Montrer que si c et c' sont deux cycles de même longueur, il existe une permutation σ telle que

$$\sigma c \sigma^{-1} = c'$$

et que $\text{supp}(c') = \sigma(\text{supp}(c))$.

3. Soit σ une permutation distincte de id_n et $\sigma = c_1 \cdots c_s$ une décomposition de σ en cycles à supports deux à deux disjoints. On appelle *type* de σ la suite des longueurs des cycles c_1, \dots, c_s , ordonnée de manière décroissante.
- Justifier que le type d'une permutation est bien défini c'est-à-dire qu'il ne dépend que de σ .
 - Quel est le type des permutations σ_1 et σ_2 de l'exercice 1.1 ?
 - Montrer que deux permutations sont conjuguées dans \mathcal{S}_n si et seulement si elles ont même type.

Exercice 1.9 (Matrices de permutations). ☹☹☹

Soit n un entier naturel non nul. À toute permutation $\sigma \in \mathcal{S}_n$ on associe la matrice $M_\sigma = (m_{i,j})_{1 \leq i,j \leq n}$ de $M_n(\mathbb{R})$ définie par

$$m_{i,j} = \begin{cases} 1 & \text{si } i = \sigma(j) \\ 0 & \text{sinon.} \end{cases}$$

- Si $n = 4$, écrire la matrice M_σ pour $\sigma = (1, 2, 3, 4)$ et pour $\sigma = (1, 3)(2, 4)$.
- L'entier n et la permutation σ sont dorénavant quelconques. Montrer que la trace de M_σ est égale au nombre de points fixes de σ .
- Montrer que le déterminant de M_σ est égal à la signature $\varepsilon(\sigma)$ de σ .
- Soient σ et σ' deux permutations dans \mathcal{S}_n . Montrer que $M_{\sigma\sigma'} = M_\sigma M_{\sigma'}$.

Exercices du chapitre 2

Exercice 2.1 (Groupe à carrés triviaux).

Soit G un groupe dans lequel tout élément x vérifie $x^2 = 1_G$. Montrer que G est abélien.

Exercice 2.2 (Démonstration de la proposition 2.7).

Soit G un groupe.

1. Montrer que $e_G^{-1} = e_G$.
2. Montrer que pour tout $x \in G$, on a $(x^{-1})^{-1} = x$.
3. Montrer que pour tous x, y, z dans G , on a :

$$xy = xz \implies y = z \quad \text{et} \quad yx = zx \implies y = z.$$

4. Montrer que si x et y sont deux éléments de G alors $(xy)^{-1} = y^{-1}x^{-1}$.
5. Soit $x \in G$. Supposons qu'il existe $y \in G$ satisfaisant $xy = e_G$. Montrer que $y = x^{-1}$.

Exercice 2.3 (Exemples et contre-exemples de groupes).

Dans chacun des cas suivants, étudier si la loi munit l'ensemble d'une structure de groupe ; lorsqu'il l'est, dire si ce groupe est abélien.

1. L'ensemble $M_{n,p}(\mathbb{R})$ des matrices à n lignes et p colonnes à coefficients réels, muni de l'addition.
2. L'ensemble $\mathcal{P}(E)$ des parties d'un d'ensemble non vide E , muni de la loi intersection \cap .
3. L'ensemble \mathbb{R} muni de la loi donnée par : $\forall (x, y) \in \mathbb{R} \times \mathbb{R}, x * y = x^{-1}y^{-1}$.
4. L'ensemble $X =]-1, 1[$ muni de la loi \star donnée par :

$$\forall (x, y) \in X \times X, x \star y = \frac{x + y}{1 + xy}.$$

Exercice 2.4 (Un isomorphisme de groupes).

1. Montrer que \mathbb{R} muni de la loi $*$ donnée par :

$$\forall (x, y) \in \mathbb{R} \times \mathbb{R}, \quad x * y = (x^3 + y^3)^{1/3}$$

est un groupe abélien.

2. Montrer que l'application $x \mapsto x^3$ est un isomorphisme de groupes de $(\mathbb{R}, *)$ sur $(\mathbb{R}, +)$.

Exercice 2.5 (Les morphismes de \mathcal{S}_n dans \mathbb{C}^*).  

L'objectif est de montrer que si $n \geq 2$ les seuls morphismes de groupes du groupe symétrique \mathcal{S}_n dans \mathbb{C}^* sont le morphisme trivial $\sigma \mapsto 1$ et la signature ε .

1. Soit (i, j) une transposition de \mathcal{S}_n .
 - (a) Soit σ un élément de \mathcal{S}_n . Montrer que $\sigma(i, j)\sigma^{-1} = (\sigma(i), \sigma(j))$.
 - (b) En déduire que pour toute transposition (i', j') de \mathcal{S}_n , il existe $\sigma \in \mathcal{S}_n$ tel que $\sigma(i, j)\sigma^{-1} = (i', j')$.
2. Soit f un morphisme de groupes de \mathcal{S}_n dans \mathbb{C}^* . En utilisant la question précédente, montrer qu'il existe un nombre complexe z tel que, pour toute transposition τ de \mathcal{S}_n , $f(\tau) = z$.
3. Que vaut le carré d'une transposition? En déduire que $z \in \{\pm 1\}$.
4. Conclure que les seuls morphismes de groupes \mathcal{S}_n dans \mathbb{C}^* sont ceux annoncés.

Exercice 2.6 (Les morphismes de \mathbb{Z} , \mathbb{Q} et \mathbb{R} dans eux-mêmes).   

1. Déterminer tous les morphismes de groupes de $(\mathbb{Z}, +)$ dans lui-même.
Indication : montrer qu'un tel morphisme est déterminé de manière unique par sa valeur en 1.
Parmi ces morphismes, lesquels sont injectifs? surjectifs? des isomorphismes?
2. Mêmes questions avec les morphismes de groupes de $(\mathbb{Q}, +)$ dans lui-même.
Indication : montrer qu'un tel morphisme est déterminé de manière unique par sa valeur en 1.
3. Déterminer tous les morphismes continus de groupes de $(\mathbb{R}, +)$ dans lui-même.

Exercice 2.7 (Groupes d'ordre 1, 2 et 3).  

Déterminer à isomorphisme près tous les groupes d'ordre 1, 2 et 3.

Indication : deux groupes étant isomorphes lorsque leurs tables de Cayley se correspondent (remarque 2.13), il s'agit d'établir toutes les tables possibles pour les groupes de cet ordre.

Exercice 2.8 (Sous-groupes matriciels). 

On considère le groupe $\mathrm{GL}_2(\mathbb{R})$ muni de la multiplication matricielle.

1. L'ensemble des matrices de la forme $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ avec $a \in \mathbb{R}$ est-il un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$?
2. Même question pour l'ensemble des matrices de la forme $\begin{pmatrix} 1 & a \\ b & 1 \end{pmatrix}$ avec a et b dans \mathbb{R} et $ab \neq 1$.

Exercice 2.9 (Sous-groupes des puissances n -èmes). 

Soit G un groupe abélien. Montrer que pour tout entier naturel n , l'ensemble

$$H_n = \{x \in G \mid \exists a \in G, x = a^n\}$$

est un sous-groupe de G .

Exercice 2.10 (Sous-groupes de \mathcal{S}_3). 

Donner la liste de tous les sous-groupes de \mathcal{S}_3 .

Indication : ces sous-groupes sont nécessairement de type fini ; énumérer ceux engendrés par un élément, puis deux éléments, etc.

Exercice 2.11 (Union de sous-groupes).  

Soient H et K deux sous-groupes d'un groupe G . Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

Exercice 2.12 (Les sous-groupes de $(\mathbb{Z}, +)$). 

Montrer les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Indication. Soit H un sous-groupe distinct de $\{0\}$. Considérons le plus petit entier naturel non nul n dans H . Montrer que $H = n\mathbb{Z}$ par double inclusion et en utilisant la division euclidienne par n .

Exercice 2.13 ($(\mathbb{Q}, +)$ n'est pas de type fini).   

Montrer que le groupe $(\mathbb{Q}, +)$ n'est pas de type fini.

Indication : raisonner par l'absurde.

Exercice 2.14 (Morphisme de projection). 

Soient G et H deux groupes. Montrer que l'application

$$\begin{aligned} \pi : G \times H &\longrightarrow G \\ (g, h) &\longmapsto g \end{aligned}$$

est un morphisme de groupes surjectif et de noyau isomorphe à H .

Exercice 2.15 (Un sous-groupe d'un produit direct).  

Soient G_1 et G_2 deux groupes, H_1 un sous-groupe de G_1 et H_2 un sous-groupe de G_2 . Montrer que $H_1 \times H_2$ est un sous-groupe de $G_1 \times G_2$.

Exercices du chapitre 3

Exercice 3.1 (Ordre et puissance de permutations).

On considère les permutations σ_1 et σ_2 du groupe symétrique \mathcal{S}_9 étudiées dans l'exercice 1.1 page 107.

1. Déterminer les ordres de σ_1 et σ_2 .
2. Calculer σ_1^{2017} et σ_2^{2017} .

Exercice 3.2 (Permutations d'ordre premier).

1. Dans le groupe symétrique \mathcal{S}_n , montrer que les éléments d'ordre p premier, avec $p \leq n$, sont les produits de p -cycles à supports deux à deux disjoints.
2. Déterminer les éléments d'ordre 2 du groupe symétrique \mathcal{S}_5 en fonction de leur factorisation en cycles, puis dénombrer ces éléments.

Exercice 3.3 (Matrices d'ordre fini de $\text{GL}_n(\mathbb{C})$).

Démontrer que toute matrice d'ordre fini dans le groupe multiplicatif $\text{GL}_n(\mathbb{C})$ est diagonalisable. Donner des exemples de telles matrices.

Exercice 3.4 (Ordres d'éléments).

Soient G un groupe et a, b deux éléments d'ordre fini dans G .

1. Calculer l'ordre de a^{-1} en fonction de l'ordre de a .
2. Calculer l'ordre de bab^{-1} en fonction de l'ordre de a .
3. Notons n l'ordre de a . Si $k \in \mathbb{Z}$, montrer que l'ordre de a^k est $\frac{n}{\text{pgcd}(n, k)}$.
4. Dans cette question, G est un groupe cyclique et g un générateur de G . Déterminer en fonction de g les éléments $x \in G$ tels que $G = \langle x \rangle$.
5. Dans cette question, on suppose que $ab = ba$.
 - (a) Montrer que l'ordre de ab divise $\text{ppcm}(\text{ord}(a), \text{ord}(b))$.
 - (b) Donner un exemple où l'ordre est distinct de ce ppcm.
 - (c) Montrer que si $\text{ord}(a)$ et $\text{ord}(b)$ sont premiers entre eux alors $\text{ord}(ab) = \text{ppcm}(\text{ord}(a), \text{ord}(b)) = \text{ord}(a)\text{ord}(b)$.

Exercice 3.5 (Critères pour l'ordre).

Soit x un élément d'ordre fini dans un groupe G . Soit $\ell \geq 1$ un entier.

1. Montrer que x est d'ordre ℓ si et seulement si

$$x^\ell = 1_G \quad \text{et} \quad \forall d \mid \ell, d \neq \ell : x^d \neq 1_G.$$

2. Montrer que dans le critère précédent, on peut se contenter de tester les diviseurs $d \mid \ell, d \neq \ell$ de la forme $d = \frac{\ell}{p}$ où p est un nombre premier divisant ℓ .
3. On veut montrer que x est d'ordre 12. Écrire les conditions à vérifier, selon qu'on utilise le théorème 3.4, la question 1 ou la question 2 de cet exercice.

Exercice 3.6 (Étude du groupe additif $\mathbb{Z}/12\mathbb{Z}$). 

Calculer les ordres des éléments du groupe $(\mathbb{Z}/12\mathbb{Z}, +)$ puis déterminer tous ses sous-groupes.

Exercice 3.7 (Morphismes entre $(\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$). 

Déterminer tous les morphismes de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$ puis tous ceux de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$.

Indication : si f est un tel morphisme, commencer par montrer que f est déterminé de manière unique par $f(1)$.

Exercice 3.8 (Sous-groupes d'un groupe cyclique).  

Il s'agit de démontrer que tous les sous-groupes d'un groupe cyclique sont cycliques. Soient G un groupe cyclique, a un générateur de G , et H un sous-groupe de G distinct de $\{1_G\}$.

1. Justifier qu'il existe un entier $m \geq 1$ minimal pour la propriété $a^m \in H$.
2. Montrer que H est cyclique et engendré par a^m .

Indication : raisonner par double-inclusion et pour l'une d'entre elles, utiliser une division euclidienne par m .

Exercice 3.9 (Classes matricielles à gauche et à droite). 

Soit $G = \text{SL}_2(\mathbb{R})$ le sous-groupe de $\text{GL}_2(\mathbb{R})$ formé des matrices de déterminant 1. On considère les sous-groupes H et K de G engendrés respectivement par

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Déterminer les éléments des espaces quotients $G/H, H \backslash G, G/K$ et $K \backslash G$.

Exercice 3.10 (Sous-groupes d'ordres premiers entre eux). 

Soient H et K deux sous-groupes finis d'un groupe G . Si H et K sont d'ordres premiers entre eux, montrer que $H \cap K = \{1_G\}$.

Exercice 3.11 (Groupes d'ordre 4). 

1. Montrer que tout groupe d'ordre 4 est isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$ ou à $V = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

Indication : raisonner selon les ordres possibles des éléments du groupe.

2. Le groupe $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est appelé le *groupe de Klein*. Quels sont les ordres de ses éléments? En déduire que $\mathbb{Z}/4\mathbb{Z}$ et V ne sont pas isomorphes.
3. Si d divise l'ordre d'un groupe fini G , existe-t-il toujours un élément d'ordre d dans G ?

Exercice 3.12 (Groupe à sous-groupes triviaux).  

Soit G un groupe ayant au moins deux éléments et dont les seuls sous-groupes sont $\{1_G\}$ et G . Montrer que G est cyclique d'ordre premier.

Indication. Montrer d'abord que G est monogène puis cyclique. Pour prouver que l'ordre est premier, utiliser la question 3 de l'exercice 3.4.

Exercice 3.13 (Groupes d'ordre 6).  

L'objectif est de démontrer que les seuls groupes d'ordre 6 à isomorphisme près sont $(\mathbb{Z}/6\mathbb{Z}, +)$ et \mathcal{S}_3 . Soit G un groupe d'ordre 6.

1. Montrer que G possède au moins un élément d'ordre 3. On note x un tel élément.

Indication : distinguer les cas où G est cyclique, ou non cyclique ; dans le second cas, regarder les ordres possibles des éléments et utiliser l'exercice 2.1.

2. Montrer que G possède au moins un élément d'ordre 2. On note y un tel élément.

Indication : distinguer les cas où G est cyclique, ou non cyclique ; dans le second cas, regarder les ordres possibles des éléments.

3. Montrer que $G = \langle x, y \rangle$.

4. Si G est abélien, montrer que G est cyclique d'ordre 6.

Indication : considérer l'élément xy et utiliser l'exercice 3.4.

Conclure que $G \simeq (\mathbb{Z}/6\mathbb{Z}, +)$.

5. Si G n'est pas abélien, montrer que $yx = x^2y$. Écrire la table de Cayley de G . Conclure que $G \simeq \mathcal{S}_3$.

6. Justifier que les groupes $(\mathbb{Z}/6\mathbb{Z}, +)$ et \mathcal{S}_3 ne sont pas isomorphes.

Exercice 3.14 (Théorème chinois).   

Soit m et n deux entiers non nuls et premiers entre eux. En utilisant le critère de décomposition en produit direct (théorème 2.44), montrer que le groupe additif $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Exercices du chapitre 4

Exercice 4.1 (Matrices inversibles de déterminant positif).

Montrer que l'ensemble $GL_n^+(\mathbb{R})$ des matrices de $GL_n(\mathbb{R})$ de déterminant strictement positif est un sous-groupe de $(GL_n(\mathbb{R}), \cdot)$ puis qu'il est normal dans ce groupe.

Exercice 4.2 (\mathbb{R} modulo \mathbb{Z}).

1. Justifier que $(\mathbb{Z}, +)$ est un sous-groupe normal de $(\mathbb{R}, +)$.
2. À quelle condition deux éléments de \mathbb{R} sont-ils dans la même classe modulo \mathbb{Z} ? En déduire un système de représentants de \mathbb{R}/\mathbb{Z} .

Exercice 4.3 (Un produit normal).

Soient G un groupe, H et K deux sous-groupes de G tels que H est normal dans G . Montrer que KH est un sous-groupe de G .

Exercice 4.4 (Isomorphismes classiques).

Montrer qu'on a des isomorphismes de groupes :

1. $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$ (utiliser la partie imaginaire) ;
2. $(\mathbb{R}, +) \simeq (\mathbb{R}_+^*, \cdot)$ (utiliser l'exponentielle réelle) ;
3. $(U, \cdot) \simeq (\mathbb{R}/2\pi\mathbb{Z}, +)$ où U désigne le groupe multiplicatif des nombres complexes de module 1 (utiliser l'exponentielle complexe) ;
4. $(\mathbb{C}^*, \cdot) \simeq (\mathbb{R}_+^*, \cdot) \times (\mathbb{R}/2\pi\mathbb{Z}, +)$.

Exercice 4.5 (Étude de la simplicité de \mathcal{A}_n pour $n = 3, 4$).

1. Montrer que le groupe alterné \mathcal{A}_3 est simple.
2. Montrer que le groupe alterné \mathcal{A}_4 n'est pas simple. *Indication* : regarder le sous-groupe engendré par les produits de deux transpositions à supports disjoints.

Exercice 4.6 (Groupes abéliens d'ordre 8).

Soit G un groupe abélien d'ordre 8.

1. Quels sont les ordres possibles des éléments de G ?
2. On suppose qu'il existe un élément d'ordre 8 dans G . Montrer que $G \simeq \mathbb{Z}/8\mathbb{Z}$.
3. On suppose qu'il n'existe pas d'élément d'ordre 8 dans G mais qu'il existe un élément a d'ordre 4. Soit $b \in G - \langle a \rangle$, un élément de G n'appartenant pas à $\langle a \rangle$.

- (a) Montrer que $G = \langle a, b \rangle$. En déduire que $b^2 = 1_G$ ou $b^2 = a^2$.
- (b) En déduire qu'il existe un élément c d'ordre 2 dans G n'appartenant pas à $\langle a \rangle$.
- (c) En utilisant les sous-groupes $\langle a \rangle$ et $\langle c \rangle$, montrer que $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
4. On suppose que tous les éléments de G distincts de 1_G sont d'ordre 2. Montrer que G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 4.7 (La normalité n'est pas transitive). 

Soit D_4 un groupe diédral à 8 éléments, de générateurs r et s avec r d'ordre 4, s d'ordre 2 et $rsrs = 1_G$. On pose

$$K = \langle s \rangle, \quad H = \langle s, r^2 \rangle.$$

Montrer que K est normal dans H , H est normal dans D_4 mais K n'est pas normal dans D_4 .

Exercice 4.8 (Automorphismes fixant un sous-groupe normal).  

Soit H un sous-groupe normal d'un groupe G . Notons $\pi : G \rightarrow G/H$ la surjection canonique.

1. Soit φ un automorphisme de G vérifiant $\varphi(H) = H$. Montrer qu'il existe un unique morphisme de groupes $\Phi : G/H \rightarrow G/H$ tel que $\Phi \circ \pi = \pi \circ \varphi$. Montrer que Φ est un automorphisme de G/H .
2. On note $\text{Fix}(H)$ le sous-ensemble des automorphismes $\varphi \in \text{Aut}(G)$ vérifiant $\varphi(H) = H$. Montrer que c'est un sous-groupe de $(\text{Aut}(G), \circ)$.
3. Montrer qu'on peut définir un morphisme de groupes de $\text{Fix}(H)$ dans $\text{Aut}(G/H)$.

Exercice 4.9 (Deuxième et troisième théorèmes d'isomorphisme de Noether).   

Soient G un groupe, H un sous-groupe normal de G et K un sous-groupe de G .

1. Dans cette question on suppose que K contient H et K est normal dans G . Montrer que

$$(G/H)/(K/H) \simeq G/K.$$

Ce résultat porte le nom de *deuxième théorème d'isomorphisme*.

Indication : considérer la surjection canonique $G \rightarrow G/K, x \mapsto xK$; montrer qu'elle passe au quotient en un morphisme de groupes $G/H \rightarrow G/K$ puis étudier le noyau et l'image de ce morphisme.

2. Dans cette question, on ne fait plus d'hypothèse sur le sous-groupe K .
 - (a) Montrer que $H \cap K$ est un sous-groupe normal de K , KH est un sous-groupe de G , et H est un sous-groupe normal de KH .
 - (b) Montrer que

$$K/(H \cap K) \simeq KH/H.$$

Ce résultat porte le nom de *troisième théorème d'isomorphisme*.

Exercice 4.10 (Groupe des racines de l'unité).  

Soit $\Gamma = \{z \in \mathbb{C}^* \mid \exists n \in \mathbb{N}, n \geq 1, z^n = 1\}$.

1. Montrer que Γ est un sous-groupe de (U, \cdot) où U désigne le groupe des nombres complexes de module 1.
2. Montrer que si $z \in \Gamma$ il existe $n \in \mathbb{N}, n \geq 1$ et $k \in \mathbb{Z}$ tels que $z = e^{\frac{2i\pi k}{n}}$.
3. En déduire un isomorphisme de groupes $(\Gamma, \cdot) \simeq (\mathbb{Q}/\mathbb{Z}, +)$.
4. Justifier l'existence d'un isomorphisme de groupes $(U, \cdot) \simeq (\mathbb{R}/\mathbb{Z}, +)$.
5. À l'aide du deuxième théorème d'isomorphisme (question 2b de l'exercice 4.9), conclure qu'il existe un isomorphisme de groupes

$$U/\Gamma \simeq (\mathbb{R}/\mathbb{Q}, +).$$

Exercice 4.11 (Un groupe symétrique et diédral). 

Montrer que le groupe symétrique \mathcal{S}_3 est diédral.

Exercice 4.12 (Groupes non abéliens d'ordre 8).   

Soit G un groupe non abélien d'ordre 8.

1. Montrer qu'il existe un élément a d'ordre 4 dans G .
2. Montrer que le sous-groupe $\langle a \rangle$ est normal dans G .
3. Soit $b \in G - \{1_G, a, a^2, a^3\}$. Montrer que $G = \langle a, b \rangle$.
4. Montrer qu'on a $b^2 = 1_G$ ou $b^2 = a^2$.
5. Calculer l'ordre de bab^{-1} . En déduire que $ba = a^3b$.
6. En déduire que G est :
 - soit un groupe diédral D_4 à 8 éléments ;
 - soit isomorphe à un groupe H engendré par deux éléments α et β avec α d'ordre 4, $\beta^2 = \alpha^2$ et $\beta\alpha = \alpha^{-1}\beta$.

Montrer que D_4 et H ne sont pas isomorphes. Le groupe H s'appelle le *groupe des quaternions*.

Exercice 4.13 (Groupe linéaire et produit semi-direct). 

Soit H le sous-groupe de $(\mathrm{GL}_n(K), \cdot)$ formé des matrices

$$\begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

avec $\lambda \in K^*$ et les coefficients en-dehors de la diagonale tous nuls. Montrer que $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes H$. Ce produit est-il direct ?

Exercices du chapitre 5

Exercice 5.1 (Règle de simplification pour une action).

Soit G un groupe agissant sur un ensemble X . Si $g \in G$ et x, y sont dans X , montrer que

$$g \star x = g \star y \Rightarrow x = y.$$

Exercice 5.2 (Étude de l'action de \mathcal{S}_3).

Déterminer les orbites et les stabilisateurs de l'action du groupe symétrique \mathcal{S}_3 sur $\{1, 2, 3\}$. L'action est-elle transitive ? libre ? fidèle ? simplement transitive ?

Exercice 5.3 (Demi-plan de Poincaré).

Considérons le groupe

$$G = \{M \in \text{GL}_2(\mathbb{R}) \mid \det M = 1\}.$$

Soit $\mathcal{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$, appelé le demi-plan de Poincaré.

1. Montrer que la formule $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \star z = \frac{az + b}{cz + d}$ définit une action de G sur \mathcal{H} .
2. Quel est le stabilisateur du nombre complexe i de \mathcal{H} ?
3. Cette action est-elle fidèle ?
4. Montrer que l'action est transitive.

Exercice 5.4 (Actions classiques d'un groupe sur lui-même).

Cet exercice démontre que les opérations de la définition 5.5 sont des actions.

1. Montrer qu'un groupe agit sur lui-même par translation à gauche et par conjugaison. Déterminer les orbites et les stabilisateurs pour ces actions.
2. Montrer que l'action par translation est simplement transitive.
3. Montrer qu'un groupe agit par conjugaison sur l'ensemble de ses sous-groupes.

Exercice 5.5 (Conjugaison des stabilisateurs).

Soit G un groupe agissant sur un ensemble X . Si x et y sont des éléments de X dans la même orbite, montrer que leurs stabilisateurs G_x et G_y sont conjugués, c'est-à-dire qu'il existe $g \in G$ tel que $G_x = gG_yg^{-1}$.

Exercice 5.6 (Action et morphisme).

Démontrer la proposition 5.6 du cours.

Exercice 5.7 (Un isomorphisme entre $GL_2(\mathbb{F}_2)$ et S_3).  

Soit $G = GL_2(\mathbb{F}_2)$ où \mathbb{F}_2 désigne le corps $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$.

1. Soit $X = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x \in \mathbb{F}_2, y \in \mathbb{F}_2, (x, y) \neq (\bar{0}, \bar{0}) \right\}$. Justifier que le groupe G agit sur l'ensemble X par, pour tous $M \in G$ et $v \in X$, $M \star v = Mv$ (produit d'une matrice et d'un vecteur colonne).
2. Montrer que le morphisme de groupes $\varphi : G \rightarrow \mathcal{S}_X$ associé à cette action est injectif. En déduire que G et S_3 sont isomorphes.

Exercice 5.8 (Dénombrement). 

Soit G un groupe d'ordre 21 agissant sur un ensemble E à $n \geq 1$ éléments.

1. Quel est le cardinal possible de chaque orbite ?
2. Notons N_i le nombre d'orbites à i éléments, pour i entier ≥ 1 . En utilisant la partition de E en orbites, trouver une relation entre les N_i .
3. On suppose $n = 11$. Montrer que l'action a au moins un point fixe.
4. On suppose que $n = 19$ et que G agit sans point fixe. Combien y a-t-il d'orbites ?

Exercice 5.9 (Groupes d'ordre p^2).  

1. Soit G est un groupe tel que le groupe quotient $G/Z(G)$ est cyclique. Montrer que G est abélien.
Indication : utiliser un générateur de $G/Z(G)$.
2. En déduire que tout groupe d'ordre p^2 , où p est un nombre premier, est abélien.

Exercice 5.10 (Groupes d'ordre 63). 

Soit G un groupe d'ordre 63. En étudiant ses 7-Sylow, prouver que G n'est pas simple.

Exercice 5.11 (Groupes d'ordre 35).  

Soit G un groupe d'ordre 35.

1. Montrer que G possède un unique sous-groupe d'ordre 5, noté H et un unique sous-groupe d'ordre 7, noté K . Justifier que H et K sont normaux dans G .
2. À quel groupe connu H est-il isomorphe ? Même question pour K . En utilisant le théorème chinois (voir l'exercice 3.14 ou le chapitre 6), en déduire que G est cyclique.

Exercice 5.12 (Groupes d'ordre 30).  

L'objectif de cet exercice est d'établir qu'aucun groupe d'ordre 30 n'est simple.

1. *Préliminaire.* Soient un groupe G et un nombre premier p tels que p divise $\text{ord}(G)$ mais p^2 ne divise pas $\text{ord}(G)$.
 - (a) Quel est l'ordre de chaque p -Sylow de G ? Combien un tel p -Sylow a-t-il d'éléments d'ordre p ?

-
- (b) Si H_1 et H_2 sont des p -Sylow de G avec $H_1 \neq H_2$, montrer que $H_1 \cap H_2 = \{1_G\}$.
- (c) En déduire le nombre d'éléments d'ordre p dans G .
2. Soit G un groupe d'ordre 30. Si $n_3 \neq 1$, déterminer à l'aide du préliminaire le nombre d'éléments d'ordre 3 dans G . Même question si $n_5 \neq 1$ avec les éléments d'ordre 5.
3. En déduire que G n'est pas simple.

Exercice 5.13 (Groupes d'ordre $2p$). 

Soit p un nombre premier tel que $p > 2$. L'objectif est de démontrer que tout groupe d'ordre $2p$ est isomorphe à $(\mathbb{Z}/2p\mathbb{Z}, +)$ ou au groupe diédral D_p . Soit G un groupe d'ordre $2p$.

1. Justifier que G possède au moins un élément d'ordre p et un élément d'ordre 2. Notons a (resp. b) un élément d'ordre p (resp. 2). Ces éléments sont distincts puisque $p > 2$.
2. Déterminer le nombre de p -Sylow de G .
3. En déduire que ba n'est pas d'ordre p .
4. Quels sont les ordres possibles pour ba ? Conclure que G est isomorphe à $(\mathbb{Z}/2p\mathbb{Z}, +)$ ou au groupe diédral D_p .
5. Montrer que les groupes $(\mathbb{Z}/2p\mathbb{Z}, +)$ et D_p ne sont pas isomorphes.

Exercices du chapitre 6

Exercice 6.1 (Diviseurs).

Donner la liste des diviseurs dans \mathbb{N} de 36, 59 et 30.

Exercice 6.2 (Calculs de pgcd).

Calculer :

1. $\text{pgcd}(792, 318)$;
2. $\text{pgcd}((n+1)! + 1, n! + 1)$ pour $n \in \mathbb{N}$;
3. $\text{pgcd}(a^2 - b^2, a^3 - b^3)$ pour a et b non nuls dans \mathbb{N} satisfaisant $\text{pgcd}(a, b) = 1$.

Exercice 6.3 (Une équation diophantienne).

1. Calculer le pgcd de 679 et 455 puis donner deux entiers u et v tels que $679u + 455v = \text{pgcd}(679, 455)$.
2. Déterminer toutes les solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ de l'équation

$$679x + 455y = \text{pgcd}(679, 455).$$

Exercice 6.4 (Nombres de Fibonacci).

La suite de Fibonacci est la suite d'entiers naturels $(f_n)_{n \in \mathbb{N}}$ définie par $f_0 = 0$, $f_1 = 1$ et $f_{n+1} = f_n + f_{n-1}$ pour tout $n \geq 2$.

1. Montrer que f_n et f_{n+1} sont premiers entre eux pour tout $n \in \mathbb{N}$.
2. Est-il vrai que deux nombres de Fibonacci f_n et f_m sont premiers entre eux si $m \neq n$?
3. Montrer que pour tout $n \in \mathbb{N}$ on a

$$f_n = \frac{1}{\sqrt{5}} (\varphi^n - \varphi'^n)$$

où $\varphi = (1 + \sqrt{5})/2$ et $\varphi' = (1 - \sqrt{5})/2$.

Indication. Montrer que φ et φ' sont les solutions réelles de $x^2 - x - 1 = 0$, puis en déduire que $\varphi - 1 = \frac{1}{\varphi}$ et que $\varphi' - 1 = \frac{1}{\varphi'}$.

Exercice 6.5 (Générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$).

1. Soient n un entier ≥ 1 et $k \in \mathbb{Z}$. Montrer que \bar{k} est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $\text{pgcd}(k, n) = 1$.
2. Donner la liste des générateurs de $(\mathbb{Z}/18\mathbb{Z}, +)$.

Exercice 6.6 (Écritures dans des bases). 

On considère le nombre $m = 1024$ écrit en base 10. Écrire m en base 2, en base 3 puis en base 5.

Exercice 6.7 (Premiers dans une progression arithmétique).  

Soit X l'ensemble des nombres premiers de la forme $4k + 3$ avec $k \in \mathbb{N}$. L'objet de l'exercice est de montrer que X est infini.

1. Justifier que X est non vide.
2. Montrer que le produit de deux nombres entiers de la forme $4k + 1$ est encore de la forme $4k + 1$.
3. Supposons l'ensemble X fini. Notons $X = \{p_1, \dots, p_n\}$ et posons

$$N = 4p_1 \cdots p_n - 1.$$

- (a) Montrer par l'absurde que N admet un diviseur premier de la forme $4k + 3$.
- (b) Conclure.

Exercice 6.8 (Nombres parfaits).  

Dans cet exercice, « diviseur » désignera un diviseur positif. Si $m \in \mathbb{N}$ on note $\sigma(m)$ la somme des diviseurs de m .

1. Donner une condition nécessaire et suffisante pour que $\sigma(m) = m + 1$.
2. Si m et n sont premiers entre eux, montrer que pour tout diviseur d de mn il existe un unique couple $(d_1, d_2) \in \mathbb{N} \times \mathbb{N}$ tel que $d = d_1 d_2$ avec d_1 divise m et d_2 divise n .
3. Si m et n sont premiers entre eux, montrer que $\sigma(mn) = \sigma(m)\sigma(n)$.
4. Un entier $m > 0$ est dit *parfait* s'il est égal à la somme de ses diviseurs stricts (c'est-à-dire de ses diviseurs distincts de m). Montrer que m est parfait si et seulement si $\sigma(m) = 2m$.
5. Soit $n \in \mathbb{N}$. Montrer que si $2^{n+1} - 1$ est un nombre premier alors $m = 2^n(2^{n+1} - 1)$ est un nombre parfait.
6. Montrer que si $2^{n+1} - 1$ n'est pas un nombre premier alors $m = 2^n(2^{n+1} - 1)$ vérifie $\sigma(m) > 2m$ (on dit que m est un nombre *abondant*).
7. Inversement, montrer que tout nombre parfait pair est de la forme $m = 2^n(2^{n+1} - 1)$ où $2^{n+1} - 1$ est un nombre premier.

Exercice 6.9 (Somme de carrés). 

1. Pour tout $a \in \mathbb{Z}$, montrer qu'on a $a^2 \equiv 0 \pmod{4}$ ou $a^2 \equiv 1 \pmod{4}$.
2. En déduire que si $n = a^2 + b^2$ avec a et b dans \mathbb{Z} alors $n \not\equiv 3 \pmod{4}$.
3. Donner la liste de tous les nombres premiers $p \equiv 1 \pmod{4}$ avec $p \leq 50$. Pour chacun d'eux, montrer que p peut s'écrire comme somme de deux carrés dans \mathbb{Z} .

Exercice 6.10 (Critères de divisibilité). 

Montrer qu'un entier naturel n est :

1. divisible par 3 si et seulement si la somme de ses chiffres (en base 10) est un multiple de 3;
2. divisible par 4 si et seulement si ses deux derniers chiffres (en base 10) forment un nombre multiple de 4.

Exercice 6.11 (Congruences). 

Soit $n \in \mathbb{N}$.

1. Calculer $2^{2^n} - 1 \pmod{4}$.
2. Calculer $2^{3^n} - 1 \pmod{7}$.
3. Montrer que $5^{2^n} \equiv 1 + 2^{n+2} \pmod{2^{n+3}}$. *Indication.* Raisonner par récurrence.

Exercice 6.12 (Partage d'un butin). 

Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or. Ils décident de se les partager de manière égale et de donner le reste au cuisinier, qui n'est pas un pirate. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent et onze d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Quelle est la fortune minimale que peut espérer le cuisinier s'il empoisonne le reste des pirates ?

Exercice 6.13 (Un inverse modulo 241). 

Montrer que 21 est inversible modulo 241 et calculer son inverse.

Exercice 6.14 (Étude du groupe $(\mathbb{Z}/9\mathbb{Z})^\times$). 

Soit G le groupe $((\mathbb{Z}/9\mathbb{Z})^\times, \times)$.

1. Écrire la table de Cayley de G .
2. Calculer l'ordre de chaque élément de G .
3. Le groupe G est-il cyclique ?

Exercice 6.15 (Une équation polynomiale).  

Montrer que l'équation $x^5 - x^2 + x - 3 = 0$ n'a aucune solution dans \mathbb{Z} .

Exercice 6.16 (Fonction indicatrice d'Euler).  

1. Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}/56\mathbb{Z}$? dans $\mathbb{Z}/504\mathbb{Z}$?
2. Déterminer les entiers $n \geq 1$ pour lesquels $\varphi(n)$ est impair.

Exercice 6.17 (Derniers chiffres). 

1. Pour l'entier 2018^{2017} , calculer son dernier chiffre en base 5 et ses deux derniers chiffres en base 10.
2. Calculer les deux derniers chiffres en base 10 de $79^{79^{79}}$.

Exercice 6.18 (Nombres de Fermat).  

1. Montrer que si $2^m + 1$ est premier alors m est une puissance de 2.
2. Les *nombres de Fermat* sont les $F_n = 2^{2^n} + 1$ pour tout $n \in \mathbb{N}$. Montrer par récurrence sur n que

$$\prod_{k=0}^{n-1} F_k = F_n - 2.$$

3. Montrer que les F_n sont premiers entre eux deux à deux.
4. En déduire une preuve de l'infinitude des nombres premiers.
5. Montrer que les diviseurs premiers de F_n sont de la forme $1 + 2^{n+1}k$.
Indication. Si p est un tel diviseur premier, montrer que $2^{2^{n+1}} \equiv 1 \pmod{p}$ puis utiliser le théorème de Lagrange dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 6.19 (Propriétés de l'addition dans \mathbb{N}).   

1. Prouver le lemme 6.57 page 94 : pour tous a et b dans \mathbb{N} on a $s(a) + b = s(a + b)$.
2. Prouver le résultat suivant de la proposition 6.56 page 94 : pour tous a, b, c dans \mathbb{N} , on a $a + b = a + c \implies b = c$.

Exercice 6.20 (Toute partie finie non vide de \mathbb{N} a un plus grand élément).   

1. Montrer que le principe de récurrence (troisième axiome de Peano) entraîne la deuxième forme de récurrence suivante :
Soit $\mathcal{P}(n)$ une propriété de l'entier $n \in \mathbb{N} - \{0\}$. Supposons que $\mathcal{P}(1)$ est vraie et que pour tout $n \in \mathbb{N}$, $\mathcal{P}(n)$ implique $\mathcal{P}(n + 1)$. Alors $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N} - \{0\}$.
2. Montrer que toute partie non vide finie de \mathbb{N} a un plus grand élément.
Indication : raisonner par récurrence sur le cardinal de la partie.

Troisième partie

Algèbre 1

Les corrigés des exercices

Corrigé des exercices du chapitre 1

Solution de l'exercice 1.1. 1. (a) En prenant garde au sens de calcul des composées (cf. exemple 1.4), on a :

$$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 9 & 7 & 5 & 2 & 1 & 3 & 6 \end{pmatrix},$$

$$\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 1 & 4 & 2 & 8 & 3 & 7 & 5 \end{pmatrix}.$$

Pour calculer l'inverse d'une permutation σ , il suffit de trouver les antécédents de $1, 2, \dots$ par σ : cela revient à échanger les lignes du tableau puis à réordonner les colonnes de façon à avoir $1, 2, \dots, 9$ sur la première ligne. Ici cela donne :

$$\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 8 & 5 & 4 & 3 & 2 & 6 & 7 \end{pmatrix},$$

$$\sigma_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 9 & 5 & 1 & 2 & 3 & 8 & 7 \end{pmatrix}.$$

(b) En suivant la méthode décrite dans l'exemple 1.16 du cours, on obtient

$$\sigma_1 = (1, 2, 7, 9)(3, 6, 8)(4, 5),$$

$$\sigma_2 = (1, 5, 4, 2, 6)(3, 7, 9).$$

(c) Pour déterminer la signature, on peut calculer le nombre d'inversions à la main mais c'est long et fastidieux. Il vaut mieux utiliser la décomposition en cycles à supports deux à deux disjoints, le fait que la signature est un morphisme, et la connaissance de la signature des cycles (voir l'exemple 1.29 du cours) :

$$\varepsilon(\sigma_1) = (-1)^3(-1)^2(-1) = 1,$$

$$\varepsilon(\sigma_2) = (-1)^4(-1)^2 = 1.$$

(d) On utilise les décompositions en cycles obtenues et la relation $(a_1, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2)$ vue dans le cours :

$$\sigma_1 = (1, 9)(1, 7)(1, 2)(3, 8)(3, 6)(4, 5),$$

$$\sigma_2 = (1, 6)(1, 2)(1, 4)(1, 5)(3, 9)(3, 7).$$

2. (a) En prenant garde au sens de calcul des composées (cf. exemple 1.4 et remarque de l'exemple 1.17), on a :

$$\begin{aligned}c_1 c_2 &= (1, 2, 7, 3, 6, 4)(5, 2, 6, 1) = (1, 5, 7, 3, 6, 2, 4), \\c_2 c_1 &= (5, 2, 6, 1)(1, 2, 7, 3, 6, 4) = (1, 6, 4, 5, 2, 7, 3).\end{aligned}$$

- (b) Un calcul donne $c_1^2 = (1, 2, 7, 3, 6, 4)(1, 2, 7, 3, 6, 4) = (1, 7, 6)(2, 3, 4)$. Ce n'est pas un cycle (c'est un produit de deux cycles de longueur 3 à supports disjoints). En général une puissance d'un cycle n'est pas un cycle.

3. Soit $c = (a_1, \dots, a_k)$ un cycle de longueur k dans \mathcal{S}_n . Son inverse est $c^{-1} = (a_k, a_{k-1}, \dots, a_1)$ (noter qu'il y a d'autres manières de l'écrire, voir remarque 1.14). C'est un cycle de même longueur et de même support que c , mais distinct de c en général.

Solution de l'exercice 1.2. Les éléments de \mathcal{S}_4 sont les 24 permutations suivantes :

$$\begin{aligned}\text{id}_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \\ \sigma_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \\ \sigma_6 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad \sigma_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \sigma_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \\ \sigma_9 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \sigma_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad \sigma_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \\ \sigma_{12} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \sigma_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad \sigma_{14} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \\ \sigma_{15} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad \sigma_{16} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \sigma_{17} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \\ \sigma_{18} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \quad \sigma_{19} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad \sigma_{20} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\ \sigma_{21} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \quad \sigma_{22} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \quad \sigma_{23} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.\end{aligned}$$

Pour leur décomposition en cycles à supports deux à deux disjoints, on obtient :

$$\begin{aligned}\sigma_1 &= (3, 4), & \sigma_2 &= (2, 3), & \sigma_3 &= (2, 3, 4), & \sigma_4 &= (2, 4), \\ \sigma_5 &= (2, 4, 3), & \sigma_6 &= (1, 2), & \sigma_7 &= (1, 2)(3, 4), & \sigma_8 &= (1, 2, 3), \\ \sigma_9 &= (1, 2, 3, 4), & \sigma_{10} &= (1, 2, 4), & \sigma_{11} &= (1, 2, 4, 3), & \sigma_{12} &= (1, 3), \\ \sigma_{13} &= (1, 3, 4), & \sigma_{14} &= (1, 3, 2), & \sigma_{15} &= (1, 3, 4, 2), & \sigma_{16} &= (1, 3)(2, 4), \\ \sigma_{17} &= (1, 3, 2, 4), & \sigma_{18} &= (1, 4), & \sigma_{19} &= (1, 4, 3), & \sigma_{20} &= (1, 4)(2, 3), \\ \sigma_{21} &= (1, 4, 2, 3), & \sigma_{22} &= (1, 4, 2), & \sigma_{23} &= (1, 4, 3, 2).\end{aligned}$$

On utilise ces décompositions pour obtenir les signatures :

$$\varepsilon(\sigma_1) = \varepsilon(\sigma_2) = \varepsilon(\sigma_4) = \varepsilon(\sigma_6) = \varepsilon(\sigma_9) = \varepsilon(\sigma_{11}) = \varepsilon(\sigma_{12}) = -1,$$

$$\varepsilon(\sigma_{15}) = \varepsilon(\sigma_{17}) = \varepsilon(\sigma_{18}) = \varepsilon(\sigma_{21}) = \varepsilon(\sigma_{23}) = -1.$$

Tous les autres éléments sont de signature 1 et forment donc le groupe alterné \mathcal{A}_4 .

Solution de l'exercice 1.3. 1. Soit $n \geq 2$. Les transpositions sont les (i, j) avec $i \neq j$. Noter qu'une même transposition a deux écritures : $(i, j) = (j, i)$ (voir remarque 1.14). Les transpositions sont donc déterminées de manière unique par leur support $\{i, j\}$ avec $i \neq j$. Il y a $\binom{n}{2} = \frac{n(n-1)}{2}$ choix possibles pour ce support, c'est-à-dire autant de transpositions.

2. Soit $n \geq 3$. Les 3-cycles sont les (i, j, k) avec i, j, k deux à deux distincts. Noter qu'un même 3-cycle a trois écritures : $(i, j, k) = (j, k, i) = (k, i, j)$ obtenues par permutation circulaire des lettres (voir remarque 1.14). Les 3-cycles sont donc déterminés de manière unique par leur support $\{i, j, k\}$ et par l'ordre donné à ces lettres à permutation circulaire près. Pour le support il y a $\binom{n}{3} = \frac{n(n-1)(n-2)}{3!}$ possibilités ; pour l'ordre à permutation circulaire près, il y a $\frac{3!}{3} = 2$ possibilités. Le nombre de 3-cycles est donc

$$\frac{n(n-1)(n-2)}{3!} \times 2 = \frac{n(n-1)(n-2)}{3}.$$

3. En généralisant le raisonnement précédent, on obtient que le nombre de k -cycles dans \mathcal{S}_n est

$$\binom{n}{k} \times \frac{k!}{k} = \frac{n(n-1) \cdots (n-k+1)}{k}.$$

Solution de l'exercice 1.4. Soient σ et σ' deux permutations dans \mathcal{S}_n telles que $\text{supp}(\sigma) \cap \text{supp}(\sigma') = \emptyset$. Soit $i \in \{1, \dots, n\}$.

Supposons $i \notin \text{supp}(\sigma)$ et $i \notin \text{supp}(\sigma')$. Alors i est fixe par σ et par σ' . Donc on a $\sigma(\sigma'(i)) = i = \sigma'(\sigma(i))$.

Supposons maintenant $i \in \text{supp}(\sigma)$ et $i \notin \text{supp}(\sigma')$. Alors i est fixe par σ' donc $\sigma(\sigma'(i)) = \sigma(i)$. Par ailleurs, $\sigma(i)$ appartient à $\text{supp}(\sigma)$: en effet, si ce n'était pas le cas on aurait $\sigma(\sigma(i)) = \sigma(i)$ donc $\sigma(i) = i$, ce qui contredit $i \in \text{supp}(\sigma)$. Comme $\text{supp}(\sigma) \cap \text{supp}(\sigma') = \emptyset$, on déduit de $\sigma(i) \in \text{supp}(\sigma)$ le fait que $\sigma(i) \notin \text{supp}(\sigma')$, d'où $\sigma'(\sigma(i)) = \sigma(i)$. Cela donne finalement $\sigma(\sigma'(i)) = \sigma'(\sigma(i))$.

Il reste le cas où $i \notin \text{supp}(\sigma)$ et $i \in \text{supp}(\sigma')$, mais comme σ et σ' jouent des rôles symétriques, il se traite comme le précédent.

Ainsi on obtient $\sigma(\sigma'(i)) = \sigma'(\sigma(i))$ pour tout i , ce qui entraîne $\sigma\sigma' = \sigma'\sigma$.

Solution de l'exercice 1.5. Soient a, b, c, d des éléments deux à deux distincts de \mathbb{N}^* .

1. Un calcul direct comme dans l'exemple 1.17 donne $(a, b)(b, c) = (a, b, c)$, qui est un cycle de longueur 3.

2. En utilisant la question précédente et le fait que le carré d'une transposition est l'identité, on a $(a, b)(c, d) = (a, b)(b, c)(b, c)(c, d) = (a, b, c)(b, c, d)$. Ainsi $(a, b)(c, d)$ est le produit de deux cycles de longueur 3.
3. Soit $n \geq 3$. On sait que toute permutation est produit de transpositions (corollaire 1.22). Les transpositions étant de signature -1 , il vient que tout élément du groupe *alterné* \mathcal{A}_n est produit d'un nombre *pair* de transpositions (voir page 14). Considérons donc un produit de deux transpositions, distinct de l'identité. Il est soit de la forme $(a, b)(b, c)$, soit de la forme $(a, b)(c, d)$. En utilisant les deux questions précédentes, on obtient que tout élément de \mathcal{A}_n est produit de cycles de longueur 3.
4. On a

$$\begin{aligned} (1, 2, a)(1, 2, b)(1, 2, a)^{-1} &= (1, 2, a)(1, 2, b)(a, 2, 1) = (2, a, b), \\ (1, 2, a)(2, b, c)(1, 2, a)^{-1} &= (1, 2, a)(2, b, c)(a, 2, 1) = (a, b, c). \end{aligned}$$

Dans la même veine, on remarque que

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

Ces relations montrent que tout 3-cycle est produit de cycles de la forme $(1, 2, c)$ ou $(1, 2, c)^{-1}$ avec $c \geq 3$. D'après la question précédente, tout élément de \mathcal{A}_n est donc produit de cycles de longueur 3 de la forme $(1, 2, c)$ ou $(1, 2, c)^{-1}$ avec $c \geq 3$.

Solution de l'exercice 1.6. Soit $Z(\mathcal{S}_n) = \{\sigma \in \mathcal{S}_n \mid \forall \sigma' \in \mathcal{S}_n, \sigma\sigma' = \sigma'\sigma\}$ le centre de \mathcal{S}_n . Soient $n \geq 3$, $\sigma \in Z(\mathcal{S}_n)$ et $i \neq j$ dans $\{1, \dots, n\}$. On note τ la transposition (i, j) .

1. Comme σ est dans le centre, il commute avec τ donc $(\tau\sigma)(i) = \sigma(\tau(i)) = \sigma(j)$.
2. D'après la question précédente, τ envoie $\sigma(i)$ sur $\sigma(j)$. Mais $\sigma(i) \neq \sigma(j)$ puisque $i \neq j$ et σ est injective. Ainsi $\sigma(i)$ n'est pas un point fixe de τ . Il appartient donc au support de τ , qui n'est autre que $\{i, j\}$.
3. Soit $k \in \{1, \dots, n\} - \{i, j\}$ (un tel k existe car $n \geq 3$). Le même raisonnement que précédemment avec la transposition (i, k) au lieu de (i, j) donne $\sigma(i) \in \{i, k\}$. Donc $\sigma(i)$ appartient à $\{i, j\}$ et à $\{i, k\}$. Comme i, j, k sont deux à deux distincts, on en déduit $\sigma(i) = i$.
Pour tout $i \in \{1, \dots, n\}$, on a démontré que $\sigma(i) = i$. Cela entraîne que $\sigma = \text{id}_n$ donc $Z(\mathcal{S}_n) = \{\text{id}_n\}$.
4. Si $n = 2$, l'argument précédent ne fonctionne plus car on ne peut pas choisir k distinct à la fois de i et de j . Pour $n = 2$ on a $\mathcal{S}_2 = \{\text{id}_2, (1, 2)\}$ et ces deux éléments commutent, donc $Z(\mathcal{S}_2) = \mathcal{S}_2$.

Solution de l'exercice 1.7. 1. Soit $\tau = (i, j)$ une transposition de \mathcal{S}_n . Quitte à échanger i et j , on peut supposer $i < j$. Écrivons alors

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & i-1 & i & i+1 & \cdots & j-1 & j & j+1 & \cdots & n \\ 1 & 2 & \cdots & i-1 & j & i+1 & \cdots & j-1 & i & j+1 & \cdots & n \end{pmatrix}.$$

Les inversions de τ sont donc positionnées comme suit :

- le couple (i, j) , puisque $i < j$ et $\sigma(i) = j > \sigma(j) = i$;
- les couples (i, k) avec $i + 1 \leq k \leq j - 1$, puisque $i < k$ et $\sigma(i) = j > \sigma(k) = k$ (il y a $j - i - 1$ tels couples, puisque i est fixé);
- les couples (k, j) avec $i + 1 \leq k \leq j - 1$, puisque $k < j$ et $\sigma(k) = k > \sigma(j) = i$ (il y a $j - i - 1$ tels couples, puisque j est fixé).

Le nombre d'inversions est donc $1 + 2(j - i - 1)$. Il est impair d'où $\varepsilon(\tau) = -1$.

2. Soit n un entier fixé supérieur ou égal à 2. Démontrons que pour tout $k \in \{0, \dots, n\}$, une permutation de \mathcal{S}_n ayant au moins k points fixes est un produit de transpositions. On procède par récurrence descendante sur k . Si $k = n$, une permutation dans \mathcal{S}_n ayant au moins n points fixes n'est autre que l'identité, qui s'écrit aussi $(1, 2)(1, 2)$ car $n \geq 2$.

Supposons la propriété vérifiée pour toute permutation ayant au moins k points fixes. Montrons qu'elle l'est aussi pour celles ayant au moins $k - 1$ points fixes. Soit σ une telle permutation. Le résultat étant clair si $\sigma = \text{id}_n$, qui a n points fixes, supposons maintenant $\sigma \neq \text{id}_n$. Il existe alors $j \in \{1, \dots, n\}$ tel que $\sigma(j) \neq j$. Posons $l = \sigma(j)$. Notons τ la transposition (j, l) et ψ la permutation $\tau\sigma$. On a $\psi(i) = i$ quand i parcourt les $k - 1$ points fixes de σ , et de plus $\psi(j) = \tau(l) = j$. Donc ψ a au moins k points fixes. Par hypothèse de récurrence, ψ est un produit de transpositions. En composant ψ à gauche par τ , on en déduit que $\sigma = \tau\psi$ est aussi produit de transpositions, ce qui démontre la propriété au rang k et conclut la récurrence.

Solution de l'exercice 1.8. 1. Posons $c = (a_1, \dots, a_k)$. Soit $i \in \{1, \dots, n\}$. Si $i \notin \{\sigma(a_1), \dots, \sigma(a_k)\}$ alors $\sigma^{-1}(i) \notin \{a_1, \dots, a_k\}$ c'est-à-dire $\sigma^{-1}(i) \notin \text{supp}(c)$, et donc

$$(\sigma c \sigma^{-1})(i) = \sigma(c(\sigma^{-1}(i))) = \sigma(\sigma^{-1}(i)) = i.$$

Si $i = \sigma(a_j)$ pour un certain $j \in \{1, \dots, k\}$ alors

$$(\sigma c \sigma^{-1})(i) = (\sigma c \sigma^{-1})\sigma(a_j) = \sigma(c(a_j)) = \sigma(a_{j+1})$$

(en posant $a_{k+1} = a_1$). Ainsi on obtient $\sigma(a_1, \dots, a_k)\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k))$.

2. Posons $c' = (b_1, \dots, b_k)$. Par la question précédente, pour tout $\sigma \in \mathcal{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

Soit maintenant $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ l'application définie par les conditions suivantes :

- (a) $\sigma(a_i) = b_i$ pour tout $i \in \{1, \dots, k\}$;
- (b) σ restreinte à $\{1, \dots, n\} - \{a_1, \dots, a_k\}$ est une bijection quelconque sur $\{1, \dots, n\} - \{b_1, \dots, b_k\}$ (cette condition est toujours réalisable car les ensembles $\{1, \dots, n\} - \{a_1, \dots, a_k\}$ et $\{1, \dots, n\} - \{b_1, \dots, b_k\}$ ont même cardinal).

Alors σ est une permutation dans \mathcal{S}_n et $\sigma c \sigma^{-1} = c'$ par construction. De plus on a $\text{supp}(c') = \{b_1, \dots, b_k\} = \{\sigma(a_1), \dots, \sigma(a_k)\} = \sigma(\text{supp}(c))$.

3. (a) Le type de σ ne dépend pas de la décomposition en cycles à supports deux à deux disjoints qui est choisie : en effet, cette décomposition est unique à l'ordre près des facteurs, et dans la définition du type, les cycles sont de toute manière réordonnés par longueur décroissante.
- (b) On a $\sigma_1 = (1, 2, 7, 9)(3, 6, 8)(4, 5)$ et $\sigma_2 = (1, 5, 4, 2, 6)(3, 7, 9)$. Donc leurs types sont respectivement 4, 3, 2 et 5, 3.
- (c) Supposons que deux permutations σ et σ' distinctes de l'identité sont conjuguées dans \mathcal{S}_n : il existe $g \in \mathcal{S}_n$ tel que $\sigma' = g\sigma g^{-1}$. Soit $\sigma = c_1 \dots c_s$ la décomposition en cycles à supports deux à deux disjoints de σ , en supposant $\ell(c_1) \geq \dots \geq \ell(c_s)$. En posant pour tout $i \in \{1, \dots, s\}$, $c'_i = gc_i g^{-1}$, on a

$$\sigma' = gc_1 \dots c_s g^{-1} = (gc_1 g^{-1})(gc_2 g^{-1}) \dots (gc_s g^{-1}) = c'_1 \dots c'_s.$$

D'après la question 1, c'_i est un cycle de même longueur que c_i et de support $g(\text{supp}(c_i))$. Ainsi les cycles c'_1, \dots, c'_s sont à supports deux à deux disjoints par bijectivité de g . Par unicité dans le théorème 1.21, l'écriture $\sigma' = c'_1 \dots c'_s$ est la décomposition en cycles à supports deux à deux disjoints de σ' , à l'ordre près des facteurs. On en déduit que σ et σ' ont même type.

Réciproquement supposons que σ et σ' ont même type. On écrit leurs décompositions en cycles à supports deux à deux disjoints :

$$\sigma = c_1 \dots c_s, \quad \sigma' = d_1 \dots d_k$$

où les cycles sont ordonnés par longueur décroissante. Par hypothèse, on a $s = k$ et $\ell(c_i) = \ell(d_i)$ quelque soit i . La question 2 entraîne qu'ils sont conjugués deux à deux : il existe $g_i \in \mathcal{S}_n$ tel que

$$d_i = g_i c_i g_i^{-1}$$

et $\text{supp}(d_i) = g_i(\text{supp}(c_i))$. Soit $g : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ l'application définie par

$$\forall i \in \{1, \dots, s\}, g|_{\text{supp}(c_i)} = g_i$$

et $g(x) = x$ pour tout point fixe x de σ . Alors on peut vérifier que g ainsi construite est une permutation dans \mathcal{S}_n et que, du fait que les supports des c_i sont deux à deux disjoints,

$$g\sigma g^{-1} = gc_1 \dots c_s g^{-1} = (gc_1 g^{-1}) \dots (gc_s g^{-1}) = d_1 \dots d_s = \sigma'.$$

Ainsi σ et σ' sont conjugués dans \mathcal{S}_n .

Solution de l'exercice 1.9. Soit n un entier naturel non nul. À toute permutation $\sigma \in \mathcal{S}_n$ on associe la matrice $M_\sigma = (m_{i,j})_{1 \leq i,j \leq n}$ de $M_n(\mathbb{R})$ définie par

$$m_{i,j} = \begin{cases} 1 & \text{si } i = \sigma(j) \\ 0 & \text{sinon.} \end{cases}$$

1. Supposons $n = 4$. Pour $\sigma = (1, 2, 3, 4)$ on a $M_\sigma = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. Pour

$$\sigma = (1, 3)(2, 4) \text{ on a } M_\sigma = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

2. L'entier n et la permutation σ sont dorénavant quelconques. La trace de M_σ est par définition $\text{Tr } M_\sigma = \sum_{j=1}^n m_{j,j}$. Or $m_{j,j}$ est non nul si et seulement si $j = \sigma(j)$ c'est-à-dire si j est un point fixe de σ ; dans ce cas, le coefficient correspondant vaut 1. On en déduit

$$\text{Tr } M_\sigma = \sum_{1 \leq j \leq n, m_{j,j} \neq 0} m_{j,j} = \sum_{1 \leq j \leq n, j = \sigma(j)} 1,$$

qui est égal au nombre de points fixes de σ .

3. Une formule classique d'algèbre linéaire affirme que

$$\det M_\sigma = \sum_{\rho \in \mathcal{S}_n} \varepsilon(\rho) \prod_{j=1}^n m_{\rho(j),j}.$$

Or le produit est non nul si et seulement si tous ses termes sont non nuls c'est-à-dire si $\rho(j) = \sigma(j)$ pour tout j , autrement dit si $\rho = \sigma$. On conclut que la somme ne comporte qu'un terme non nul, celui correspondant à $\rho = \sigma$, et donc $\det M_\sigma = \varepsilon(\sigma) \prod_{j=1}^n m_{\sigma(j),j} = \varepsilon(\sigma) \times 1 = 1$.

4. Soient σ et σ' deux permutations dans \mathcal{S}_n . Notons $m_{i,j}$ (resp. $m'_{i,j}$) les coefficients de la matrice M_σ (resp. $M_{\sigma'}$). D'après une autre formule classique d'algèbre linéaire, les coefficients de la matrice produit $M_\sigma M_{\sigma'}$ sont, pour i et j dans $\{1, \dots, n\}$,

$$(M_\sigma M_{\sigma'})_{i,j} = \sum_{k=1}^n m_{i,k} m'_{k,j}.$$

Or $m_{i,k}$ est non nul seulement si $i = \sigma(k)$ et $m'_{k,j}$ est non nul seulement si $k = \sigma'(j)$. On en déduit que $m_{i,k} m'_{k,j}$ est non nul seulement quand i vaut $\sigma(k) = \sigma(\sigma'(j)) = (\sigma\sigma')(j)$. Dans ce cas, le coefficient vaut $1 \times 1 = 1$. En conclusion, on a

$$(M_\sigma M_{\sigma'})_{i,j} = \begin{cases} 1 & \text{si } i = (\sigma\sigma')(j) \\ 0 & \text{sinon.} \end{cases}$$

ce qui prouve que $M_{\sigma\sigma'} = M_\sigma M_{\sigma'}$.

Corrigé des exercices du chapitre 2

Solution de l'exercice 2.1. Soient x et y deux éléments de G . Montrons que $xy = yx$. Par hypothèse on a $1_G = (xy)^2 = xyxy$. En multipliant les deux membres de l'égalité à gauche par x et en utilisant $x^2 = 1_G$, cela donne $x = yxy$. En multipliant ensuite les deux membres à droite par y et en utilisant $y^2 = 1_G$, on obtient bien $xy = yx$. Le groupe G est donc abélien.

Solution de l'exercice 2.2. Soit G un groupe, de neutre noté e_G .

1. On a $e_G e_G = e_G$ d'après la définition 2.1, d'où $e_G^{-1} = e_G$ par unicité de l'inverse (proposition 2.2).
2. Soit $x \in G$. Par définition de x^{-1} on a $xx^{-1} = e_G = x^{-1}x$. Par unicité de l'inverse, cela entraîne que l'inverse de x^{-1} dans G est x c'est-à-dire $(x^{-1})^{-1} = x$.
3. Soient x, y, z dans G . Si $xy = xz$, en multipliant à gauche par x^{-1} dans G on obtient $y = z$. Même chose à partir de $yx = zx$ en multipliant à droite par $x^{-1} \in G$.
4. Soient x, y dans G . Calculons le produit suivant :

$$(xy)(y^{-1}x^{-1}) = xyy^{-1}x^{-1} = xe_Gx^{-1} = xx^{-1} = e_G$$

et de même

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

Par unicité de l'inverse, l'inverse de xy dans G est donc $y^{-1}x^{-1}$.

5. Soit $x \in G$. Supposons qu'il existe $y \in G$ satisfaisant $xy = e_G$. Pour montrer que y est l'inverse de x^{-1} , il ne reste qu'à établir que $yx = e_G$. En multipliant $xy = e_G$ à droite par x , on obtient $xyx = x$. En multipliant à gauche par x^{-1} , on en déduit $yx = e_G$.

Remarque. Cette propriété montre que, dans un groupe, tout inverse à droite est automatiquement un inverse à gauche (et réciproquement).

Solution de l'exercice 2.3. 1. — L'addition est une loi interne sur $M_{n,p}(\mathbb{R})$.
— L'addition est associative : pour tous $(A, B, C) \in M_{n,p}(\mathbb{R})^3$, on a $A + (B + C) = (A + B) + C$.

- L'addition admet un élément neutre : la matrice nulle notée $0 \in M_{n,p}(\mathbb{R})$. En effet pour tout $A \in M_{n,p}(\mathbb{R})$, on a $A + 0 = 0 + A = A$.
- Tout élément $A \in M_{n,p}(\mathbb{R})$ admet un inverse dans $M_{n,p}(\mathbb{R})$ pour l'addition : c'est la matrice $-A$, dont les coefficients sont les opposés de ceux de A . En effet on a bien $A + (-A) = (-A) + A = 0$.

Ceci montre que $(M_{n,p}(\mathbb{R}), +)$ est un groupe. Noter qu'il est abélien car $A + B = B + A$ pour tous A, B dans $M_{n,p}(\mathbb{R})$.

2. Munissons l'ensemble $\mathcal{P}(E)$ des parties de E de l'intersection \cap .
 - L'intersection est une loi interne sur $\mathcal{P}(E)$ car l'intersection de deux parties de E est une partie de E .
 - L'intersection est associative. En effet, pour toutes parties A, B et C de E , on a bien $A \cap (B \cap C) = (A \cap B) \cap C$.
 - Muni de \cap , $\mathcal{P}(E)$ possède un élément neutre qui est E . En effet, pour toute partie A de E , on a $A \cap E = E \cap A = A$.
 - Par contre, si $E \neq \emptyset$, tout élément de $\mathcal{P}(E)$ n'admet pas forcément un inverse pour \cap : par exemple la partie \emptyset de E n'a pas d'inverse pour \cap car pour tout $A \in \mathcal{P}(E)$, on a $A \cap \emptyset = \emptyset \neq E$.

On conclut que si $E \neq \emptyset$ alors $(\mathcal{P}(E), \cap)$ n'est pas un groupe. Lorsque $E = \emptyset$ alors $\mathcal{P}(E) = \{\emptyset\}$, qui est un groupe abélien pour l'intersection.

Remarque. Pour les structures où seuls les axiomes d'associativité et d'existence de l'élément neutre sont satisfaites comme c'est le cas ici, on parle de monoïde.

3. L'ensemble \mathbb{R} muni $*$ n'est pas un groupe : en effet la loi $*$ n'est pas définie sur \mathbb{R} car 0 n'admet pas d'inverse dans \mathbb{R} .
4. On remarque au préalable que $1 + xy \neq 0$ lorsque x, y appartiennent à X , ce qui fait que la fraction $\frac{x+y}{1+xy}$ a bien un sens dans \mathbb{R} .
 - Montrons que la loi \star est interne sur X . Pour tous x et y réels vérifiant $|x| < 1$ et $|y| < 1$ on a

$$x + y - (1 + xy) = (1 - x)(y - 1) < 0$$

donc $\frac{x+y}{1+xy} < 1$. On montre de même que $\frac{x+y}{1+xy} > -1$. Cela prouve que $\frac{x+y}{1+xy} \in X$.

- La loi \star est associative. En effet, pour tous x, y, z dans X on a

$$x \star (y \star z) = x \star \frac{y+z}{1+yz} = \frac{x + \frac{y+z}{1+yz}}{1 + x \frac{y+z}{1+yz}} = \frac{x + y + z + xyz}{1 + xy + xz + yz}$$

et un calcul similaire pour $(x \star y) \star z$ donne le même résultat.

- La loi possède un élément neutre qui est 0 . En effet pour tout $x \in X$, on a $x \star 0 = \frac{x}{1} = x$ et de même $0 \star x = x$.
- Tout élément x de X possède un inverse pour \star qui est $-x$. En effet on a $x \star (-x) = 0$ et $(-x) \star x = 0$.

Ceci montre que (X, \star) est un groupe. Noter qu'il est abélien car $x \star y = y \star x$ pour tous x, y dans X .

Solution de l'exercice 2.4. 1. On procède comme dans l'exercice précédent. L'expression $(x^3 + y^3)^{1/3}$ a un sens pour tous x, y réels et c'est un nombre réel. Donc $*$ est un loi interne sur \mathbb{R} . Elle est associative car pour tous x, y, z réels on a

$$\begin{aligned}(x * y) * z &= (x^3 + y^3)^{1/3} * z = (x^3 + y^3 + z^3)^{1/3}, \\ x * (y * z) &= x * (y^3 + z^3)^{1/3} = (x^3 + y^3 + z^3)^{1/3}\end{aligned}$$

(on utilise le fait que, pour tout α réel, $(\alpha^{1/3})^3 = \alpha$). De plus la loi admet un élément neutre qui est 0 car tout $x \in \mathbb{R}$ vérifie $x * 0 = x = 0 * x$. Enfin l'inverse de x pour $*$ est $-x$ car $x * (-x) = 0 = (-x) * x$. Ceci montre que $(\mathbb{R}, *)$ est un groupe. De plus il est abélien car $x * y = (x^3 + y^3)^{1/3} = (y^3 + x^3)^{1/3} = y * x$ pour tous $x, y \in \mathbb{R}$.

Remarque. Cet exemple montre qu'un même ensemble peut être muni de différentes lois de groupe (ici \mathbb{R} avec $+$ et $*$).

2. Notons $f : (\mathbb{R}, *) \rightarrow (\mathbb{R}, +)$ l'application $x \mapsto x^3$. Pour tous x, y dans \mathbb{R} on a

$$f(x * y) = f((x^3 + y^3)^{1/3}) = x^3 + y^3 = f(x) + f(y)$$

ce qui montre que f est un morphisme de groupes. Il est injectif car son noyau est réduit à l'élément neutre 0 : en effet si $f(x) = 0$ alors $x^3 = 0$ dans \mathbb{R} d'où $x = 0$. Enfin il est surjectif car tout élément $y \in \mathbb{R}$ s'écrit $y = x^3 = f(x)$ en prenant $x = y^{1/3} \in \mathbb{R}$. Ainsi f est isomorphisme de groupes de $(\mathbb{R}, *)$ sur $(\mathbb{R}, +)$.

Solution de l'exercice 2.5. 1. (a) C'est une formule de la proposition 1.15 du cours, qui a été démontrée dans l'exercice 1.8.

- (b) Si (i', j') est une transposition, il existe une permutation $\sigma \in \mathcal{S}_n$ telle que $\sigma(i) = i'$ et $\sigma(j) = j'$ car $i \neq j$ et $i' \neq j'$. Avec la question précédente, on conclut que $\sigma(i, j)\sigma^{-1} = (i', j')$.

2. Soit $f : \mathcal{S}_n \rightarrow \mathbb{C}^*$ un morphisme de groupes. Soit (i, j) une transposition. On pose $z = f(i, j) \in \mathbb{C}^*$. Soit (i', j') une autre transposition dans \mathcal{S}_n . D'après la question précédente, il existe une permutation $\sigma \in \mathcal{S}_n$ telle que $\sigma(i, j)\sigma^{-1} = (i', j')$. On a donc, en utilisant le fait que f est un morphisme de groupes,

$$f(i', j') = f(\sigma(i, j)\sigma^{-1}) = f(\sigma)f(i, j)f(\sigma)^{-1}.$$

Mais \mathbb{C}^* étant commutatif, on conclut que

$$f(i', j') = f(\sigma)f(\sigma)^{-1}f(i, j) = f(i, j) = z$$

d'où le résultat.

3. Toute transposition τ vérifie $\tau^2 = \text{id}$. Donc $f(\tau^2) = f(\text{id}) = 1$. Comme $f(\tau^2) = f(\tau)^2$ du fait que f est un morphisme de groupes, cela entraîne $z^2 = 1$ dans \mathbb{C}^* d'où z vaut 1 ou -1 .

4. On sait que \mathcal{S}_n est engendré par l'ensemble de ses transpositions (corollaire 1.22). Par conséquent, tout morphisme de groupes de \mathcal{S}_n dans \mathbb{C}^* est déterminé de manière unique par les valeurs qu'il prend sur les transpositions. Or on a montré que pour tout morphisme $f : \mathcal{S}_n \rightarrow \mathbb{C}^*$, les transpositions ont toutes même image $z = \pm 1$ par f . Ainsi il existe au plus deux morphismes de \mathcal{S}_n dans \mathbb{C}^* , selon que z vaut 1 ou -1 . Il reste à montrer que chacune de ces valeurs de z donne bien un morphisme de groupes. Si $z = 1$, c'est le morphisme trivial qui envoie tout élément de \mathcal{S}_n sur 1. Si $z = -1$, alors f n'est autre que le morphisme signature ε puisque la signature de toute transposition vaut -1 .

Remarque. Cette caractérisation en termes de morphismes de \mathcal{S}_n peut justifier l'intérêt qu'on porte à la signature.

Solution de l'exercice 2.6. 1. Soit $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ un morphisme de groupes. On a alors $f(0) = 0$. Si $n \in \mathbb{Z} - \{0\}$ on a

$$f(n) = \begin{cases} f(\underbrace{1+1+\dots+1}_{n \text{ fois}}) = nf(1) & \text{si } n \geq 0 \\ f(\underbrace{-1-1-\dots-1}_{-n \text{ fois}}) = (-n)f(-1) & \text{si } n \leq 0. \end{cases}$$

Comme $f(-1)$ doit être égal à l'opposé de l'image de 1 on a $f(-1) = -f(1)$. Ainsi pour tout $n \in \mathbb{Z}$ on a $f(n) = nf(1)$. Nous avons montré que si f est un morphisme de $(\mathbb{Z}, +)$ dans lui-même alors il existe $a \in \mathbb{Z}$ tel que $f(n) = na$ pour tout $n \in \mathbb{Z}$.

Réciproquement, fixons $a \in \mathbb{Z}$ et considérons l'application $f_a : \mathbb{Z} \rightarrow \mathbb{Z}$ donnée par $f_a(n) = na$ pour tout $n \in \mathbb{Z}$. Alors f_a est un morphisme de groupes : en effet, si n, m sont dans \mathbb{Z} , on a $f_a(n+m) = (n+m)a = f_a(n) + f_a(m)$.

En conclusion, les morphismes de $(\mathbb{Z}, +)$ dans lui-même sont les applications de la forme $f_a : n \mapsto na$ avec $a \in \mathbb{Z}$.

Calculons le noyau de f_a . Si $a = 0$ alors f_a étant identiquement nulle, son noyau est \mathbb{Z} et l'application n'est pas injective. Supposons $a \neq 0$. Soit $n \in \mathbb{Z}$ tel que $f(n) = 0$. On a alors $na = 0$ dans \mathbb{Z} d'où $n = 0$. Dans ce cas, $\text{Ker } f_a = \{0\}$. Donc f_a est injective pour tout a non nul dans \mathbb{Z} .

Concernant l'image de f_a , il est immédiat de voir que $\text{Im } f_a = a\mathbb{Z}$, l'ensemble des multiples de a . Il s'ensuit que f_a est surjective si et seulement si $a = 1$ ou $a = -1$ (rappelons que $m\mathbb{Z} = (-m)\mathbb{Z}$).

Ainsi les seuls automorphismes de groupes de $(\mathbb{Z}, +)$ sont les f_a avec $a \in \{\pm 1\}$.

2. On procède comme dans la question précédente. Soit $f : (\mathbb{Q}, +) \rightarrow (\mathbb{Q}, +)$ un morphisme de groupes. Soit p/q un élément de \mathbb{Q} avec p et q des entiers positifs et $q \neq 0$. On a

$$qf(p/q) = \underbrace{f(p/q) + f(p/q) + \dots + f(p/q)}_{q \text{ fois}} = f(q(p/q)) = f(p) = pf(1).$$

On a donc $f(p/q) = (p/q)f(1)$. Cette égalité est aussi vraie si $p/q \leq 0$ car $f(-p/q) = -f(p/q)$. Donc il existe $a \in \mathbb{Q}$ tel que, pour tout $x \in \mathbb{Q}$, on ait $f(x) = xa$.

Réciproquement, fixons $a \in \mathbb{Q}$ et considérons l'application $f_a : \mathbb{Q} \rightarrow \mathbb{Q}$ donnée par $f_a(x) = xa$ pour tout $x \in \mathbb{Q}$. Alors f_a est un morphisme de groupes car pour tous x, y dans \mathbb{Q} , on a $f_a(x + y) = f_a(x) + f_a(y)$.

En conclusion, les morphismes de $(\mathbb{Q}, +)$ dans lui-même sont les applications de la forme $f_a : x \mapsto xa$ avec $a \in \mathbb{Q}$.

Calculons le noyau de f_a : si $a = 0$ alors f_a est identiquement nulle et si $a \neq 0$ alors f_a est injective.

Concernant l'image de f_a , il est immédiat de voir que $\text{Im } f_a = a\mathbb{Q}$. Si $a = 0$, l'image est nulle et f_a n'est pas surjective. Si $a \neq 0$, on a $a\mathbb{Q} = \mathbb{Q}$: en effet, on a clairement $a\mathbb{Q} \subset \mathbb{Q}$, et réciproquement, si $x \in \mathbb{Q}$ alors l'élément $y = x/a$ vérifie $ay = x$. On conclut que f_a est surjective si et seulement si $a \neq 0$.

Ainsi les automorphismes de groupes de $(\mathbb{Q}, +)$ sont les f_a avec $a \neq 0$ dans \mathbb{Q} .

3. Soit $f : (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$ un morphisme de groupes qui est continu. Un raisonnement comme auparavant montre l'existence de $a = f(1) \in \mathbb{R}$ tel que, pour tout $x \in \mathbb{Q}$, on a $f(x) = xa$. Montrons qu'on a en fait $f(x) = xa$ pour tout $x \in \mathbb{R}$. On utilise pour cela un argument analytique reposant sur la densité de \mathbb{Q} de \mathbb{R} . Soit donc $x \in \mathbb{R}$. Par densité, il existe une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de \mathbb{Q} qui converge vers x . Comme les x_n sont rationnels, on a pour tout $n \in \mathbb{N}$, $f(x_n) = x_n a$. En passant à la limite de part et d'autre, on obtient $\lim_{n \rightarrow \infty} f(x_n) = xa$. Or, f est continue donc $\lim_{n \rightarrow \infty} f(x_n) = f(\lim_{n \rightarrow \infty} x_n)$. On en déduit $f(x) = xa$ comme souhaité. Comme dans les questions précédentes, on vérifie que pour tout $a \in \mathbb{R}$ l'application $f_a : \mathbb{R} \rightarrow \mathbb{R}$ donnée par $f_a(x) = xa$ pour tout $x \in \mathbb{R}$, est un morphisme continu de groupes de $(\mathbb{R}, +)$ dans lui-même.

Solution de l'exercice 2.7. Soit G un groupe d'ordre 1. Il ne possède qu'un élément, son neutre 1_G . Sa table de Cayley est simplement

(G, \cdot)	1_G
1_G	1_G

À isomorphisme près, il n'existe donc qu'un groupe d'ordre 1.

Soit G un groupe d'ordre 2 : notons 1_G et a ses éléments, avec $a \neq 1_G$. Alors a^2 vaut 1_G ou a . Or si $a^2 = a$ alors on déduit $a = 1_G$ par simplification, qui est impossible. Donc $a^2 = 1_G$. Ainsi la table de Cayley de G est nécessairement :

(G, \cdot)	1_G	a
1_G	1_G	a
a	a	1_G

À identification près, on reconnaît la table de (\mathcal{S}_2, \circ) (cf. remarque 2.13) ou encore celle de $(\{\pm 1\}, \cdot)$. Donc tout groupe d'ordre 2 est isomorphe à \mathcal{S}_2 (ou à $\{\pm 1\}$, ce qui revient au même).

Soit G un groupe d'ordre 3 : notons $1_G, a, b$ ses éléments distincts deux à deux. Le même raisonnement que précédemment montre que $ab \neq a$ et $ab \neq b$. On a donc $ab = 1_G$. De la même manière on montre que $ba = 1_G$. On a ainsi $b = a^{-1}$ et on en déduit $a^2 = b$ (puisque $a^2 \neq 1_G$ et $a^2 \neq a$). Un raisonnement similaire donne $b^2 = a$. Ainsi la table de Cayley de G est nécessairement :

(G, \cdot)	1_G	a	b
1_G	1_G	a	b
a	a	b	1_G
b	b	1_G	a

On reconnaît la table de (U_3, \cdot) , le groupe multiplicatif des racines 3-èmes de l'unité, en identifiant a à $e^{2i\pi/3}$ et b à $e^{4i\pi/3}$. Donc tout groupe d'ordre 3 est isomorphe à U_3 .

Solution de l'exercice 2.8. 1. On sait que $\text{GL}_2(\mathbb{R})$ est un groupe pour la

multiplication. Constatons d'abord qu'une matrice de la forme $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$

avec $a \in \mathbb{R}$ est bien inversible, d'inverse $\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$. Ainsi le sous-ensemble H

des matrices de la forme $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ avec $a \in \mathbb{R}$ est bien contenu dans $\text{GL}_2(\mathbb{R})$.

Maintenant utilisons la proposition 2.23.

— L'ensemble H contient la matrice identité.

— Si on se donne deux éléments $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ dans H avec a et b dans \mathbb{R} , on a

$$AB^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix}$$

qui est bien un élément de H .

On conclut que H est un sous-groupe de $\text{GL}_2(\mathbb{R})$.

Remarque. Il est facile de voir que H est abélien, tandis que $\text{GL}_2(\mathbb{R})$ n'est pas.

2. Les matrices de la forme $\begin{pmatrix} 1 & a \\ b & 1 \end{pmatrix}$ sont inversibles car leur déterminant est $1 - ab$, qui est supposé non nul. Donc l'ensemble K formé de ces matrices est bien contenu dans $\text{GL}_2(\mathbb{R})$.

— L'ensemble K contient la matrice identité (prendre $a = b = 0$).

— Si on se donne $A = \begin{pmatrix} 1 & a \\ b & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & a' \\ b' & 1 \end{pmatrix}$ dans K alors

$$AB = \begin{pmatrix} 1 + ab' & a + a' \\ b + b' & 1 + ba' \end{pmatrix}.$$

Mais cette matrice n'est généralement pas dans K car $1 + ab' \neq 1$. Donc K n'est pas stable par multiplication.

On en déduit que K n'est pas un sous-groupe de $\text{GL}_2(\mathbb{R})$.

Solution de l'exercice 2.9. Soit $n \in \mathbb{N}$. Montrons que H_n est un sous-groupe de G .

— D'abord, H_n contient 1_G car $1_G^n = 1_G$.

— Soient x, y deux éléments de H_n . Il existe alors a et b dans G tels que $x = a^n$ et $y = b^n$. On en déduit $xy^{-1} = a^n(b^n)^{-1} = a^n(b^{-1})^n$. Comme G est abélien, on en déduit $a^n(b^{-1})^n = (ab^{-1})^n$ (attention ceci est faux si G ne l'est pas). On a donc : $xy^{-1} = (ab^{-1})^n$ avec $ab^{-1} \in G$ d'où $xy^{-1} \in H_n$.

On conclut par la proposition 2.23 que H_n est un sous-groupe de G .

Solution de l'exercice 2.10. Les sous-groupes de \mathcal{S}_3 sont finis. Ils sont donc engendrés par une famille finie d'éléments.

Cherchons ceux engendrés par un élément. À l'aide du corollaire 2.36 et du calcul des puissances successives des permutations, on trouve

$$\begin{aligned} \langle \text{id} \rangle &= \{\text{id}\}, \\ \langle (1, 2) \rangle &= \{\text{id}, (1, 2)\}, \\ \langle (1, 3) \rangle &= \{\text{id}, (1, 3)\}, \\ \langle (2, 3) \rangle &= \{\text{id}, (2, 3)\}, \\ \langle (1, 2, 3) \rangle &= \{\text{id}, (1, 2, 3), (1, 3, 2)\}, \\ \langle (1, 3, 2) \rangle &= \{\text{id}, (1, 3, 2), (1, 2, 3)\} = \langle (1, 2, 3) \rangle \end{aligned}$$

car lorsque c est un k -cycle, k est le plus petit entier tel que $c^k = \text{id}$ (voir chapitre 1). On a ainsi obtenu 5 sous-groupes distincts.

Cherchons les sous-groupes engendrés par une famille à deux éléments distincts. On peut supposer ces éléments distincts de id (sinon on retombe dans le cas précédent). Il s'agit de déterminer les sous-groupes suivants :

$$\begin{aligned} &\langle (1, 2), (1, 3) \rangle, \langle (1, 2), (2, 3) \rangle, \langle (1, 3), (2, 3) \rangle, \\ &\langle (1, 2), (1, 2, 3) \rangle, \langle (1, 2), (1, 3, 2) \rangle, \\ &\langle (1, 3), (1, 2, 3) \rangle, \langle (1, 3), (1, 3, 2) \rangle, \\ &\langle (2, 3), (1, 2, 3) \rangle, \langle (2, 3), (1, 3, 2) \rangle. \end{aligned}$$

Nous allons voir que tous sont égaux à \mathcal{S}_3 . Pour ceux engendrés par une transposition et un 3-cycle, on procède comme dans l'exemple 2.35. Pour ceux engendrés par deux transpositions, on procède comme suit. Par exemple le sous-groupe $\langle (1, 2), (1, 3) \rangle$ contient $(1, 2)(1, 3) = (1, 3, 2)$ et $(1, 2)(1, 3)(1, 2) = (2, 3)$: il contient donc toutes les transpositions. D'après le corollaire 1.22, on a donc $\langle (1, 2), (1, 3) \rangle = \mathcal{S}_3$.

Il n'est pas nécessaire de chercher les sous-groupes engendrés par au moins 3 éléments : en effet, un tel sous-groupe contient un sous-groupe engendré par deux éléments distincts et sera donc égal à \mathcal{S}_3 par ce qui précède. En conclusion, la liste des sous-groupes de \mathcal{S}_3 est

$$\langle \text{id} \rangle, \langle (1, 2) \rangle, \langle (1, 3) \rangle, \langle (2, 3) \rangle, \langle (1, 2, 3) \rangle, \mathcal{S}_3.$$

Solution de l'exercice 2.11. Soient H et K deux sous-groupes d'un groupe G .

Si $H \subset K$ ou $K \subset H$, alors $H \cup K$ vaut K ou H , et dans tous les cas c'est un sous-groupe de G .

Réciproquement supposons que $H \cup K$ est un sous-groupe de G . Soient $h \in H$ et $k \in K$. Alors hk appartient au sous-groupe $H \cup K$. On en déduit :

- ou bien $hk \in H$; dans ce cas, $hk = h'$ avec $h' \in H$ d'où $k = h'h^{-1}$; comme H est un sous-groupe, on obtient $k \in H$;
- ou bien $hk \in K$; dans ce cas, $hk = k'$ avec $k' \in K$ d'où $h = k'k^{-1}$; comme K est un sous-groupe, on obtient $h \in K$.

Maintenant supposons H non contenu dans K . Le raisonnement précédent montre que tout $k \in K$ est alors contenu dans H . On a ainsi montré que $K \subset H$, ce qu'il fallait démontrer.

Solution de l'exercice 2.12. On a vu dans le cours que l'ensemble $n\mathbb{Z}$, pour $n \in \mathbb{Z}$, est un sous-groupe de $(\mathbb{Z}, +)$. Réciproquement soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, on peut écrire $H = 0\mathbb{Z}$. Supposons donc H non nul. Alors l'ensemble $H \cap (\mathbb{N} - \{0\})$ d'entiers naturels est non vide. Il a un plus petit élément, noté n . Comme $n \in H$ et H est stable par addition, on a $n\mathbb{Z} \subset H$. Inversement soit $a \in H$. La division euclidienne de a par n s'écrit $a = nq + r$ avec $0 \leq r < n$. Alors $a - nq$ appartient à $H \cap \mathbb{N}$ et $a - nq < n$. Par minimalité de n , on en déduit $a - nq = 0$ d'où $a \in n\mathbb{Z}$. On a ainsi montré que $H = n\mathbb{Z}$.

Solution de l'exercice 2.13. Supposons que le groupe $(\mathbb{Q}, +)$ est de type fini. Il est alors engendré par une famille finie $\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}$ de nombres rationnels. En utilisant la proposition 2.34 et le fait que \mathbb{Q} est abélien, on en déduit que pour tout élément $x \in \mathbb{Q}$, il existe $\lambda_1, \dots, \lambda_n$ dans \mathbb{Z} tels que

$$x = \lambda_1 \frac{p_1}{q_1} + \dots + \lambda_n \frac{p_n}{q_n}.$$

En réduisant au même dénominateur, on obtient $x = \frac{a}{m}$ où $a \in \mathbb{Z}$ et m est le ppcm des dénominateurs q_1, \dots, q_n . Ainsi il existe m tel que tout $x \in \mathbb{Q}$ vérifie $mx \in \mathbb{Z}$. C'est impossible : prendre par exemple $x = \frac{1}{2m} \in \mathbb{Q}$. Ainsi le groupe $(\mathbb{Q}, +)$ n'est pas de type fini.

Solution de l'exercice 2.14. Soient G et H deux groupes. Considérons l'application

$$\begin{aligned} \pi : G \times H &\longrightarrow G \\ (g, h) &\longmapsto g. \end{aligned}$$

où il est sous-entendu que $G \times H$ est le groupe produit direct. Soient (g_1, h_1) et (g_2, h_2) dans $G \times H$. On a

$$\begin{aligned} \pi((g_1, h_1)(g_2, h_2)) &= \pi(g_1g_2, h_1h_2) \\ &= g_1g_2 \\ &= \pi(g_1, h_1)\pi(g_2, h_2). \end{aligned}$$

Ainsi π est un morphisme de groupes.

Calculons son noyau. Pour $(g, h) \in G \times H$, on a $\pi(g, h) = 1_G$ si et seulement si $g = 1_G$. On en conclut $\text{Ker } \pi = \{1_G\} \times H$. Il est clair que $\text{Ker } \pi$ est isomorphe

à H , via l'application $\{1_G\} \times H \rightarrow H$, $(1_G, h) \mapsto h$. De plus on a $\text{Im } \pi = G$: en effet, par définition, on a $\text{Im } \pi \subset G$ et si $g \in G$, on a $\pi(g, 1_H) = g$ donc $G \subset \text{Im } \pi$. On en déduit que π est surjectif. Ainsi π est un isomorphisme.

Solution de l'exercice 2.15. Soient G_1 et G_2 deux groupes, H_1 un sous-groupe de G_1 et H_2 un sous-groupe de G_2 . Posons $H = H_1 \times H_2$, qui est un sous-ensemble de $G = G_1 \times G_2$. Alors H contient le neutre $1_G = (1_{G_1}, 1_{G_2})$ car $1_{G_1} \in H_1$ et $1_{G_2} \in H_2$. De plus, pour tous $x = (x_1, x_2)$ et $y = (y_1, y_2)$ dans H , avec x_1, y_1 dans H_1 et x_2, y_2 dans H_2 , on a

$$\begin{aligned}xy &= (x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2) \in H, \\x^{-1} &= (x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1}) \in H\end{aligned}$$

puisque H_1 et H_2 sont stables par multiplication et passage à l'inverse. On conclut que H est un sous-groupe de G .

Corrigé des exercices du chapitre 3

Solution de l'exercice 3.1. 1. Dans l'exercice 1.1, on a obtenu les décompositions en cycles à supports deux à deux disjoints :

$$\sigma_1 = (1, 2, 7, 9)(3, 6, 8)(4, 5)$$

$$\sigma_2 = (1, 5, 4, 2, 6)(3, 7, 9).$$

En appliquant la proposition 3.8, on obtient que les ordres de σ_1 et σ_2 sont $\text{ord}(\sigma_1) = \text{ppcm}(4, 3, 2) = 12$ et $\text{ord}(\sigma_2) = \text{ppcm}(5, 3) = 15$.

2. Bien entendu, il n'est pas question de calculer à la main σ_1^{2017} et σ_2^{2017} . Comme σ_1 est d'ordre 12 et σ_2 d'ordre 15, nous allons utiliser le fait que $\sigma_1^{12} = \text{id}$ et $\sigma_2^{15} = \text{id}$. Le lemme 3.3 nous sera bien utile.

On a $2017 = 12 \times 168 + 1$. D'après le lemme 3.3, on en déduit $\sigma_1^{2017} = \sigma_1^1 = \sigma_1$. Pour σ_2 , la division euclidienne est $2017 = 15 \times 134 + 7$ d'où $\sigma_2^{2017} = \sigma_2^7$. Il reste à déterminer cette permutation. On utilise la décomposition en cycles plutôt qu'un calcul direct. Posons $s = (1, 5, 4, 2, 6)$ et $s' = (3, 7, 9)$. Le 5-cycle s (resp. 3-cycle s') est d'ordre 5 (resp. 3) donc $s^5 = \text{id}$ (resp. $s'^3 = \text{id}$). Puisque les cycles à supports deux à deux disjoints commutent deux à deux et en utilisant le lemme 3.3, on en déduit

$$\sigma_2^7 = (ss')^7 = s^7(s')^7 = s^2s'.$$

Un calcul direct donne $s^2 = (1, 4, 6, 5, 2)$ d'où $\sigma_2^{2017} = (1, 4, 6, 5, 2)(3, 7, 9)$.

Solution de l'exercice 3.2. 1. Soit p premier. Tout produit de p -cycles à supports deux à deux disjoints est d'ordre $\text{ppcm}(p, \dots, p)$ d'après le cours, c'est-à-dire p , puisque p est premier. Réciproquement soit σ une permutation d'ordre p . Décomposons σ en produit de cycles $c_1 \cdots c_s$ à supports deux à deux disjoints, de longueurs respectives ℓ_1, \dots, ℓ_s . En particulier l'ordre de c_i est ℓ_i . L'ordre de σ est donc $p = \text{ppcm}(\ell_1, \dots, \ell_s)$. Comme p est premier, cela impose $\ell_i \in \{1, p\}$ pour tout i d'où $\ell_i = p$ puisque $\ell_i \geq 2$. Ainsi σ est un produit de p -cycles à supports deux à deux disjoints.

2. D'après la question précédente, comme 2 est premier, les éléments d'ordre 2 de \mathcal{S}_5 sont les transpositions (i, j) et les produits de deux transpositions $(i, j)(k, l)$ à supports disjoints (on ne peut pas considérer les produits

d'au moins 3 transpositions à supports deux à deux disjoints car elles feraient intervenir davantage d'éléments dans leur support que l'ensemble $\{1, \dots, 5\}$). Les premières sont déterminées par leur support $\{i, j\}$ (il y a $\binom{5}{2} = 10$ possibilités). Les seconds sont déterminés par d'une part le choix de $\{i, j, k, l\}$ distincts dans $\{1, \dots, 5\}$ (5 possibilités) et d'autre part leur écriture en produits de deux transpositions (3 possibilités). Il y a donc au total $10 + 5 \times 3 = 25$ éléments d'ordre 2 dans \mathcal{S}_5 .

Solution de l'exercice 3.3. Soit M une matrice de $\text{GL}_n(\mathbb{C})$ d'ordre fini : il existe $k \geq 1$ tel que $M^k = I$ où I désigne la matrice identité de taille n . Le polynôme $P(X) = X^k - 1$ annule donc M . De plus il est scindé sur \mathbb{C} et à racines simples (ses racines sont les racines k -èmes de l'unité). Par un critère classique de réduction des endomorphismes, la matrice M est diagonalisable sur \mathbb{C} .

Par exemple, la matrice M de diagonale (z_1, \dots, z_n) où $z_i \in U_k$ sont des racines k -èmes de l'unité, et tous les coefficients en dehors de la diagonale sont nuls, est inversible et d'ordre fini car $M^k = I$.

Solution de l'exercice 3.4. Cet exercice fait appel à des résultats classiques d'arithmétique concernant le pgcd et le ppcm, ainsi que le lemme de Gauss. On renvoie au chapitre 6 en cas de besoin.

1. D'après le cours, l'ordre de a est le cardinal de $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Or cet ensemble coïncide avec $\{(a^{-1})^n \mid n \in \mathbb{Z}\} = \langle a^{-1} \rangle$. Donc l'ordre de a^{-1} est égal à l'ordre de a .
2. On a $(bab^{-1})^2 = bab^{-1}bab^{-1} = ba^2b^{-1}$. Une récurrence immédiate donne $(bab^{-1})^k = ba^k b^{-1}$ pour tout $k \in \mathbb{Z}$. De plus $a^k = 1_G$ si et seulement si $ba^k b^{-1} = b1_G b^{-1} = 1_G$. Donc $\text{ord}(bab^{-1}) = \text{ord}(a)$.
3. Notons d le pgcd de n et k . On peut écrire $n = dn'$ et $k = dk'$ avec n', k' entiers premiers entre eux (voir chapitre 6 pour des rappels). Il s'agit donc de montrer que a^k est d'ordre n' . Pour cela, montrons que si ℓ est un entier relatif, on a $(a^k)^\ell = 1_G$ si et seulement si $n' \mid \ell$ (voir le théorème 3.6). En utilisant le fait que a est d'ordre n , on a la succession d'équivalences :

$$(a^k)^\ell = 1_G \iff a^{dk'\ell} = 1_G \iff n \mid dk'\ell \iff dn' \mid dk'\ell \iff n' \mid k'\ell.$$

Or n' et k' sont premiers entre eux. Donc par le lemme de Gauss, la dernière affirmation équivaut à $n' \mid \ell$, ce qu'on voulait montrer.

4. Soient G un groupe cyclique d'ordre n et g un générateur de G ; en particulier g est d'ordre n . Tout élément de G est de la forme $x = g^k$ avec $k \in \{0, \dots, n-1\}$. Or x engendre G si et seulement si x est d'ordre n d'après la proposition 3.17. Il s'agit donc de déterminer les k pour lesquels $\text{ord}(g^k) = n$. Par la question précédente, ce sont les $k \in \{0, \dots, n-1\}$ tels que $\text{pgcd}(n, k) = 1$.
5. Supposons $ab = ba$.
 - (a) Notons $\alpha = \text{ord}(a)$, $\beta = \text{ord}(b)$ et $m = \text{ppcm}(\alpha, \beta)$. Alors α et β divisent m donc $a^m = 1_G$ et $b^m = 1_G$. Puisque a et b commutent, il en est de même de toutes puissances de a et de b d'où

$$(ab)^m = a^m b^m = 1_G 1_G = 1_G.$$

On en déduit que l'ordre de ab divise m .

- (b) En prenant $b = a^{-1}$ on a $\alpha = \beta$ (voir la première question de l'exercice) donc $m = \alpha$. Pourtant $ab = 1_G$ est d'ordre 1.
- (c) Supposons α et β premiers entre eux et montrons que $\text{ord}(ab) = \text{ppcm}(\alpha, \beta)$ c'est-à-dire ici $\alpha\beta$. Par une question précédente on sait que $\text{ord}(ab)$ divise $\alpha\beta$. D'après le théorème 3.6, il reste donc à établir

$$\forall k \in \mathbb{Z} : ((ab)^k = 1_G \implies \alpha\beta \mid k).$$

Supposons $(ab)^k = 1_G$ pour un entier $k \in \mathbb{Z}$. Alors $a^k = b^{-k}$ puisque a et b commutent. On en déduit :

$$a^{\beta k} = (a^k)^\beta = b^{-k\beta} = (b^\beta)^{-k} = 1_G^{-k} = 1_G$$

donc α divise βk . Or α et β sont premiers entre eux : le lemme de Gauss entraîne $\alpha \mid k$. Un raisonnement similaire donne $\beta \mid k$. Comme α et β sont premiers entre eux, leur produit $\alpha\beta$ divise k . En conclusion, l'ordre de ab est $\alpha\beta$.

Solution de l'exercice 3.5. On suppose $\ell > 1$, sinon l'exercice est immédiat.

1. Dans la démonstration du théorème 3.6, on a vu que

$$\{k \in \mathbb{Z} \mid x^k = 1_G\} = \text{ord}(x)\mathbb{Z},$$

qui est l'ensemble des multiples de $\text{ord}(x)$. Cela montre que $\text{ord}(x)$ est le plus petit entier ≥ 1 , pour la divisibilité, vérifiant $x^{\text{ord}(x)} = 1_G$. Par conséquent x est d'ordre ℓ si et seulement si

$$x^\ell = 1_G \quad \text{et} \quad \forall d \mid \ell, d \neq \ell : x^d \neq 1_G.$$

2. Soit d un diviseur de ℓ et $d \neq \ell$. On peut donc écrire $\ell = dqk$ où q est un nombre premier divisant ℓ et $k \in \mathbb{N}$. Alors

$$x^d = 1_G \implies (x^d)^k = 1_G \implies x^{\frac{\ell}{q}} = 1_G.$$

Donc il suffit que le critère de la question précédente soit satisfait pour tous les diviseurs de la forme $\frac{\ell}{p}$ où p est premier divisant ℓ .

3. Avec le théorème 3.4, les conditions sont :

$$x \neq 1_G, x^2 \neq 1_G, x^3 \neq 1_G, \dots, x^{11} \neq 1_G, x^{12} = 1_G.$$

Avec la question 1, les conditions sont :

$$\forall d \in \{1, 2, 3, 4, 6\}, x^d \neq 1 \quad \text{et} \quad x^{12} = 1_G.$$

Avec la question 2, les conditions sont :

$$x^4 \neq 1_G, x^6 \neq 1_G, x^{12} = 1_G.$$

Solution de l'exercice 3.6. Posons $G = (\mathbb{Z}/12\mathbb{Z}, +)$. Calculer l'ordre de $\bar{k} \in G$ revient à trouver le plus petit entier $n \geq 1$ tel que $n\bar{k} = \bar{0}$ c'est-à-dire tel que 12 divise nk dans \mathbb{Z} . On peut faire ces calculs à la main mais on peut aussi invoquer la troisième question de l'exercice 3.4, en les traduisant en notation additive : l'élément $a = \bar{1}$ est d'ordre additif 12 donc l'ordre de \bar{k} est $\frac{12}{\text{pgcd}(12, k)}$.

On obtient les résultats suivants :

élément	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$	$\bar{11}$
ordre	1	12	6	4	3	12	2	12	3	4	6	12.

Pour déterminer les sous-groupes de G , on procède comme dans l'exercice 2.10. Commençons par déterminer ceux engendrés par un élément :

$$\begin{aligned} \langle \bar{0} \rangle &= \{\bar{0}\}, \\ \langle \bar{1} \rangle &= G = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle, \\ \langle \bar{2} \rangle &= \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} = \langle \bar{10} \rangle, \\ \langle \bar{3} \rangle &= \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} = \langle \bar{9} \rangle, \\ \langle \bar{4} \rangle &= \{\bar{0}, \bar{4}, \bar{8}\} = \langle \bar{8} \rangle, \\ \langle \bar{6} \rangle &= \{\bar{0}, \bar{6}\}. \end{aligned}$$

Ensuite on montre par des calculs que tout sous-groupe de G engendré par au moins deux éléments distincts fait déjà partie de la liste : par exemple $\langle \bar{2}, \bar{4} \rangle = \langle \bar{2} \rangle$, $\langle \bar{2}, \bar{3} \rangle = G$, et ainsi de suite. La liste des sous-groupes est donc complète.

Remarque. On constate que ces sous-groupes sont tous cycliques. Plus généralement nous verrons dans l'exercice 3.8) que tout sous-groupe d'un groupe cyclique est cyclique.

Solution de l'exercice 3.7. Tout morphisme de groupes $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ vérifie $f(m) = f(m \cdot 1) = mf(1)$ pour tout $m \in \mathbb{Z}$. Réciproquement, fixons $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ alors on vérifie aisément que

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ m &\longmapsto \bar{m}\bar{a} = m\bar{a} \end{aligned}$$

est un morphisme de groupes ($f(m+m') = \overline{(m+m')a} = \overline{ma+m'a} = \overline{m\bar{a}+m'\bar{a}} = f(m)+f(m')$). En conclusion, les morphismes de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$ sont ceux de la forme $m \mapsto m\bar{a}$ avec \bar{a} fixé dans $\mathbb{Z}/n\mathbb{Z}$.

De même, comme $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique engendré par $\bar{1}$, tout morphisme $f : (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ est déterminé par l'image de $\bar{1}$: pour tout $m \in \mathbb{Z}$, on a $f(\bar{m}) = mf(\bar{1})$. Mais si on prend $m = n$, on obtient $f(\bar{m}) = f(\bar{0}) = 0$ car l'élément neutre a pour image l'élément neutre par f . Donc on a $f(1) = 0$: le seul morphisme de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$ est le morphisme nul.

Solution de l'exercice 3.8. Soient G un groupe cyclique, a un générateur de G et H un sous-groupe de G distinct de $\{1_G\}$.

1. Comme $H \neq \{1_G\}$, H contient un élément non trivial. Le groupe G étant engendré par a , cet élément est de la forme a^k avec $k \in \{1, \dots, n-1\}$ où $n = \text{ord}(G)$. Ainsi l'ensemble d'entiers naturels $\{m \geq 1 \mid a^m \in H\}$ est non vide. Il possède un plus petit élément, qu'on note encore m par commodité.
2. Montrons que $H = \langle a^m \rangle$. L'inclusion \supset est immédiate car $a^m \in H$. Réciproquement soit x un élément de H . Comme G est engendré par a , on peut écrire $x = a^k$ avec $k \in \mathbb{Z}$. La division euclidienne de k par m est $k = mq + r$ avec $0 \leq r < m$ d'où $a^k = (a^m)^q a^r$. Comme $a^m \in H$ et $a^k \in H$, on en déduit $a^r = a^k (a^m)^{-q} \in H$. La minimalité de m entraîne que $r = 0$ donc $x = a^{mq} \in \langle a^m \rangle$.

Solution de l'exercice 3.9. Le sous-groupe H est engendré par $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Or on a $C^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $C^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $C^4 = \text{id}$, autrement dit C est d'ordre 4. Ainsi $H = \{\text{id}, C, C^2, C^3\}$. Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans G , les éléments de sa classe à gauche AH modulo H sont :

$$A, \quad AC = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}, \quad AC^2 = -A, \quad AC^3 = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}.$$

De même, si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans G , les éléments de sa classe à droite HA modulo H sont donc

$$A, \quad CA = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix}, \quad C^2A = -A, \quad C^3A = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}.$$

Le sous-groupe K est engendré par $D = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On vérifie aisément par récurrence que pour tout $n \in \mathbb{N}$, la matrice D^n est $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Donc si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans G , les éléments de sa classe à gauche AK modulo K sont les $AD^n = \begin{pmatrix} a & b + na \\ c & d + nc \end{pmatrix}$. De même les éléments de sa classe à droite KA modulo K sont les $D^n A = \begin{pmatrix} a + cn & b + nd \\ c & d \end{pmatrix}$.

Solution de l'exercice 3.10. Soient H et K deux sous-groupes d'un groupe G , d'ordres premiers entre eux. Alors $H \cap K$ est un sous-groupe de H , et aussi de K . Par le théorème de Lagrange, l'ordre de $H \cap K$ divise à la fois l'ordre de H et celui de K . Comme ils sont premiers entre eux, on en déduit que $H \cap K$ est d'ordre 1, c'est-à-dire $H \cap K = \{1_G\}$.

Solution de l'exercice 3.11. 1. Soit G un groupe d'ordre 4. Par le théorème de Lagrange, ses éléments sont d'ordre 1 (c'est l'élément neutre), 2 ou 4. S'il existe un élément d'ordre 4, il engendre G qui est donc cyclique et $G \simeq (\mathbb{Z}/4\mathbb{Z}, +)$ (voir proposition 3.17 et théorème 3.19). Supposons maintenant que tout élément distinct de 1_G est d'ordre 2 : on a donc $G = \{1_G, a, b, c\}$ où les éléments sont deux à deux distincts et a, b, c sont d'ordre 2. On a alors $ab \neq 1_G$ (sinon $a = b^{-1} = b$, ce qui est impossible), $ab \neq a$ (car $b \neq 1_G$) et $ab \neq b$ (même argument). Donc on a $ab = c$ d'où $G = \{1_G, a, b, ab\}$. De même on montre que $ba = ab$ par élimination. La table de Cayley de G est donc :

G	1_G	a	b	ab
1_G	1_G	a	b	ab
a	a	1_G	ab	b
b	b	ab	1_G	a
ab	ab	b	a	1_G

Elle s'identifie à celle de $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$:

$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

Donc G est isomorphe à $V = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

2. Les ordres des éléments du groupe additif V sont :

élément	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
ordre	1	2	2	2

Il n'y a aucun élément d'ordre 4 donc V n'est pas cyclique. En particulier V n'est pas isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$ (les isomorphismes conservent le fait d'être cyclique).

3. Non : 4 divise l'ordre de V mais V ne contient pas d'élément d'ordre 4 par le tableau précédent.

Solution de l'exercice 3.12. Soit G un groupe de cardinal au moins deux et dont les seuls sous-groupes sont $\{1_G\}$ et G (noter que l'énoncé ne suppose pas G fini). Alors G possède un élément x d'ordre > 1 . Par hypothèse, le sous-groupe $\langle x \rangle$, qui ne peut être égal à $\{1_G\}$, est donc G tout entier. Cela montre que G est monogène.

Supposons G infini. D'après le théorème 3.19, G est isomorphe à $(\mathbb{Z}, +)$. Or $(\mathbb{Z}, +)$ possède une infinité de sous-groupes non triviaux : les $m\mathbb{Z}$ avec $m \in \mathbb{N}$. Cela contredit l'hypothèse. Donc G est fini c'est-à-dire finalement cyclique. Notons n son ordre. Il reste à montrer que n est premier.

Rappelons que

$$G = \langle x \rangle = \{1_G, x, \dots, x^{n-1}\}.$$

D'après l'exercice 3.4 l'ordre de x^k est $\frac{n}{\text{pgcd}(n, k)}$. Or le même raisonnement que précédemment montre que tout élément de G distinct de 1_G engendre G , donc est d'ordre n . On en déduit :

$$\forall k \in \{1, \dots, n-1\}, \quad \text{pgcd}(n, k) = 1.$$

Cela implique que n est premier.

Solution de l'exercice 3.13. Soit G un groupe d'ordre 6.

1. Si G est cyclique, il possède au moins un élément g d'ordre 6 par la proposition 3.17. Alors g^2 est d'ordre 3 car $(g^2)^3 = 1_G$ et $g^2 \neq 1_G$. Supposons maintenant G non cyclique. Il n'a donc aucun élément d'ordre 6. Par le théorème de Lagrange tous ses éléments, sauf le neutre, sont d'ordre 2 ou 3. Raisonnons maintenant par l'absurde en supposant qu'ils sont tous d'ordre 2. D'après l'exercice 2.1, le groupe G est abélien. Soient a, b deux éléments de G distincts et d'ordre 2. Alors le sous-groupe engendré par a et b est $\{1_G, a, b, ab\}$ puisque $ab = ba$. Donc G contient un sous-groupe d'ordre 4. Cela contredit le théorème de Lagrange. Ainsi G possède au moins un élément d'ordre 3. On note x un tel élément.
2. Si G est cyclique, alors g^3 est d'ordre 2 car $(g^3)^2 = 1_G$ et $g^3 \neq 1_G$. Supposons maintenant G non cyclique. Il n'a donc aucun élément d'ordre 6. Par le théorème de Lagrange tous ses éléments, sauf le neutre, sont d'ordre 2 ou 3. Raisonnons maintenant par l'absurde en supposant qu'ils sont tous d'ordre 3. Soient a, b deux éléments de G distincts et d'ordre 3. Alors G contient $1_G, a, a^2, b, b^2$ qui sont deux à deux distincts. Pour des raisons de cardinal, on a donc

$$G = \{1_G, a, a^2, b, b^2, c\}$$

avec $c \in G$ distinct des précédents. De plus c est nécessairement d'ordre 3. Mais G doit aussi contenir c^2 . On vérifie par un calcul direct que c^2 est distinct de $1_G, a, a^2, b, b^2, c$, ce qui est impossible. Ainsi G possède au moins un élément d'ordre 2. On note y un tel élément.

3. Le groupe G contient $1_G, x, x^2, y$ qui sont distincts deux à deux. On peut compléter cette liste en considérant xy et x^2y : en effet on vérifie que ces éléments sont distincts des précédents (par exemple $xy = y$ entraînerait $x = 1_G$, etc.) Ainsi $G = \{1_G, x, x^2, y, xy, x^2y\}$. En particulier $G = \langle x, y \rangle$.
4. Supposons G abélien. Comme $xy = yx$ avec x d'ordre 3 et y d'ordre 2 premiers entre eux, la question 5 de l'exercice 3.4 montre que xy est d'ordre 6. Donc G est cyclique et engendré par xy . D'après le théorème de classification des groupes cycliques, G est isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$.
5. Supposons G non abélien. On a $yx \neq 1_G$ (sinon $x = y$, ce qui est impossible), $yx \neq x$ (sinon $y = 1_G$, ce qui est impossible), $yx \neq y$ et $yx \neq x^2$ (pour des raisons similaires). On en déduit que yx vaut xy ou x^2y . Mais comme $G = \langle x, y \rangle$ est non abélien, on a nécessairement $yx = x^2y$. On peut

compléter alors la table de Cayley de G :

G	1_G	x	x^2	y	xy	x^2y
1_G	1_G	x	x^2	y	xy	x^2y
x	x	x^2	1_G	xy	x^2y	y
x^2	x^2	1_G	x	x^2y	y	xy
y	y	x^2y	xy	1_G	x^2	x
xy	xy	y	x^2y	x	1_G	x^2
x^2y	x^2y	xy	y	x^2	x	1_G

C'est la table de Cayley du groupe symétrique \mathcal{S}_3 , en identifiant x au 3-cycle $(1, 2, 3)$ et y à la transposition $(1, 2)$. Donc $G \simeq \mathcal{S}_3$.

6. Les groupes $(\mathbb{Z}/6\mathbb{Z}, +)$ et \mathcal{S}_3 ne sont pas isomorphes car le premier est abélien et le second ne l'est pas (les isomorphismes conservent le fait d'être abélien).

Remarque. Dans l'exercice 5.13, nous montrerons plus généralement (et avec plus de facilité, du fait des outils plus puissants utilisés) le théorème de classification suivant : tout groupe d'ordre $2p$ avec p premier > 2 est isomorphe à $(\mathbb{Z}/2p\mathbb{Z}, +)$ ou au groupe diédral D_p .

Solution de l'exercice 3.14. Soit m et n deux entiers non nuls et premiers entre eux. Posons dans $(\mathbb{Z}/mn\mathbb{Z}, +)$:

$$a = (m \bmod mn) \quad \text{et} \quad b = (n \bmod mn)$$

la classe de a , resp. b , modulo mn . Alors il est clair que a est d'ordre n et b est d'ordre m dans $(\mathbb{Z}/mn\mathbb{Z}, +)$. Soient $H_1 = \langle a \rangle$ et $H_2 = \langle b \rangle$, sous-groupes de $\mathbb{Z}/mn\mathbb{Z}$.

- Le groupe H_1 est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ puisqu'ils sont tous les deux cycliques d'ordre n . De même H_2 est isomorphe à $(\mathbb{Z}/m\mathbb{Z}, +)$.
- Comme m et n sont premiers entre eux, on a $H_1 \cap H_2 = \{0\}$ d'après l'exercice 3.10.
- Pour tous $h_1 \in H_1$ et $h_2 \in H_2$ on a $h_1 + h_2 = h_2 + h_1$ car $(\mathbb{Z}/mn\mathbb{Z}, +)$ est abélien.
- Montrons enfin que $\mathbb{Z}/mn\mathbb{Z} = H_1 + H_2 = \{h_1 + h_2 \mid h_1 \in H_1, h_2 \in H_2\}$. Considérons l'application (qui n'est pas un morphisme de groupes !)

$$\begin{aligned} H_1 \times H_2 &\longrightarrow H_1 + H_2 \\ (x, y) &\longmapsto x + y. \end{aligned}$$

Par construction, elle est surjective. Elle est injective : en effet si $x + y = x' + y'$ avec x, x' dans H_1 et y, y' dans H_2 alors $-x' + x = y' - y \in H_1 \cap H_2 = \{0\}$ d'où $x' = x$ et $y' = y$ par ce qui précède. Elle est donc bijective. En particulier $H_1 + H_2$ est de cardinal nm . Comme c'est un sous-ensemble de $\mathbb{Z}/mn\mathbb{Z}$, qui est de même cardinal, on en déduit $\mathbb{Z}/mn\mathbb{Z} = H_1 + H_2$.

On peut donc appliquer le critère du théorème 2.44 : le groupe $(\mathbb{Z}/mn\mathbb{Z}, +)$ est isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Remarque. Nous revisiterons cet énoncé au chapitre 6 dans le cadre du théorème chinois, en prenant en compte une loi supplémentaire de multiplication sur ces ensembles.

Corrigé des exercices du chapitre 4

Solution de l'exercice 4.1. Soit $GL_n^+(\mathbb{R})$ l'ensemble des matrices de $GL_n(\mathbb{R})$ de déterminant strictement positif. Il est contenu dans $GL_n(\mathbb{R})$ et contient la matrice identité. De plus pour toutes matrices M, N dans $GL_n^+(\mathbb{R})$ on a

$$\det(MN^{-1}) = \det(M) \det(N^{-1}) = \det(M) \det(N)^{-1}$$

qui est strictement positif comme produit de deux réels de \mathbb{R}_+^* . Donc MN^{-1} appartient à $GL_n^+(\mathbb{R})$. Cela prouve que $GL_n^+(\mathbb{R})$ est un sous-groupe de $(GL_n(\mathbb{R}), \cdot)$.

Montrons qu'il est normal dans $GL_n(\mathbb{R})$. D'après la proposition 4.1, il s'agit de montrer que toute matrice $M \in GL_n(\mathbb{R})$ satisfait $MGL_n^+(\mathbb{R})M^{-1} \subset GL_n^+(\mathbb{R})$. Or si $N \in GL_n^+(\mathbb{R})$, la matrice MNM^{-1} est de déterminant $\det(M) \det(N) \det(M)^{-1} = \det(N) > 0$ donc $MNM^{-1} \in GL_n^+(\mathbb{R})$. Cela démontre l'inclusion souhaitée, et le fait que $GL_n^+(\mathbb{R})$ est normal dans $GL_n(\mathbb{R})$.

Solution de l'exercice 4.2. 1. Comme $(\mathbb{R}, +)$ est un groupe abélien, tous ses sous-groupes sont normaux. C'est donc le cas de $(\mathbb{Z}, +)$.

2. Soient x, y dans \mathbb{R} . Alors x et y sont équivalents modulo \mathbb{Z} si et seulement si $x - y \in \mathbb{Z}$ c'est-à-dire si et seulement si x et y ont même partie fractionnaire (rappel : pour $x \in \mathbb{R}$, la partie fractionnaire $\{x\}$ est définie comme $\{x\} = x - [x]$ où $[x]$ désigne la partie entière de x ; elle vérifie $0 \leq \{x\} < 1$). Donc on peut prendre comme système de représentants de \mathbb{R}/\mathbb{Z} l'intervalle $[0, 1[$.

Solution de l'exercice 4.3. Soient G un groupe, H et K deux sous-groupes de G avec H normal dans G . Montrons que KH est un sous-groupe de G . Il est contenu dans G et contient $1_G = 1_G 1_G$. De plus, pour tous kh et $k'h'$ dans KH , avec k, k' dans K et h, h' dans H , on écrit

$$(kh)(k'h')^{-1} = kh h'^{-1} k'^{-1} = (k k'^{-1})(k' h k'^{-1})(k' h'^{-1} k'^{-1}).$$

De plus $k k'^{-1} \in K$, $k' h k'^{-1} \in H$ et $k' h'^{-1} k'^{-1} \in H$ car H est normal dans G . Donc $(kh)(k'h')^{-1}$ appartient à KH . Cela montre que KH est un sous-groupe de G .

Solution de l'exercice 4.4. La démarche usuelle pour construire un isomorphisme de G/H dans un groupe G' est la suivante :

- on construit un morphisme de groupes $f : G \rightarrow G'$, approprié à la situation, surjectif et de noyau H (il y a souvent une manière naturelle de le construire);
- on passe f au quotient par H (théorème d'isomorphisme, corollaire 4.14).

1. Considérons l'application partie imaginaire :

$$\begin{aligned} f : (\mathbb{C}, +) &\longrightarrow (\mathbb{R}, +) \\ x + iy &\longmapsto y. \end{aligned}$$

C'est un morphisme de groupes : pour tous $x + iy$ et $x' + iy'$ dans \mathbb{C} avec x, y, x', y' réels, on a

$$f((x+iy)+(x'+iy')) = f(x+x'+i(y+y')) = y+y' = f(x+iy)+f(x'+iy').$$

De plus f est surjectif car tout élément $a \in \mathbb{R}$ s'écrit $f(ai)$ avec $ai \in \mathbb{C}$. Enfin le noyau de f est l'ensemble des nombres complexes $x + iy$ tels que $y = 0$ c'est-à-dire $\text{Ker } f = \mathbb{R}$. On en déduit par passage au quotient un isomorphisme $\mathbb{C}/\text{Ker } f \simeq \text{Im } f$ c'est-à-dire $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$.

2. Dans cette question, il n'y a pas de groupe quotient : il est inutile d'invoquer le théorème d'isomorphisme. Considérons l'application exponentielle réelle :

$$\begin{aligned} \exp : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}_+^*, \cdot) \\ x &\longmapsto \exp(x), \end{aligned}$$

bien définie car à valeurs dans \mathbb{R}_+^* . C'est un morphisme de groupes : pour tous x, y réels on a $\exp(x+y) = \exp(x)\exp(y)$. Elle est surjective : en effet pour tout $a \in \mathbb{R}_+^*$, on peut considérer le nombre réel $\ln(a)$ et alors $a = \exp(\ln(a))$. Enfin elle est injective car la seule solution réelle de l'équation $\exp(x) = 1$ est $x = 0$. Ainsi \exp est un isomorphisme.

3. Considérons l'application exponentielle complexe :

$$\begin{aligned} g : (\mathbb{R}, +) &\longrightarrow (U, \cdot) \\ x &\longmapsto \exp(ix). \end{aligned}$$

Elle est bien à valeurs dans U , le groupe des nombres complexes de module 1. C'est un morphisme de groupes car pour tous x, y réels on a $g(x+y) = \exp(i(x+y)) = \exp(ix+iy) = \exp(ix)\exp(iy) = g(x)g(y)$. De plus g est surjectif car tout nombre complexe de module 1 est de la forme $\exp(i\theta)$ avec $\theta \in \mathbb{R}$. Enfin le noyau de g est $\text{Ker } g = \{x \in \mathbb{R} \mid \exp(ix) = 1\} = 2\pi\mathbb{Z}$. Par passage au quotient, on en déduit l'isomorphisme $(\mathbb{R}/2\pi\mathbb{Z}, +) \simeq (U, \cdot)$.

4. Tout nombre complexe non nul z s'écrit $z = ru$ avec (r, u) unique dans $\mathbb{R}_+^* \times U$. On a donc une bijection

$$\begin{aligned} h : \mathbb{C}^* &\longrightarrow \mathbb{R}_+^* \times U \\ z &\longmapsto (r, u). \end{aligned}$$

De plus h est un morphisme de groupes multiplicatifs : pour tous z, z' dans \mathbb{C} d'écritures polaires $z = ru$ et $z' = r'u'$ on a $h(zz') = h(rur'u') =$

$h(rr'uu') = (rr', uu') = (r, u)(r', u') = h(z)h(z')$. Donc h est un isomorphisme de groupes $\mathbb{C}^* \simeq \mathbb{R}_+^* \times U$. Par la question précédente, on en déduit $(\mathbb{C}^*, \cdot) \simeq (\mathbb{R}_+^*, \cdot) \times (\mathbb{R}/2\pi\mathbb{Z}, +)$.

Solution de l'exercice 4.5. 1. Rappelons que le groupe alterné \mathcal{A}_n est d'ordre $n!/2$. Donc \mathcal{A}_3 est d'ordre 3. Comme 3 est premier, l'argument (classique et à connaître) de l'exemple 4.18 assure que ce groupe est simple.

2. Énumérons les 12 éléments de \mathcal{A}_4 en écrivant leurs décompositions en cycles à supports deux à deux disjoints (s'aider au besoin de l'exercice 1.2) :

$$\begin{aligned} & \text{id,} \\ & (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), \\ & (1, 2, 3), (1, 3, 2), (2, 3, 4), (2, 4, 3), (3, 4, 1), (3, 1, 4), (4, 1, 2), (4, 2, 1). \end{aligned}$$

Les doubles transpositions (c'est-à-dire les produits de deux transpositions à supports disjoints) sont d'ordre 2 : on le vérifie à la main ou en utilisant la proposition 3.8. Les 3-cycles sont d'ordre 3. Considérons le sous-groupe H engendré par la partie $\{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$. Un calcul montre que

$$H = \{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

Prouvons que H est normal dans \mathcal{A}_4 . Il s'agit de montrer que, pour tout $\sigma \in \mathcal{A}_4$, on a $\sigma H \sigma^{-1} \subset H$. D'après la liste des éléments de \mathcal{A}_4 , distinguons deux cas :

- si $\sigma \in H$ alors il est clair que $\sigma H \sigma^{-1} \subset H$;
- sinon, σ est un 3-cycle ; mais d'après le deuxième point de la proposition 1.15, on peut écrire pour toute double transposition $(a, b)(c, d)$:

$$\sigma(a, b)(c, d)\sigma^{-1} = \sigma(a, b)\sigma^{-1}\sigma(c, d)\sigma^{-1} = (\sigma(a), \sigma(b))(\sigma(c), \sigma(d)).$$

avec $(\sigma(a), \sigma(b))$ et $(\sigma(c), \sigma(d))$ transpositions à supports disjoints. Donc $\sigma(a, b)(c, d)\sigma^{-1}$ est encore une double transposition (on aurait pu aussi le démontrer en utilisant le résultat de l'exercice 1.8). Cela entraîne que $\sigma(a, b)(c, d)\sigma^{-1}$ appartient à H .

On a ainsi l'inclusion voulue. Le sous-groupe H est normal dans G mais non trivial. Le groupe \mathcal{A}_4 n'est donc pas simple.

Solution de l'exercice 4.6. Soit G un groupe abélien d'ordre 8.

1. D'après le théorème de Lagrange, les éléments de G peuvent être d'ordre 1 (le neutre), 2, 4 ou 8.
2. On suppose qu'il existe un élément d'ordre 8 dans G . Le sous-groupe engendré par cet élément est d'ordre 8. Par égalité des cardinaux, on en déduit que cet élément engendre G (voir aussi la proposition 3.17). Par le théorème de classification des groupes cycliques, on a donc $G \simeq (\mathbb{Z}/8\mathbb{Z}, +)$.
3. On suppose qu'il n'existe pas d'élément d'ordre 8 dans G mais qu'il existe un élément a d'ordre 4. Soit $b \in G - \langle a \rangle$.

- (a) On a $G = \{1_G, a, a^2, a^3, b, ab, a^2b, a^3b\}$: en effet comme a est d'ordre 4 et $b \notin \langle a \rangle$, on peut vérifier que tous ces éléments sont deux à deux distincts ; étant donné qu'il y en a 8, ils forment G tout entier. Cela montre que $G = \langle a, b \rangle$. Par hypothèse, l'ordre de b est 2 ou 4. S'il est d'ordre 2 alors $b^2 = 1_G$. Supposons b d'ordre 4. On a $b^2 \neq ab$, $b^2 \neq a^2b$ et $b^2 \neq a^3b$ (sinon b serait dans le sous-groupe engendré par a , ce qui a été exclu). Vu la liste des éléments de G , on en déduit $b^2 \in \{a, a^2, a^3\}$. Or b étant d'ordre 4, b^2 est d'ordre 2 (on le démontre à la main ou on utilise l'exercice 3.4). De plus a étant d'ordre 4, l'élément $a^3 = a^{-1}$ est aussi d'ordre 4 (même référence). On en déduit $b^2 = a^2$.
- (b) Si $b^2 = 1_G$ alors b est d'ordre 2 ; en posant $c = b$ alors c convient. Si $b^2 = a^2$, on a $abab = a^2b^2 = a^4 = 1_G$ car G est abélien. On vérifie aussi que ab n'appartient pas à $\langle a \rangle$. On pose alors $c = ab$ et c convient.
- (c) Comme a (resp. c) est d'ordre 4 (resp. 2), le sous-groupe $\langle a \rangle$ (resp. $\langle c \rangle$) est cyclique d'ordre 4 (resp. 2) donc isomorphe au groupe additif $\mathbb{Z}/4\mathbb{Z}$ (resp. $\mathbb{Z}/2\mathbb{Z}$). Montrons que $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ en appliquant le critère du produit direct (théorème 4.23 ou 2.44).
- Les sous-groupes $\langle a \rangle$ et $\langle c \rangle$ sont normaux dans G car G est abélien.
 - On a $\langle a \rangle \cap \langle c \rangle = \{1_G\}$ car c n'appartient pas à $\langle a \rangle$.
 - Comme $c \notin \langle a \rangle$, le même raisonnement qu'à la question 3a montre que $G = \langle a, c \rangle$ et même que $G = \langle a \rangle \langle c \rangle$.
- Par le critère, on conclut que $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
4. On suppose que tous les éléments de G distincts de 1_G sont d'ordre 2. Soit $a \neq 1_G$ dans G . Par cardinalité, il existe b dans G qui est distinct de 1_G et de a . Les éléments $1_G, a, b, ab$ sont deux à deux distincts. Par cardinalité encore, il existe un élément c dans $G - \{1_G, a, b, ab\}$. On en déduit

$$G = \{1_G, a, b, ab, c, ac, bc, abc\},$$

les éléments de cet ensemble étant deux à deux distincts et au nombre de 8. Le groupe G est abélien et les éléments a, b, c sont d'ordre 2. Cela permet d'écrire sa table de Cayley (par abélianité, on ne remplit que la moitié supérieure du tableau) :

G	1_G	a	b	ab	c	ac	bc	abc
1_G	1_G	a	b	ab	c	ac	bc	abc
a		1_G	ab	b	ac	c	abc	bc
b			1_G	a	bc	abc	c	ac
ab				1_G	abc	bc	ac	c
c					1_G	a	b	ab
ac						1_G	ab	b
bc							1_G	a
abc								1_G .

On constate que c'est la table de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Donc ces deux groupes sont isomorphes. On pouvait aussi considérer l'application

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\longrightarrow G \\ (\bar{i}, \bar{j}, \bar{k}) &\longmapsto a^i b^j c^k \end{aligned}$$

et vérifier que c'est un isomorphisme de groupes.

Solution de l'exercice 4.7. Soit D_4 un groupe diédral à 8 éléments, de générateurs r et s avec r d'ordre 4, s d'ordre 2 et $rsrs = 1$. On a donc

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}.$$

On pose $K = \langle s \rangle \subset H = \langle s, r^2 \rangle$.

Le sous-groupe $K = \{1, s\}$ est d'ordre 2. Déterminons les éléments de H . L'élément r^2 est d'ordre 2. Comme on a $sr^k = r^{-k}s$ pour tout $k \in \mathbb{Z}$, on peut montrer que r^2s est d'ordre 2 et $r^2s = sr^2$ d'où

$$H = \langle s, r^2 \rangle = \{1, s, r^2, r^2s\}.$$

Ainsi H est d'ordre 4. En particulier l'indice de K dans H est $\text{ord}(H)/\text{ord}(K) = 2$. D'après la proposition 4.5, K est normal dans H . De même l'indice de H dans D_4 est $\text{ord}(D_4)/\text{ord}(H) = 8/4 = 2$ donc H est normal dans D_4 .

Montrons que K n'est pas normal dans D_4 . Pour cela, considérons l'élément rsr^{-1} ; il vaut

$$rsr^{-1} = rsr^3 = rr^{-3}s = r^{-2}s = r^2s.$$

Cet élément n'appartient pas à K car sinon on en déduirait $r^2 \in \langle s \rangle = \{1, s\}$, ce qui est impossible. Cela prouve que K n'est pas normal dans D_4 .

Solution de l'exercice 4.8. Soit H un sous-groupe normal d'un groupe G . Notons $\pi : G \rightarrow G/H$ la surjection canonique.

1. Soit φ un automorphisme de G vérifiant $\varphi(H) = H$. On construit le morphisme cherché Φ en appliquant le théorème de factorisation (théorème 4.12) à un morphisme de groupes bien choisi, qui, d'après le contexte, doit aller de G dans G/H . Posons $f = \pi \circ \varphi$. C'est le morphisme de groupes $G \rightarrow G/H$ qui envoie x sur $\varphi(x)H$. Il est surjectif car π et φ le sont. De plus son noyau est l'ensemble des $x \in G$ tels que $\varphi(x)H = H$ c'est-à-dire $\varphi(x) \in H$. Comme $\varphi(H) = H$ et φ est bijectif, cela équivaut à $x \in H$ d'où finalement $\text{Ker } f = H$. En passant f au quotient, on obtient un isomorphisme de groupes $\Phi : G/H \rightarrow G/H$ c'est-à-dire un automorphisme de G/H , qui satisfait $\Phi \circ \pi = f = \pi \circ \varphi$. De plus ce morphisme est unique d'après le théorème de factorisation.
2. On note $\text{Fix}(H)$ le sous-ensemble des automorphismes $\varphi \in \text{Aut}(G)$ vérifiant $\varphi(H) = H$. Il contient l'automorphisme identité. Si φ, ψ sont deux automorphismes de G vérifiant $\varphi(H) = H$ et $\psi(H) = H$ alors on a $(\varphi \circ \psi^{-1})(H) = \varphi(H) = H$ d'où $\varphi \circ \psi^{-1} \in \text{Fix}(H)$. Ainsi $\text{Fix}(H)$ est un sous-groupe de $(\text{Aut}(G), \circ)$.
3. Inspirés par la première question, définissons une application $u : \text{Fix}(H) \rightarrow \text{Aut}(G/H)$ en associant à $\varphi \in \text{Fix}(H)$ l'unique morphisme $\Phi : G/H \rightarrow G/H$ tel que $\Phi \circ \pi = \pi \circ \varphi$. Nous devons maintenant montrer que u est un morphisme de groupes. Soit φ, φ' deux éléments de $\text{Fix}(H)$. On veut montrer que

$$u(\varphi) \circ u(\varphi') = u(\varphi \circ \varphi').$$

Par définition, $u(\varphi \circ \varphi')$ est l'unique morphisme tel que $u(\varphi \circ \varphi') \circ \pi = \pi \circ \varphi \circ \varphi'$. Par définition de u , on sait que $u(\varphi) \circ \pi = \pi \circ \varphi$ et $u(\varphi') \circ \pi = \pi \circ \varphi'$. On a alors $u(\varphi) \circ u(\varphi') \circ \pi = u(\varphi) \circ \pi \circ \varphi' = \pi \circ \varphi \circ \varphi'$. On a donc $u(\varphi \circ \varphi') = u(\varphi) \circ u(\varphi')$, ce qu'on voulait montrer.

Solution de l'exercice 4.9. Soient G un groupe, H un sous-groupe normal de G et K un sous-groupe de G .

1. Comme $K \triangleleft G$, on munit l'ensemble G/K de sa structure de groupe quotient (théorème 4.8). Considérons le morphisme de groupes

$$\begin{aligned} f : G &\longrightarrow G/K \\ x &\longmapsto xK. \end{aligned}$$

Son noyau est K , qui contient H , donc d'après le théorème 4.12, on peut factoriser f en le morphisme de groupes

$$\begin{aligned} \bar{f} : G/H &\longrightarrow G/K \\ xH &\longmapsto xK. \end{aligned}$$

Comme f est surjective, \bar{f} l'est aussi d'après le corollaire 4.14. De plus le noyau de \bar{f} est

$$\text{Ker } \bar{f} = \{xH \in G/H \mid xK = K\} = \{xH \in G/H \mid x \in K\} = \pi(K) = K/H.$$

En utilisant le théorème d'isomorphisme (corollaire 4.14), on conclut que \bar{f} se factorise en un isomorphisme de groupes $(G/H)/(K/H) \simeq G/K$.

2. (a) D'après l'exercice 4.3 et compte tenu des hypothèses, KH est un sous-groupe de G .

Montrons que $H \cap K$ est un sous-groupe normal de K . C'est déjà un sous-groupe de G , donc un sous-groupe de K . Soit $x \in K$ et montrons que $x(H \cap K)x^{-1} \subset H \cap K$. Il est immédiat que $x(H \cap K)x^{-1} \subset K$. De plus on a $x(H \cap K)x^{-1} \subset xHx^{-1} = H$ car H est normal dans G . On en déduit $x(H \cap K)x^{-1} \subset H \cap K$ d'où la normalité.

Montrons que H est un sous-groupe normal de KH . Il est clair que H est un sous-groupe de KH : en effet, il est contenu dans KH (écrire $h = 1_G h$ pour tout $h \in H$) et c'est un groupe. Il reste à montrer que pour tout $kh \in KH$ on a $khH(kh)^{-1} \subset H$. Pour tout $x \in H$ on écrit

$$kx(kh)^{-1} = kxh^{-1}k^{-1}.$$

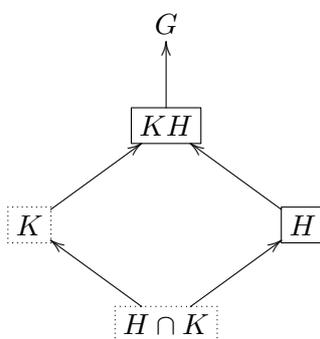
Or $hkh^{-1} \in H$ car H est normal dans G . On en déduit $k(hkh^{-1})k^{-1} \in H$, ce qu'il fallait montrer.

- (b) Comme dans la question 1, il s'agit de construire l'isomorphisme cherché en factorisant un morphisme de groupes approprié. Considérons le morphisme de groupes

$$\begin{aligned} f : K &\longrightarrow KH/H \\ k &\longmapsto kH \end{aligned}$$

obtenu en composant l'inclusion $K \rightarrow KH$, $k \mapsto k = k1_G$ avec la surjection canonique $KH \rightarrow KH/H$. Le morphisme f est surjectif : en effet tout élément de KH/H est de la forme khH avec $k \in K$ et $h \in H$; mais comme $h \in H$ on a $khH = k(hH) = kH$ donc $khH = f(k)$. Par ailleurs le noyau de f est l'ensemble des $k \in K$ tels que $kH = H$ (l'élément neutre de KH/H), c'est-à-dire l'ensemble des éléments de K qui appartiennent à H , autrement dit $\text{Ker } f = K \cap H$. Par le théorème d'isomorphisme du cours, on en déduit par factorisation de f un isomorphisme de groupes entre $K/\text{Ker } f$ et $\text{Im } f$ c'est-à-dire entre $K/(K \cap H)$ et KH/K .

Remarque. Voici une manière de représenter graphiquement la conclusion de l'isomorphisme $K/(H \cap K) \simeq KH/H$:



où les flèches \rightarrow représentent des inclusions.

Solution de l'exercice 4.10. Soient $\Gamma = \{z \in \mathbb{C}^* \mid \exists n \in \mathbb{N}, n \geq 1, z^n = 1\}$ et U le groupe multiplicatif des nombres complexes de module 1.

1. L'ensemble Γ est contenu dans U : en effet si $z^n = 1$ alors $1 = |z^n| = |z|^n$, ce qui entraîne $|z| = 1$ d'où $z \in U$. De plus Γ est non vide puisqu'il contient 1. Soient z et z' dans Γ . Il existe n et n' dans $\mathbb{N} - \{0\}$ tels que $z^n = 1$ et $(z')^{n'} = 1$. Alors on a $(z')^{-n'} = 1$ d'où $(zz'^{-1})^{nn'} = z^{nn'}(z')^{-nn'} = (z^n)^{n'}(z')^{-n} = 1 \cdot 1 = 1$, ce qui prouve que zz'^{-1} appartient à Γ . Ainsi Γ est un sous-groupe de (U, \cdot) .
2. Soit $z \in \Gamma$. Comme z est un nombre complexe de module 1, il s'écrit $z = e^{i\theta}$ avec $\theta \in \mathbb{R}$. De plus il existe $n \in \mathbb{N}, n \geq 1$, tel que $z^n = 1$ c'est-à-dire $e^{i\theta n} = 1$. On en déduit qu'il existe $k \in \mathbb{Z}$ tel que $\theta n = 2k\pi$ donc $\theta = 2k\pi/n$, ce qu'il fallait démontrer.
3. Considérons l'application

$$f: \mathbb{Q} \longrightarrow \Gamma$$

$$\frac{k}{n} \longmapsto e^{\frac{2i\pi k}{n}}$$

c'est-à-dire définie par $f(\alpha) = e^{2i\pi\alpha}$. Pour tous α, β dans \mathbb{Q} , on a

$$f(\alpha + \beta) = e^{2i\pi(\alpha+\beta)} = e^{2i\pi\alpha} e^{2i\pi\beta} = f(\alpha)f(\beta).$$

Donc f est un morphisme de groupes de $(\mathbb{Q}, +)$ dans (Γ, \cdot) . D'après la question précédente, f est surjectif. Déterminons $\text{Ker } f$: c'est l'ensemble

de $\alpha \in \mathbb{Q}$ tels que $e^{2i\pi\alpha} = 1$ c'est-à-dire tels que $2\pi\alpha$ est de la forme $2\pi k$ avec $k \in \mathbb{Z}$. Autrement dit $\text{Ker } f$ est contenu dans \mathbb{Z} , et même égal à \mathbb{Z} , l'autre inclusion étant immédiate. Par le théorème d'isomorphisme du cours (corollaire 4.14) appliqué à f , on conclut que $(\mathbb{Q}/\mathbb{Z}, +) \simeq (\Gamma, \cdot)$.

4. Considérons l'application suivante, inspirée de f ,

$$\begin{aligned} \mathbb{R} &\longrightarrow U \\ \alpha &\longmapsto e^{2i\pi\alpha}. \end{aligned}$$

On démontre que c'est un morphisme de groupes de $(\mathbb{R}, +)$ dans (U, \cdot) (vérification laissée au lecteur). Par factorisation (comme dans la question 3 de l'exercice 4.4), on obtient un isomorphisme de groupes $(\mathbb{R}/\mathbb{Z}, +) \simeq (U, \cdot)$.

5. Les isomorphismes $(\mathbb{Q}/\mathbb{Z}, +) \simeq (\Gamma, \cdot)$ et $(\mathbb{R}/\mathbb{Z}, +) \simeq (U, \cdot)$ que nous avons construits sont tous les deux induits par le même morphisme $\alpha \mapsto e^{2i\pi\alpha}$. En particulier, la restriction de l'isomorphisme $(\mathbb{R}/\mathbb{Z}, +) \simeq (U, \cdot)$ au sous-groupe \mathbb{Q}/\mathbb{Z} de \mathbb{R}/\mathbb{Z} donne précisément l'isomorphisme $(\mathbb{Q}/\mathbb{Z}, +) \simeq (\Gamma, \cdot)$ construit à la question 3. On en déduit :

$$U/\Gamma \simeq (\mathbb{R}/\mathbb{Z})/(\mathbb{Q}/\mathbb{Z})$$

Or d'après le deuxième théorème d'isomorphisme (question 2b de l'exercice 4.9), on a aussi $(\mathbb{R}/\mathbb{Z})/(\mathbb{Q}/\mathbb{Z}) \simeq (\mathbb{R}/\mathbb{Q}, +)$. En conclusion, on a un isomorphisme de groupes $U/\Gamma \simeq (\mathbb{R}/\mathbb{Q}, +)$.

Solution de l'exercice 4.11. Posons $a = (1, 2, 3)$ et $b = (1, 2)$ dans le groupe symétrique \mathcal{S}_3 . Le 3-cycle a est d'ordre 3 et la transposition b est d'ordre 2. De plus un calcul donne

$$baba = (1, 2)(1, 2, 3)(1, 2)(1, 2, 3) = \text{id}.$$

Enfin montrons que $\mathcal{S}_3 = \langle a, b \rangle$. Le sous-groupe $\langle a, b \rangle$ contient les éléments distincts suivants :

$$\begin{aligned} &\text{id}, \\ &a = (1, 2, 3), \\ &a^2 = (1, 3, 2), \\ &b = (1, 2), \\ &ab = (1, 3), \\ &a^2b = (2, 3). \end{aligned}$$

Comme ce sont tous les éléments de \mathcal{S}_3 , on conclut que $\mathcal{S}_3 = \langle a, b \rangle$. D'après la proposition 4.28 et la définition 4.29, \mathcal{S}_3 est un groupe diédral d'ordre 6.

Remarque. En général, le groupe symétrique \mathcal{S}_n n'est pas diédral.

Solution de l'exercice 4.12. Soit G un groupe non abélien d'ordre 8.

1. Par le théorème de Lagrange, les éléments de G distincts de 1_G sont d'ordre 2, 4 ou 8. S'il existe un élément d'ordre 8 alors G est cyclique (voir l'argument de la question 2 de l'exercice 4.6) donc abélien, ce qui est impossible. Si tous les éléments sont d'ordre 2 alors G est abélien (voir l'exercice 2.1), ce qui est impossible. Donc il existe un élément a d'ordre 4 dans G .
2. Comme a est d'ordre 4, le sous-groupe $\langle a \rangle$ est d'indice 2 dans G , donc normal dans G d'après le cours.
3. Soit $b \in G - \{1_G, a, a^2, a^3\}$. Il est facile de voir que

$$G = \{1_G, a, a^2, a^3, b, ab, a^2b, a^3b\},$$

ces éléments étant deux à deux distincts et au nombre de 8. Ainsi on a $G = \langle a, b \rangle$.

4. L'élément b n'est pas d'ordre 8 (sinon G serait abélien car cyclique). Donc par le théorème de Lagrange, b est d'ordre 2 ou 4. On en déduit que b^2 est d'ordre 1 ou 2. Si b^2 est d'ordre 1 alors $b^2 = 1_G$. Supposons maintenant b^2 d'ordre 2. On ne peut pas avoir $b^2 = a^j b$ (car b n'est pas dans le sous-groupe engendré par a). De plus comme a est d'ordre 4, l'élément $a^3 = a^{-1}$ est d'ordre 4. Donc, en regardant la liste des éléments de G , on montre que b^2 vaut a^2 .
5. De manière générale, l'ordre de bab^{-1} est égal à celui de a (voir l'exercice 3.4). Donc ici bab^{-1} est d'ordre 4. De plus ba n'est pas de la forme a^j car $b \notin \langle a \rangle$. De la liste des éléments de G , on déduit $ba \in \{b, ab, a^2b, a^3b\}$. Le premier cas est exclu (car $a \neq 1_G$), le deuxième entraînerait que G est abélien, ce qui est impossible. Pour le troisième, si $ba = a^2b$ alors $bab^{-1} = a^2$ est d'ordre 2, ce qui est impossible car on a montré qu'il est d'ordre 4. Il ne reste que le dernier cas : $ba = a^3b$.
6. Supposons être dans le cas $b^2 = 1_G$. Alors b est d'ordre 2. Par ce qui précède, G est engendré par deux éléments a et b avec a d'ordre 4, b d'ordre 2 et $baba = a^3bba = a^4 = 1_G$. D'après la proposition 4.28, G est un groupe diédral D_4 . Supposons maintenant que $b^2 = a^2$. Alors G est engendré par deux éléments a et b avec a d'ordre 4, $b^2 = a^2$, $ba = a^3b = a^{-1}b$. Il est isomorphe au groupe H de l'énoncé.

Montrons que D_4 et H ne sont pas isomorphes. On a

$$H = \{1_H, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}.$$

En utilisant les propriétés de α et β , on peut montrer que H a un seul élément d'ordre 2, α^2 . Or on peut aussi voir que D_4 possède 5 éléments d'ordre 2. Donc D_4 et H ne sont pas isomorphes (les isomorphismes de groupes conservent l'ordre de chaque élément).

Solution de l'exercice 4.13. Soit H le sous-groupe de $(\mathrm{GL}_n(K), \cdot)$ formé des

matrices

$$A_\lambda = \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

avec $\lambda \in K^*$ et les coefficients en-dehors de la diagonale tous nuls. Noter que A_λ est de déterminant λ et que $A_{\lambda\lambda'} = A_\lambda A_{\lambda'}$. On sait que $\mathrm{SL}_n(K)$ est normal dans $\mathrm{GL}_n(K)$. Par ailleurs il est clair que $\mathrm{SL}_n(K) \cap H = \{I\}$. Montrons enfin que $\mathrm{GL}_n(K) = \mathrm{SL}_n(K)H$. Pour cela, il suffit d'écrire, pour toute matrice M dans $\mathrm{GL}_n(K)$,

$$M = (MA_{\frac{1}{\det M}})A_{\det M}$$

car $A_{\frac{1}{\det M}}A_{\det M}$ est la matrice identité. Or la matrice $MA_{\frac{1}{\det M}}$ est de déterminant $\det M \cdot \frac{1}{\det M} = 1$ donc elle appartient à $\mathrm{SL}_n(K)$. On a donc montré que M appartient à $\mathrm{SL}_n(K)H$. Cela prouve que $\mathrm{GL}_n(K) = \mathrm{SL}_n(K)H$. Par conséquent, G est le produit semi-direct $\mathrm{SL}_n(K) \rtimes H$.

Si le produit est direct alors, d'après le cours, H est normal dans G . D'après la démonstration du théorème 4.23, les éléments de $\mathrm{SL}_n(K)$ et de H commuteraient

entre eux. Mais c'est faux : un calcul montre que la matrice $\begin{pmatrix} 1 & \dots & 1 \\ & \ddots & \vdots \\ & & 1 \end{pmatrix} \in \mathrm{SL}_n(K)$

qui est triangulaire supérieure à coefficients égaux à 1, et la matrice $A_2 \in H$ ne commutent pas. Donc le produit n'est pas direct.

Corrigé des exercices du chapitre 5

Solution de l'exercice 5.1. Soit G un groupe agissant sur un ensemble X . Si $g \in G$ et x, y sont dans X , on a, en utilisant les axiomes d'une action,

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

Solution de l'exercice 5.2. Il est sous-entendu qu'on fait agir \mathcal{S}_3 sur $\{1, 2, 3\}$ de la manière usuelle c'est-à-dire par permutations (voir exemple 5.4.1). Les éléments de \mathcal{S}_3 sont :

$$\text{id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2).$$

L'orbite de 1 est $\{1, 2, 3\}$ puisque la transposition $(1, 2)$ (resp. $(1, 3)$) envoie 1 sur 2 (resp. 3). De même, les orbites de 2 et 3 sont $\{1, 2, 3\}$. Il n'y a donc qu'une orbite. L'action est transitive.

Une permutation σ est dans le stabilisateur de 1 si et seulement si $\sigma(1) = 1$. Donc le stabilisateur de 1 est $\{\text{id}, (2, 3)\}$. De même celui de 2 est $\{\text{id}, (1, 3)\}$, et celui de 3 est $\{\text{id}, (1, 2)\}$. Certains de ces stabilisateurs ne sont pas réduits à $\{\text{id}\}$ donc l'action n'est pas libre, et encore moins simplement transitive. Par contre, l'intersection des stabilisateurs est $\{\text{id}\}$ donc l'action est fidèle.

Solution de l'exercice 5.3. Soient $G = \{M \in \text{GL}_2(\mathbb{R}) \mid \det M = 1\}$ et $\mathcal{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$.

1. Posons $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \star z = \frac{az + b}{cz + d}$ pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ et $z \in \mathcal{H}$. On a, en multipliant par la quantité conjuguée,

$$M \star z = \frac{az + b}{cz + d} = \frac{(az + b)(\overline{cz + d})}{|cz + d|^2} = \frac{ac|z|^2 + bd + adz + bc\bar{z}}{|cz + d|^2}$$

d'où

$$\text{Im}(M \star z) = \frac{(ad - bc) \text{Im} z}{|cz + d|^2} = \frac{\text{Im} z}{|cz + d|^2} > 0.$$

Donc le nombre complexe $M \star z$ appartient à \mathcal{H} et on a une application $G \times \mathcal{H} \rightarrow \mathcal{H}$, $(M, z) \mapsto M \star z$. De plus on a $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \star z = z$ et pour tous M, M' dans G :

$$\begin{aligned} M \star (M' \star z) &= M \star \frac{a'z + b'}{c'z + d'} = \frac{a \frac{a'z + b'}{c'z + d'} + b}{c \frac{a'z + b'}{c'z + d'} + d} \\ &= \frac{(aa' + bc')z + ab' + d'b}{(a'c + c'd)z + cb' + dd'} = (MM') \star z \end{aligned}$$

(on pouvait aussi remarquer que $\begin{pmatrix} az + b \\ cz + d \end{pmatrix} = M \begin{pmatrix} z \\ 1 \end{pmatrix}$ et utiliser l'associativité du produit matriciel). Ainsi \star définit une action de G sur \mathcal{H} .

2. Le stabilisateur G_i de i est formé des matrices $M \in G$ vérifiant $i = \frac{ai + b}{ci + d}$ c'est-à-dire $b + c = (d - a)i$. Comme a, b, c, d sont réels, cela équivaut à : $b + c = 0$ et $d - a = 0$. Donc

$$G_i = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}, a^2 + b^2 = 1 \right\} = \text{SO}_2(\mathbb{R}).$$

C'est le groupe des matrices orthogonales directes en dimension 2 c'est-à-dire des rotations de l'espace euclidien \mathbb{R}^2 .

3. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ vérifiant, pour tout $z \in \mathcal{H}$: $M \star z = z$. Alors pour tout $z \in \mathcal{H}$, on a $\frac{az + b}{cz + d} = z$ c'est-à-dire $cz^2 + (d - a)z + b = 0$. Le polynôme $cX^2 + (d - a)X + b$ de $\mathbb{C}[X]$ admet une infinité de racines dans \mathbb{C} (ce sont les éléments de \mathcal{H}). Il est donc nul. On en déduit $c = 0$, $a = d$ et $b = 0$. Comme $ad - bc = 1$ il vient $a^2 = 1$ i.e. $a = \pm 1$. L'intersection des stabilisateurs est $\{I_2, -I_2\}$, où I_2 désigne la matrice identité. L'action n'est pas fidèle.

4. Pour voir que l'action est transitive, on montre que tout $z \in \mathcal{H}$ est dans l'orbite du nombre complexe i . Cela revient à trouver $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ telle que $z = \frac{ai + b}{ci + d}$. Écrivons $z = x + iy$ avec x, y réels et $y > 0$. On constate que la matrice $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$ pourrait convenir, à ceci près qu'elle n'est pas de déterminant 1. Cependant comme $y > 0$ on peut considérer la matrice

$$M = \begin{pmatrix} \frac{y}{\sqrt{y}} & \frac{x}{\sqrt{y}} \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix}$$

qui est de déterminant 1 et vérifie $M \star i = \left(\frac{yi}{\sqrt{y}} + \frac{x}{\sqrt{y}} \right) \sqrt{y} = yi + x = z$. Cela prouve la transitivité.

Solution de l'exercice 5.4. Notons G le groupe.

1. Pour la translation ($g \star x = gx$), on a pour tous $(g, g') \in G \times G$ et $x \in G$: $1_G \star x = 1_G x = x$ et $g \star (g' \star x) = g \star (g' x) = g(g' x) = gg' x = (gg') \star x$ (égalités dans G). Donc le groupe agit sur lui-même par translation. Le stabilisateur d'un élément $x \in G$ est $\{g \in G \mid gx = x\} = \{g \in G \mid g = 1_G\} = \{1_G\}$ puisque x est inversible dans G . L'orbite de $x \in G$ est G car pour tout $y \in G$ on peut écrire $y = (yx^{-1})x = (yx^{-1}) \star x \in G \star x$.

Pour la conjugaison ($g \star x = gxg^{-1}$), on a pour tous $(g, g') \in G \times G$ et $x \in G$: $1_G \star x = 1_G x 1_G^{-1} = x$ et $g \star (g' \star x) = g \star (g' x g'^{-1}) = gg' x g'^{-1} g^{-1} = (gg') x (gg')^{-1} = (gg') \star x$. Donc le groupe agit sur lui-même par conjugaison. Le stabilisateur d'un élément $x \in G$ est $\{g \in G \mid gxg^{-1} = x\}$: c'est le centralisateur de la partie $\{x\}$. L'orbite de x est l'ensemble des gxg^{-1} où g parcourt G : c'est l'ensemble des conjugués de x dans G .

2. Pour l'action par translation, tous les stabilisateurs étant réduits au neutre, l'action est libre. On a aussi vu qu'il n'y a qu'une seule orbite, donc l'action est transitive d'où simplement transitive.
3. Notons \mathcal{S} l'ensemble des sous-groupes de G . Il nous faut vérifier au préalable que pour tout sous-groupe H de G et $g \in G$, l'ensemble gHg^{-1} est encore un sous-groupe de G : en effet on a $1_G = g1_Gg^{-1} \in gHg^{-1}$ et pour tous gh_1g^{-1} et gh_2g^{-1} dans gHg^{-1} , on a

$$gh_1g^{-1}(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1}.$$

En posant $g \star H = gHg^{-1}$, on a donc $g \star H \in \mathcal{S}$.

Pour tous g, g' dans G et $H \in \mathcal{S}$, on a $1_G \star H = 1_G H 1_G^{-1} = H$ et $g \star (g' \star H) = g \star (g' H (g')^{-1}) = gg' H (g')^{-1} g^{-1} = (gg') H (gg')^{-1} = (gg') \star H$. Cela montre que G agit sur \mathcal{S} par conjugaison.

Solution de l'exercice 5.5. Comme x et y sont dans la même orbite, il existe $h \in G$ tel que $y = h \star x$. Soit $g \in G$. On a alors

$$\begin{aligned} g \in G_y &\Leftrightarrow g \star y = y \Leftrightarrow g \star (h \star x) = h \star x \Leftrightarrow (gh) \star x = h \star x \\ &\Leftrightarrow (h^{-1}gh) \star x = x \Leftrightarrow h^{-1}gh \in G_x. \end{aligned}$$

Ainsi on a $G_y = hG_xh^{-1}$ c'est-à-dire $G_x = gG_yg^{-1}$ en posant $g = h^{-1}$.

Solution de l'exercice 5.6. Soient \star une action de G sur X et φ_\star l'application définie comme dans la proposition. D'abord pour tout $g \in G$, $\varphi_\star(g)$ est bien une bijection de X : en effet il est facile de vérifier que l'application réciproque est $x \mapsto g^{-1} \star x$. Montrons ensuite que φ_\star est un morphisme de groupes. Pour tous g, g' dans G et $x \in X$ on a :

$$\varphi_\star(gg')(x) = (gg') \star x = g \star (g' \star x) = g \star (\varphi_\star(g')(x)) = \varphi_\star(g) \circ \varphi_\star(g')(x)$$

d'où $\varphi_\star(gg') = \varphi_\star(g) \circ \varphi_\star(g')$.

Maintenant considérons un morphisme $\varphi : G \rightarrow \mathcal{S}_X$ et soit \star_φ défini comme dans la proposition : $g \star_\varphi x = \varphi(g)(x)$. Pour tous $x \in X$ et g, g' dans G , on a $1_G \star_\varphi x = \varphi(1_G)(x) = \text{id}(x) = x$ et

$$g \star_\varphi (g' \star_\varphi x) = g \star_\varphi (\varphi(g')(x)) = \varphi(g)(\varphi(g')(x)) = \varphi(gg')(x)$$

car φ est un morphisme de groupes. Ainsi \star_φ définit une action de G sur X .

Enfin vérifions que les deux opérations sont réciproques l'une de l'autre. En partant d'une action \star de G sur X , on a pour tous $x \in X$ et $g \in G$,

$$g \star_{(\varphi_\star)} x = \varphi_\star(g)(x) = g \star x$$

et en partant d'un morphisme φ , on a pour tous $x \in X$ et $g \in G$

$$\varphi_{(\star_\varphi)}(g)(x) = g \star_\varphi x = \varphi(g)(x).$$

Donc $\star_{(\varphi_\star)} = \star$ et $\varphi_{(\star_\varphi)} = \varphi$.

Solution de l'exercice 5.7. 1. Soient $G = \text{GL}_2(\mathbb{F}_2)$ et

$$X = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x \in \mathbb{F}_2, y \in \mathbb{F}_2, (x, y) \neq (\bar{0}, \bar{0}) \right\}.$$

Commençons par vérifier que $M \star v = Mv$ appartient à X , pour tous $M \in G$ et $v \in X$: c'est vrai car toute matrice inversible envoie un vecteur non nul sur un vecteur non nul. Vérifions ensuite que \star définit une action : pour tous M et M' dans G et $v \in X$ on a

$$I \star v = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} v = v,$$

$$M \star (M' \star v) = M \star (M'v) = M(M'v) = (MM')v = (MM') \star v$$

où $I = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$ désigne la matrice identité dans G . Donc \star est une action de G sur X .

2. Soit $\varphi : G \rightarrow \mathcal{S}_X$, $M \mapsto (v \mapsto M \star v)$ le morphisme de groupes associé à cette action par la proposition 5.6. Supposons $\varphi(M) = \text{id}_X$. Cela signifie que tout $v \in X$ satisfait $M \star v = \text{id}_X(v) = v$. En prenant successivement pour v les vecteurs $\begin{pmatrix} \bar{1} \\ \bar{0} \end{pmatrix}$ et $\begin{pmatrix} \bar{0} \\ \bar{1} \end{pmatrix}$, qui appartiennent à X , cela entraîne que M est la matrice identité I . Donc $\text{Ker } \varphi = \{I\}$, ce qui entraîne l'injectivité de φ (autrement dit on vient de prouver que l'action est fidèle). Par ailleurs, comme $\text{Card}(X) = 4 - 1 = 3$, le groupe \mathcal{S}_X est isomorphe à \mathcal{S}_3 et de cardinal $3! = 6$. Si on montre que G et \mathcal{S}_X ont même cardinal, c'est-à-dire 6, le morphisme sera bijectif. Or si on dresse la liste des matrices 2×2 à coefficients dans $\{\bar{0}, \bar{1}\}$ et ne garde que celles qui sont de déterminant non nul, on trouve que $\text{Card}(G) = 6$. Cela permet de conclure que φ est un isomorphisme.

Solution de l'exercice 5.8. 1. Le cardinal d'une orbite divise l'ordre du groupe, d'après la proposition 5.15. Les seules possibilités sont donc 1, 3, 7 et 21.

2. L'ensemble E est la réunion de ses orbites distinctes sous l'action de G (relation (5.1) du cours). Donc la somme des cardinaux des orbites est égale au cardinal n de E . Or il y a N_i orbites de cardinal i , avec $i \in \{1, 3, 7, 21\}$. En regroupant les orbites selon leur cardinal, on en déduit

$$n = \sum_i iN_i = N_1 + 3N_3 + 7N_7 + 21N_{21}.$$

3. Rappelons qu'un élément de E est un point fixe si son orbite est ponctuelle. Supposons $n = 11$. On a donc $N_1 + 3N_3 + 7N_7 + 21N_{21} = 11$. Ceci implique $N_{21} = 0$ (sinon $11 = N_1 + 3N_3 + 7N_7 + 21N_{21}$ serait > 21 ce qui est impossible). On a ensuite $N_1 + 3N_3 + 7N_7 = 11$ donc $N_7 = 0$ ou 1 (raisonnement similaire : si $N_7 \geq 2$ alors $11 = N_1 + 3N_3 + 7N_7$ serait ≥ 14 ce qui est impossible). Si $N_7 = 0$ alors $N_1 + 3N_3 = 11$ d'où on tire $N_1 > 0$ (sinon 3 diviserait 11 , ce qui est impossible). De même, si $N_7 = 1$ alors $N_1 + 3N_3 = 4$ d'où $N_1 > 0$ (sinon 3 diviserait 4). Dans tous les cas on a $N_1 > 0$ c'est-à-dire qu'il existe au moins une orbite à un élément, autrement dit un point fixe.
4. On a ici $N_1 + 3N_3 + 7N_7 + 21N_{21} = 19$. Par hypothèse, il n'y a pas de point fixe, donc $N_1 = 0$. De plus on a nécessairement $N_{21} = 0$ (sinon le membre de gauche serait ≥ 21 et égal à 19). Donc $3N_3 + 7N_7 = 19$. A priori N_7 peut valoir $0, 1$ ou 2 (au-delà $3N_3 + 7N_7$ serait strictement supérieur à 19). Le cas $N_7 = 0$ est impossible (car 3 ne divise pas 19). Le cas $N_7 = 2$ est aussi impossible (car 3 ne divise pas 5). On a donc $N_7 = 1$ et $N_3 = 4$. Le nombre d'orbites distinctes est alors $N_1 + N_3 + N_7 + N_{21} = 5$ (on les a regroupées suivant leur cardinal).

Solution de l'exercice 5.9. 1. Soit G un groupe tel que le groupe quotient $G/Z(G)$ est cyclique (rappelons que le centre $Z(G)$ est normal dans G , ce qui fait de $G/Z(G)$ un groupe quotient). Soit \bar{a} un générateur de $G/Z(G)$. On a $G/Z(G) = \langle \bar{a} \rangle = \{\bar{a}^k \mid k \in \mathbb{Z}\}$. Montrons que G est abélien. Soient x et y dans G . Leurs classes \bar{x} et \bar{y} dans $G/Z(G)$ sont donc de la forme : $x = \bar{a}^n$ et $y = \bar{a}^m$ avec n et m dans \mathbb{Z} . On en déduit l'existence de z_1 et z_2 dans $Z(G)$ tels que $x = a^n z_1$ et $y = a^m z_2$ dans G . Comme z_1 et z_2 sont dans le centre, on a

$$xy = a^n z_1 a^m z_2 = a^{n+m} z_1 z_2 = a^m a^n z_2 z_1 = a^m z_2 a^n z_1 = yx.$$

Ceci étant valable pour tous x et y dans G , le groupe G est abélien.

2. Soit G un groupe d'ordre p^2 où p est un nombre premier. Son centre $Z(G)$ est d'ordre $1, p$ ou p^2 par le théorème de Lagrange. D'après la proposition 5.23 on sait que $Z(G) \neq \{1_G\}$. Si $Z(G)$ est d'ordre p^2 alors $G = Z(G)$ pour des raisons de cardinal ; en particulier G est abélien. Supposons maintenant $Z(G)$ d'ordre p . Alors $G/Z(G)$ est d'ordre $p^2/p = p$, qui est premier. D'après une conséquence du théorème de Lagrange (corollaire 3.29), $G/Z(G)$ est donc cyclique. On applique alors le résultat de la question précédente : le groupe G est abélien.

Solution de l'exercice 5.10. On a $63 = 3^2 \times 7$. D'après les théorèmes de Sylow, le nombre n_7 de 7-Sylow de G divise 9 (d'où $n_7 \in \{1, 3, 9\}$) et $n_7 \equiv 1 \pmod{7}$. Comme $3 \not\equiv 1 \pmod{7}$ et $9 \not\equiv 1 \pmod{7}$, la seule valeur possible est $n_7 = 1$. Il y a donc un unique 7-Sylow dans G , qu'on note H . Le sous-groupe H est normal par la proposition 5.31. Par ailleurs, H est distinct de G et de $\{1_G\}$ puisqu'il possède 7 éléments. Donc G n'est pas simple.

Solution de l'exercice 5.11. 1. On a $35 = 5 \times 7$. Soient n_5 et n_7 les nombres de 5-Sylow et 7-Sylow de G , c'est-à-dire ici de sous-groupes d'ordre 5 et 7. Les théorèmes de Sylow nous disent que $n_5 \mid 7$ (donc $n_5 = 1$ ou 7), $n_5 \equiv 1 \pmod{5}$, $n_7 \mid 5$ (donc $n_7 = 1$ ou 5) et $n_7 \equiv 1 \pmod{7}$. Les seules possibilités sont $n_5 = 1$ et $n_7 = 1$. Le groupe possède un unique sous-groupe d'ordre 5, qu'on note H , et un unique sous-groupe d'ordre 7, qu'on note K . D'après la proposition 5.31, ils sont donc normaux dans G .

2. Le groupe H (resp. K) est d'ordre premier 5 (resp. 7), donc H est isomorphe au groupe additif cyclique $\mathbb{Z}/5\mathbb{Z}$ (resp. $\mathbb{Z}/7\mathbb{Z}$) d'après le corollaire 3.29.

Montrons ensuite que $G \simeq H \times K$. Pour cela on cherche à appliquer le critère du produit direct (théorème 4.23). On sait déjà que H et K sont normaux dans G . De plus, $H \cap K = \{1_G\}$: en effet, $H \cap K$ est un sous-groupe à la fois de H et de K ; d'après le théorème de Lagrange, l'ordre de $H \cap K$ divise donc $\text{ord}(H) = 5$ et $\text{ord}(K) = 7$; comme 5 et 7 sont premiers entre eux, $H \cap K$ est d'ordre 1 d'où $H \cap K = \{1_G\}$. Maintenant considérons l'application entre ensembles :

$$\begin{aligned} H \times K &\longrightarrow G \\ (x, y) &\longmapsto xy. \end{aligned}$$

Comme $H \cap K = \{1_G\}$, elle est injective : en effet, si $xy = x'y'$ alors $x(x')^{-1} = y'y^{-1} \in H \cap K = \{1_G\}$ d'où $x = x'$ et $y = y'$. De plus l'image de cette application est HK par définition. On en déduit une bijection entre les ensemble $H \times K$ et HK d'où on tire $\text{Card}(HK) = \text{Card}(H) \times \text{Card}(K) = 35$. Comme HK est contenu dans G qui est aussi d'ordre 35, cela entraîne $G = HK$. Les hypothèses sont réunies pour appliquer le critère du produit direct : G est donc isomorphe à $H \times K$.

En conclusion, G est isomorphe à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/35\mathbb{Z}$, le dernier isomorphisme provenant du théorème chinois (voir exercice 3.14 ou chapitre 6) puisque 5 et 7 sont premiers entre eux. Par conséquent G est cyclique.

Solution de l'exercice 5.12. 1. (a) Par hypothèse, G est d'ordre pm avec $p \nmid m$. Ses p -Sylow sont donc ici d'ordre p . Soit H un p -Sylow de G . Par le théorème de Lagrange, les éléments de H sont d'ordre divisant le nombre premier p c'est-à-dire 1 (pour l'élément neutre) ou p (dans les autres cas). Donc H possède exactement $(p-1)$ éléments d'ordre p .

(b) Soient H_1 et H_2 des p -Sylow de G avec $H_1 \neq H_2$. Supposons qu'il existe $x \in H_1 \cap H_2$ avec $x \neq 1_G$. D'après la question précédente, x est d'ordre p . Donc $\langle x \rangle$ est un sous-groupe d'ordre p de $H_1 \cap H_2$. Or $H_1 \cap H_2$ est un sous-groupe de H_1 qui est lui-même d'ordre p . Donc

on a $\langle x \rangle = H_1 \cap H_2 = H_1 = H_2$, ce qui contredit $H_1 \neq H_2$. Ainsi $H_1 \cap H_2 = \{1_G\}$.

- (c) Dénombrons les éléments de G d'ordre p . D'après la première question, tout p -Sylow de G a exactement $(p-1)$ éléments d'ordre p . De plus, par la deuxième question, deux p -Sylow distincts n'ont aucun élément d'ordre p en commun. Ainsi la réunion des n_p p -Sylow de G a exactement $(p-1)n_p$ éléments d'ordre p . Par ailleurs, si $x \in G$ est d'ordre p , le sous-groupe $\langle x \rangle$ est d'ordre p , donc ici un p -Sylow de G . On en déduit que tout élément d'ordre p de G appartient à un p -Sylow. Finalement, G a exactement $(p-1)n_p$ éléments d'ordre p .
2. On a $30 = 2 \times 3 \times 5$. D'après les théorèmes de Sylow, on a d'une part $n_3 \mid 10$ (d'où $n_3 \in \{1, 2, 5, 10\}$) et $n_3 \equiv 1 \pmod{10}$, donc $n_3 \in \{1, 10\}$, et d'autre part $n_5 \mid 6$ et $n_5 \equiv 1 \pmod{5}$, donc $n_5 \in \{1, 6\}$. Supposons $n_3 \neq 1$ c'est-à-dire $n_3 = 10$. On est dans la situation du préliminaire (3 divise 30 mais 9 ne divise pas 30). Comme $n_3 = 10$, il y a donc $2n_3 = 20$ éléments d'ordre 3 dans G . De même pour $p = 5$, si $n_5 \neq 1$ on est dans la situation du préliminaire, donc $n_5 = 6$ et il existe $6 \times 4 = 24$ éléments d'ordre 5 dans G .
3. Si $n_3 \neq 1$ et $n_5 \neq 1$, par ce qui précède on connaît déjà l'existence de $20 + 24 = 44$ éléments distincts dans G . C'est impossible car G est d'ordre 30. Donc $n_3 = 1$ ou $n_5 = 1$. Dans le premier (resp. deuxième) cas, G possède un unique 3- (resp. 5-)Sylow. D'après la proposition 5.31, ce Sylow est normal dans G . Donc G ne peut pas être simple.

Solution de l'exercice 5.13. Soit p un nombre premier tel que $p > 2$. Soit G un groupe d'ordre $2p$.

- Comme p (resp. 2) est un nombre premier qui divise l'ordre de G , le groupe possède au moins un élément d'ordre p (resp. d'ordre 2) d'après le théorème de Cauchy (théorème 5.29). Notons a (resp. b) un élément d'ordre p (resp. 2). Ces éléments sont distincts puisque $p > 2$.
- D'après les théorèmes de Sylow, le nombre n_p de p -Sylow satisfait $n_p \mid 2$ (donc $n_p \in \{1, 2\}$) et $n_p \equiv 1 \pmod{p}$. Or $2 \not\equiv 1 \pmod{p}$. Donc n_p vaut 1. On note P l'unique p -Sylow de G .
- Raisonnons par l'absurde : supposons que l'élément ba est d'ordre p . Il engendre alors un sous-groupe d'ordre p dans G . Étant donné que $\text{ord}(G) = 2p$, un sous-groupe d'ordre p est nécessairement un p -Sylow de G . On conclut que $\langle ba \rangle$ est l'unique p -Sylow de G , par la question précédente. Le même raisonnement s'applique à a , qui est d'ordre p . On a donc $\langle ba \rangle = P = \langle a \rangle$. On conclut que $b = (ba)a^{-1}$ appartient à P . Comme P est d'ordre p , le théorème de Lagrange appliqué à P donne que tous les éléments de P sauf 1_G sont d'ordre p . Ainsi b est d'ordre p . C'est impossible car $\text{ord}(b) = 2 < p$. Nous avons ainsi montré que ba n'est pas d'ordre p .
- Par le théorème de Lagrange appliqué au groupe G , l'ordre de ba divise $2p$ et vaut donc 1, 2, p ou $2p$. Si $\text{ord}(ba) = 1$ alors $ba = 1_G$ d'où $a = b^{-1} = b$, ce qui est impossible. Nous avons déjà exclu le cas où $\text{ord}(ba) = 2$.

Supposons que $\text{ord}(ba) = 2p$. Alors G , qui est d'ordre $2p$ possède un élément d'ordre $2p$. D'après la proposition 3.17, G est cyclique d'ordre $2p$. Par le théorème 3.19, G est donc isomorphe à $(\mathbb{Z}/2p\mathbb{Z}, +)$.

Il reste enfin à traiter le cas où $\text{ord}(ba) = 2$. Considérons le sous-groupe $H = \langle a, b \rangle$. Comme $\text{ord}(a) = p$, $\text{ord}(b) = 2$ et $baba = 1_H = 1_G$, H est donc un groupe diédral D_p d'ordre $2p$. Par comparaison de cardinaux, on en déduit $H = G$. Ainsi G est un groupe diédral D_p .

5. Les groupes $(\mathbb{Z}/2p\mathbb{Z}, +)$ et D_p ne sont pas isomorphes : le premier est abélien, le second ne l'est pas.

Corrigé des exercices du chapitre 6

Solution de l'exercice 6.1. On a $36 = 2^2 \times 3^2$ donc ses diviseurs positifs sont 1, 2, 3, 4, 6, 9, 12, 18, 36. Le nombre 59 est premier donc ses diviseurs positifs sont 1 et 59. Enfin on a $30 = 2 \times 3 \times 5$ donc ses diviseurs positifs sont 1, 2, 3, 5, 6, 10, 15, 30.

Solution de l'exercice 6.2. 1. On applique l'algorithme d'Euclide :

$$792 = 318 \times 2 + 156$$

$$318 = 156 \times 2 + 6$$

$$156 = 6 \times 26 + 0.$$

Donc $\text{pgcd}(792, 318)$ est le dernier reste non nul c'est-à-dire 6.

2. On utilise de manière répétée la propriété $\text{pgcd}(a, b) = \text{pgcd}(b, a - bq)$ (voir corollaire 6.14) qui est le fondement de l'algorithme d'Euclide. On a

$$\begin{aligned} \text{pgcd}((n+1)! + 1, n! + 1) &= \text{pgcd}(n! + 1, (n+1)! + 1 - (n+1)(n! + 1)) \\ &= \text{pgcd}(n! + 1, n) = \text{pgcd}(n, n! + 1 - (n-1)n!) \\ &= \text{pgcd}(n, 1) = 1. \end{aligned}$$

3. On a $a^2 - b^2 = (a-b)(a+b)$ et $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$ d'où $\text{pgcd}(a^2 - b^2, a^3 - b^3) = |a-b| \text{pgcd}(a+b, a^2 + ab + b^2)$ (la valeur absolue vient du fait que le pgcd est, par définition, un entier naturel). On utilise à nouveau le corollaire 6.14 :

$$\text{pgcd}(a+b, a^2 + ab + b^2) = \text{pgcd}(a+b, a^2 + ab + b^2 - (a+b)b) = \text{pgcd}(a+b, a^2).$$

Soit p un nombre premier divisant $\text{pgcd}(a+b, a^2)$. Alors p divise a^2 donc, par le lemme d'Euclide, p divise a . Par ailleurs p divise b . On en déduit que p divise $\text{pgcd}(a, b) = 1$, ce qui est impossible. Ainsi $\text{pgcd}(a+b, a^2)$ vaut 1 d'où $\text{pgcd}(a+b, a^2 + ab + b^2) = |a-b|$.

Solution de l'exercice 6.3. 1. On applique l'algorithme d'Euclide :

$$679 = 455 \times 1 + 224$$

$$455 = 224 \times 2 + 7$$

$$224 = 7 \times 32 + 0.$$

Donc $\text{pgcd}(678, 455)$ est le dernier reste non nul c'est-à-dire 7. En remontant les lignes de l'algorithme, on obtient

$$\begin{aligned} 7 &= 455 - 2 \times 224 \\ &= 455 - 2 \times (679 - 455) \\ &= 3 \times 455 - 2 \times 679 \end{aligned}$$

donc $u = -2$ et $v = 3$ conviennent.

2. Soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ une solution de $679x + 455y = \text{pgcd}(679, 455) = 7$. En simplifiant les deux membres de l'équation par le pgcd, on obtient

$$97x + 65y = 1.$$

Par ailleurs on a $679 \times (-2) + 455 \times 3 = 7$ d'où, en simplifiant par le pgcd, $97 \times (-2) + 65 \times 3 = 1$. Par soustraction des équations cela donne

$$97(x + 2) + 65(y - 3) = 0. \quad (6.3)$$

En particulier 97 divise $65(y - 3)$. Comme 97 et 65 sont premiers entre eux, le lemme de Gauss entraîne que 97 divise $y - 3$. Il existe $t \in \mathbb{Z}$ tel que $y - 3 = 97t$ d'où $y = 97t + 3$. En reportant cette expression de y dans (6.3) on a $x = -65t - 2$. L'ensemble des solutions de $679x + 455y = 7$ est donc inclus dans l'ensemble

$$S = \{(-65t - 2, 97t + 3) \mid t \in \mathbb{Z}\}.$$

Inversement on vérifie par un calcul direct que pour tout $t \in \mathbb{N}$, le couple $(-65t - 2, 97t + 3)$ est solution de l'équation $679x + 455y = 7$. L'ensemble des solutions cherché est donc S .

Remarque. Les lecteurs attentifs constateront que cette méthode se généralise si on remplace les valeurs 679 et 455 par n'importe quels entiers naturels.

Solution de l'exercice 6.4. Posons $f_0 = 0$, $f_1 = 1$ et $f_{n+1} = f_n + f_{n-1}$ pour tout $n \geq 2$. Les premiers nombres de Fibonacci sont

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55.$$

1. En utilisant la définition de f_{n+1} et le corollaire 6.14, on a pour tout entier $n \geq 2$:

$$\begin{aligned} \text{pgcd}(f_{n+1}, f_n) &= \text{pgcd}(f_n + f_{n-1}, f_n) = \text{pgcd}(f_n, f_n + f_{n-1} - f_n) \\ &= \text{pgcd}(f_n, f_{n-1}). \end{aligned}$$

Par récurrence on en déduit $\text{pgcd}(f_{n+1}, f_n) = \text{pgcd}(f_0, f_1) = 1$. Donc f_n et f_{n+1} sont premiers entre eux pour tout $n \in \mathbb{N}$.

2. Non : on a $f_3 = 2$ et $f_6 = 8$, qui ne sont pas premiers entre eux, ou encore $f_5 = 5$ et $f_{10} = 55$.

3. Les formules usuelles pour les racines des polynômes de degré 2 montrent que φ et φ' sont les solutions réelles de $x^2 - x - 1 = 0$. On en déduit $\varphi^2 - \varphi = 1$ d'où $\varphi - 1 = \frac{1}{\varphi}$ et de même, $\varphi' - 1 = \frac{1}{\varphi'}$.

Montrons la relation cherchée par récurrence sur n . La relation est vraie pour $n = 0$ et $n = 1$. Supposons la vraie jusqu'au rang n . Au rang $n + 1$ on a

$$\begin{aligned} \frac{1}{\sqrt{5}} (\varphi^{n+1} + \varphi'^{n+1}) &= \frac{1}{\sqrt{5}} (\varphi^{n+1} - \varphi^n - \varphi'^{n+1} + \varphi'^n + \varphi^n - \varphi'^n) \\ &= \frac{1}{\sqrt{5}} (\varphi^n(\varphi - 1) - \varphi'^n(\varphi' - 1)) + f_n \\ &= \frac{1}{\sqrt{5}} (\varphi^{n-1} - \varphi'^{n-1}) + f_n \\ &= f_{n-1} + f_n = f_{n+1} \end{aligned}$$

d'où le résultat.

Solution de l'exercice 6.5. 1. Soient $n \geq 1$ et $k \in \mathbb{Z}$ deux entiers.

Supposons $\text{pgcd}(k, n) = 1$. D'après le théorème de Bézout, il existe des entiers relatifs u et v tels que $un + kv = 1$. Modulo n , on en déduit $\bar{k}\bar{v} = \bar{1}$. Pour tout $a \in \mathbb{Z}$, on a donc $\bar{a} = \bar{a} \cdot \bar{1} = \bar{a}k\bar{v} = \bar{a}\bar{v} \cdot \bar{k}$ dans $\mathbb{Z}/n\mathbb{Z}$. Ceci prouve que $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$.

Réciproquement, supposons que \bar{k} est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$. Tout élément de $\mathbb{Z}/n\mathbb{Z}$ est donc un multiple entier de la classe \bar{k} . C'est en particulier vrai pour $\bar{1}$: il existe $v \in \mathbb{Z}$ tel que $\bar{1} = \bar{v} \cdot \bar{k}$. On en déduit que n divise $1 - vk$ d'où l'existence de $u \in \mathbb{Z}$ tel que $un + vk = 1$. D'après la réciproque du théorème de Bézout, on conclut que $\text{pgcd}(k, n) = 1$.

2. Les entiers $k \in \{0, \dots, 17\}$ tels que $\text{pgcd}(k, 18) = 1$ sont 1, 5, 7, 11, 13, 17. Les générateurs de $(\mathbb{Z}/18\mathbb{Z}, +)$ sont donc $\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}$.

Solution de l'exercice 6.6. On considère le nombre $m = 1024$ écrit en base 10. La démonstration de la proposition 6.19 fournit un algorithme pour écrire m dans n'importe quelle base, en utilisant des divisions euclidiennes par b .

— On a $1024 = 2^{10}$ donc $m = \overline{10000000000}^2$.

— Posons $b = 3$. On a les divisions euclidiennes $m = 1024 = 341b + 1$, puis $341 = 113b + 2$, $113 = 37b + 2$, $37 = 12b + 1$, $12 = 4b + 0$, $4 = b + 1$ d'où

$$\begin{aligned} m &= 1 + 341b = 1 + b(2 + 113b) = 1 + b(2 + b(2 + 37b)) \\ &= 1 + b(2 + b(2 + b(12b + 1))) = 1 + b(2 + b(2 + b(1 + b^2 + b^3))). \end{aligned}$$

On obtient $m = 1 + 2b + 2b^2 + b^3 + b^5 + b^6$ donc $m = \overline{1101221}^3$.

— Un calcul similaire donne, en base $b = 5$: $m = \overline{13044}^5$.

Solution de l'exercice 6.7. Soit X l'ensemble des nombres premiers de la forme $4k + 3$ avec $k \in \mathbb{N}$.

1. L'ensemble X est non vide car il contient le nombre premier 3 (prendre $k = 0$).

2. Pour k et k' dans \mathbb{Z} , on a $4k + 1 \equiv 1 \pmod{4}$ et $4k' + 1 \equiv 1 \pmod{4}$ d'où $(4k + 1)(4k' + 1) \equiv 1 \times 1 \equiv 1 \pmod{4}$. Donc il existe $\ell \in \mathbb{Z}$ tel que $(4k + 1)(4k' + 1) = 4\ell + 1$.
3. Supposons l'ensemble X fini. Notons $X = \{p_1, \dots, p_n\}$ et posons

$$N = 4p_1 \cdots p_n - 1.$$

- (a) Raisonnons par l'absurde : supposons que tout diviseur premier de N n'est pas de la forme $4k + 3$. Remarquons que N , de par sa forme, est impair. Donc les diviseurs premiers de N sont impairs. Nécessairement ils sont congrus à 1 ou 3 modulo 4. D'après l'hypothèse, tous sont congrus à 1 modulo 4. Par la question précédente, leur produit est donc congru à 1 modulo 4. Ainsi $N \equiv 1 \pmod{4}$. Mais d'après la forme de N , on a $N \equiv -1 \pmod{4}$. Comme $1 \not\equiv -1 \pmod{4}$, c'est contradictoire. Ainsi N admet au moins un diviseur premier de la forme $4k + 3$.
- (b) D'après la question précédente, il existe $j \in \{1, \dots, n\}$ tel que p_j divise N . Comme p_j divise à la fois N et $p_1 \cdots p_n$, on en déduit que p_j divise 1 d'après l'expression de N , ce qui est impossible. En conclusion, l'ensemble X est infini.

Solution de l'exercice 6.8. Dans cet exercice, « diviseur » désigne un diviseur positif. Si $m \in \mathbb{N}$ on note $\sigma(m)$ la somme des diviseurs de m .

1. Montrons que $\sigma(m) = m + 1$ si et seulement si m est premier. Si m est premier alors ses seuls diviseurs sont 1 et m donc $\sigma(m) = m + 1$. Supposons maintenant que m n'est pas premier. Alors m a au moins trois diviseurs distincts : 1, m , d avec $1 < d < m$. On en déduit $\sigma(m) \geq 1 + m + d > 1 + m$ donc $\sigma(m) \neq m + 1$.
2. Les décompositions de m et n en facteurs premiers sont

$$m = \prod_{p \in A} p^{v_p(m)} \quad \text{et} \quad n = \prod_{q \in B} q^{v_q(n)}$$

où A (resp. B) désigne l'ensemble des diviseurs premiers de m (resp. de n). Comme m et n sont supposés premiers entre eux, A et B sont disjoints. Or on a

$$mn = \prod_{p \in A} p^{v_p(m)} \prod_{q \in B} q^{v_q(n)}. \quad (6.4)$$

Par unicité de la décomposition en facteurs premiers et du fait que A et B sont disjoints, l'écriture (6.4) est la décomposition de mn en facteurs premiers. On en déduit que tout diviseur de mn est de la forme

$$d = \prod_{p \in A} p^{\alpha_p} \prod_{q \in B} q^{\beta_q}$$

avec $0 \leq \alpha_p \leq v_p(m)$ et $0 \leq \beta_q \leq v_q(n)$ uniques. C'est l'écriture souhaitée.

3. En utilisant la question précédente, on obtient

$$\begin{aligned}\sigma(mn) &= \sum_{d|mn} d = \sum_{d_1|m, d_2|n} d_1 d_2 = \sum_{d_1|m} \left(\sum_{d_2|n} d_2 \right) d_1 \\ &= \sigma(n) \sum_{d_1|m} d_1 = \sigma(n)\sigma(m).\end{aligned}$$

4. La somme des diviseurs stricts d'un entier m est $\sigma(m) - m$. Donc m est parfait si et seulement si $\sigma(m) = 2m$.
5. Soit $n \in \mathbb{N}$. Supposons $2^{n+1} - 1$ premier. On montre que $m = 2^n(2^{n+1} - 1)$ est parfait en démontrant que $\sigma(m) = 2m$. Comme 2^n et $2^{n+1} - 1$ sont premiers entre eux et $2^{n+1} - 1$ premier, on a d'après les questions précédentes :

$$\sigma(m) = \sigma(2^n)\sigma(2^{n+1} - 1) = (1 + \dots + 2^n)2^{n+1} = (2^{n+1} - 1)2^{n+1} = 2m$$

ce qui permet de conclure que m est parfait.

6. La démonstration précédente montre que si $2^{n+1} - 1$ n'est pas premier alors

$$\sigma(m) = \sigma(2^n)\sigma(2^{n+1} - 1) > (2^{n+1} - 1)(2^{n+1} - 1 + 1) = 2m.$$

7. Soit m un nombre parfait pair. En factorisant m , on écrit $m = 2^n S$ où $n \geq 1$ et S est impair. On a

$$2m = \sigma(m) = \sigma(2^n)\sigma(S) = (2^{n+1} - 1)\sigma(S).$$

Or on a aussi $2m = 2^{n+1}S$ d'où

$$(2^{n+1} - 1)\sigma(S) = 2^{n+1}S.$$

Comme 2^{n+1} et $2^{n+1} - 1$ sont premiers entre eux, le lemme de Gauss entraîne que $2^{n+1} - 1$ divise S . On peut donc écrire

$$\sigma(S) = 2^{n+1} \frac{S}{2^{n+1} - 1}$$

où la fraction est dans \mathbb{N} . Or puisque $n > 0$ on a $2^{n+1} - 1 \neq 1$. Si $S \neq 2^{n+1} - 1$ on obtient

$$\sigma(S) \geq 1 + \frac{S}{2^{n+1} - 1} + S \geq 1 + \frac{2^{n+1}S}{2^{n+1} - 1} = 1 + \sigma(S),$$

ce qui est une contradiction. Donc $m = 2^n(2^{n+1} - 1)$. Par la question précédente, $2^{n+1} - 1$ est premier.

Solution de l'exercice 6.9. 1. Le tableau suivant indique les valeurs des carrés modulo 4 :

\bar{a}	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
\bar{a}^2	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$

donc tout $a \in \mathbb{Z}$ satisfait $a^2 \equiv 0 \pmod{4}$ ou $a^2 \equiv 1 \pmod{4}$.

2. On en déduit le tableau des valeurs de $a^2 + b^2$ modulo 4 :

$a^2 + b^2$	$a^2 = \bar{0}$	$a^2 = \bar{1}$
$b^2 = \bar{0}$	$\bar{0}$	$\bar{1}$
$b^2 = \bar{1}$	$\bar{1}$	$\bar{2}$

Donc $a^2 + b^2 \not\equiv 3 \pmod{4}$.

3. L'ensemble des nombres premiers inférieurs à 50 est

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}.$$

Le tableau recense ceux, notés p , congrus à 1 modulo 4 et constate que tous s'écrivent $p = a^2 + b^2$ avec a et b dans \mathbb{Z} :

p	5	13	17	29	37	41
a	1	2	1	2	1	4
b	2	3	4	5	6	5

Remarque. Un théorème de Fermat affirme que tout nombre premier congru à 1 modulo 4 est une somme de deux carrés d'entiers et, de manière plus générale, caractérise les entiers qui sont somme de deux carrés d'entiers.

Solution de l'exercice 6.10. En base 10, tout entier naturel n s'écrit $\sum_{i=0}^k n_i 10^i$ avec $n_i \in \{0, \dots, 9\}$, et $n_k \neq 0$ si $n \neq 0$.

1. Comme $10 \equiv 1 \pmod{3}$, on a $10^i \equiv 1^i \equiv 1 \pmod{3}$ pour tout $i \geq 1$ d'où

$$n \equiv \sum_{i=0}^k n_i 10^i \equiv \sum_{i=1}^k n_i \pmod{3}.$$

Donc $n \equiv 0 \pmod{3}$ si et seulement si la somme $\sum_{i=0}^k n_i$ des chiffres est congrue à 0 modulo 3, c'est-à-dire si c'est un multiple de 3.

2. Posons $m = n_0 10^0 + n_1 10^1 = n_0 + 10n_1$, nombre formé par les deux derniers chiffres de n en base 10. Il s'agit de montrer que $4 \mid n$ si et seulement si $4 \mid m$. Pour cela, il suffit de montrer que $n \equiv m \pmod{4}$. Comme $10 \equiv 2 \pmod{4}$, on a

$$n \equiv \sum_{i=0}^k n_i 10^i \equiv \sum_{i=0}^k n_i 2^i \pmod{4}.$$

Mais si $i \geq 2$ alors 2^i est divisible par 4 et donc $2^i \equiv 0 \pmod{4}$. Dans la somme, il ne reste que les contributions pour $i = 0$ et $i = 1$ c'est-à-dire

$$n \equiv \sum_{i=0}^1 n_i 2^i \equiv m \pmod{4}.$$

Solution de l'exercice 6.11. Soit $n \in \mathbb{N}$.

1. Si $n = 0$ alors $2^{2^n} - 1 = 1$. Si $n \geq 1$ alors $2n \geq 2$ donc 4 divise 2^{2^n} ; cela entraîne $2^{2^n} \equiv 0 \pmod{4}$ d'où $2^{2^n} - 1 \equiv -1 \equiv 3 \pmod{4}$.
2. On a $2^3 \equiv 8 \equiv 1 \pmod{7}$. Donc $2^{3n} \equiv 8^n \equiv 1 \pmod{7}$. On en déduit $2^{3n} - 1 \equiv 0 \pmod{7}$.
3. Raisonnons par récurrence sur n . L'initialisation à $n = 0$ est immédiate : $5^{2^0} = 5^1 = 5 = (1 + 4) \equiv 1 + 2^2 \pmod{2^3}$. Supposons la propriété vraie au rang n c'est-à-dire l'existence d'un $d \in \mathbb{Z}$ tel que $5^{2^n} = 1 + 2^{n+2} + 2^{n+3}d$. On en déduit alors

$$\begin{aligned} 5^{2^{n+1}} &= (5^{2^n})^2 = (1 + 2^{n+2} + 2^{n+3}d)^2 \\ &= 1 + 2^{2n+4} + 2^{2n+6}d^2 + 2^{n+3} + 2^{2n+6}d + 2^{n+4}d. \end{aligned}$$

D'où $5^{2^{n+1}} \equiv 1 + 0 + 0 + 2^{n+3} + 0 + 0 \equiv 1 + 2^{n+3} \pmod{2^{n+4}}$. Cela démontre l'hypothèse de récurrence au rang $n + 1$, ce qui conclut la récurrence.

Solution de l'exercice 6.12. Notons N le nombre de pièces d'or du butin. La première répartition donne $N = 17q + 3$ où q est le nombre de pièces d'or reçu par chacun des 17 pirates. Après la querelle, la seconde répartition donne $N = 6q' + 4$ où q' désigne le nombre de pièces d'or reçu par chacun des 6 pirates restants. Ces deux équations sont équivalentes à

$$\begin{cases} N \equiv 3 \pmod{17} \\ N \equiv 4 \pmod{6}. \end{cases}$$

On cherche à déterminer l'ensemble des solutions, puis la plus petite solution strictement positive (elle correspond à la fortune minimale que récupérerait le cuisinier s'il éliminait les pirates restants). Comme 17 et 6 sont premiers entre eux, on peut appliquer le théorème chinois et plus précisément la preuve du théorème 6.36. Une relation de Bézout entre 17 et 16 est $-17 + 3 \times 6 = 1$. L'entier relatif $x = 3 \times 18 + 4 \times (-17) = -14$ est donc solution du système. L'ensemble des solutions correspond à la classe de -14 modulo 17×6 c'est-à-dire à $\{-14 + 102\lambda \mid \lambda \in \mathbb{Z}\}$. La plus petite solution positive est donc $-14 + 102 = 88$.

Solution de l'exercice 6.13. La méthode est indiquée dans la remarque qui suit l'exemple 6.44. On applique l'algorithme d'Euclide :

$$\begin{aligned} 241 &= 21 \times 11 + 10 \\ 21 &= 2 \times 10 + 1 \\ 10 &= 10 \times 1 + 0. \end{aligned}$$

Donc $\text{pgcd}(241, 21) = 1$. En particulier, 21 est inversible modulo 241 d'après le théorème 6.43. En remontant les lignes de l'algorithme, on en déduit qu'une relation de Bézout est $1 = 23 \times 21 - 2 \times 241$. Donc $23 \times 21 \equiv 1 \pmod{241}$. L'inverse de 21 modulo 241 est 23.

Solution de l'exercice 6.14. Soit G le groupe $((\mathbb{Z}/9\mathbb{Z})^\times, \times)$.

1. D'après le théorème 6.43, les éléments de G sont les \bar{k} avec $1 \leq k \leq 9$ et $\text{pgcd}(k, 9) = 1$. Donc

$$G = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}.$$

En particulier G est d'ordre 6. En calculant les produits deux à deux de ces éléments, on obtient la table de Cayley de G (le groupe étant abélien, on ne remplit que la moitié supérieure du tableau) :

$((\mathbb{Z}/9\mathbb{Z})^\times, \times)$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{2}$		$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{5}$	$\bar{7}$
$\bar{4}$			$\bar{7}$	$\bar{2}$	$\bar{1}$	$\bar{5}$
$\bar{5}$				$\bar{7}$	$\bar{8}$	$\bar{4}$
$\bar{7}$					$\bar{4}$	$\bar{2}$
$\bar{8}$						$\bar{1}$

2. L'élément neutre $\bar{1}$ est d'ordre 1. On a

$$\begin{aligned}\bar{2} &\neq \bar{1}, \\ \bar{2}^2 &= \bar{4} \neq \bar{1}, \\ \bar{2}^3 &= \bar{8} \neq \bar{1}, \\ \bar{2}^4 &= \bar{7} \neq \bar{1}, \\ \bar{2}^5 &= \bar{5} \neq \bar{1}, \\ \bar{2}^6 &= \bar{1}\end{aligned}$$

donc $\bar{2}$ est d'ordre 6 dans $(\mathbb{Z}/9\mathbb{Z})^\times$. Des calculs similaires donnent

$$\text{ord}(\bar{4}) = 3, \text{ord}(\bar{5}) = 6, \text{ord}(\bar{7}) = 3, \text{ord}(\bar{8}) = 2.$$

Pour limiter la quantité de calcul, on peut aussi constater que $\bar{5} = \bar{2}^{-1}$ et $\bar{7} = \bar{4}^{-1}$ d'après la table de Cayley, et se rappeler que pour un élément g d'un groupe, $\text{ord}(g^{-1}) = \text{ord}(g)$ (voir exercice 3.4).

3. Le groupe possède un élément dont l'ordre est celui du groupe : par exemple $\bar{2}$, qui est d'ordre 6. Donc le groupe G est cyclique.

Remarque. Il existe des entiers n tels que le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ n'est pas cyclique (par exemple $n = 8$). Une caractérisation des entiers n pour lesquels le groupe est cyclique sera vue dans l'unité *Anneaux*.

Solution de l'exercice 6.15. Posons $f(x) = x^5 - x^2 + x - 3$ pour $x \in \mathbb{Z}$. Proposons deux méthodes de résolution.

1. Soit x une solution dans \mathbb{Z} de $f(x) = 0$. Alors $(x^4 - x + 1)x = 3$. Comme 3 est premier et x divise 3, on en déduit $x \in \{\pm 1, \pm 3\}$, ce qui donne quatre solutions éventuelles. On vérifie que ni 1, ni -1 , ni 3, ni -3 ne sont racines de f . Donc l'équation n'a aucune solution dans \mathbb{Z} .

2. Si l'équation a une solution x dans \mathbb{Z} alors $f(x) \equiv 0 \pmod{4}$ donc $\bar{x} = (x \pmod{4})$ est une solution de l'équation dans $\mathbb{Z}/4\mathbb{Z}$. Montrons que ce n'est pas le cas : on écrit par exemple $\mathbb{Z}/4\mathbb{Z} = \{\bar{-1}, \bar{0}, \bar{1}, \bar{2}\}$ et on a

$$\begin{aligned} (-1)^5 - (-1)^2 + (-1) - 3 &\equiv 2 \not\equiv \bar{0} \pmod{4}, \\ 0^5 - 0^2 + 0 - 3 &\equiv 1 \not\equiv \bar{0} \pmod{4} \\ 1^5 - 1^2 + 1 - 3 &\equiv 2 \not\equiv \bar{0} \pmod{4}, \\ 2^5 - 2^2 + 2 - 3 &\equiv -1 \not\equiv \bar{0} \pmod{4}. \end{aligned}$$

Donc l'équation n'a aucune solution dans \mathbb{Z} .

Solution de l'exercice 6.16. 1. D'après le cours, le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ est égal à $\varphi(n)$. Comme $56 = 2^3 \times 7$, en utilisant les propriétés de la fonction φ (à savoir $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont premiers entre eux, et $\varphi(p^r) = p^{r-1}(p-1)$ si p premier et $r \geq 1$), on en déduit :

$$\varphi(56) = \varphi(2^3)\varphi(7) = 2^2 \times (2-1) \times 6 = 24.$$

De même on a $504 = 2^3 \times 3^2 \times 7 = 56 \times 3^2$ et comme 56 et 3^2 sont premiers entre eux,

$$\varphi(504) = \varphi(56)\varphi(3^2) = 24 \times 3 \times 2 = 144.$$

2. Soit $n \geq 1$ tel que $\varphi(n)$ est impair. Rappelons la formule du cours

$$\varphi(n) = \prod_{p \in \mathbb{P}, p|n} p^{v_p(n)-1}(p-1).$$

Si n possède un diviseur premier impair p alors $\varphi(n)$ serait divisible par $p-1$, donc pair, ce qui est impossible. Cela montre que $n = 2^m$ avec $m \geq 0$. Si $m = 0$ alors $n = 1$ donc $\varphi(1) = 1$, qui est bien impair. Si $m \geq 1$ alors on peut écrire $\varphi(n) = 2^{m-1}(2-1) = 2^{m-1}$. Dans le cas où $m \geq 2$, l'entier $\varphi(n)$ serait pair, ce qui est à nouveau impossible. Si $m = 1$ alors $\varphi(n) = \varphi(2) = 1$, qui est bien impair. Donc les seuls entiers $n \geq 1$ pour lesquels $\varphi(n)$ est impair sont 1 et 2.

Solution de l'exercice 6.17. 1. Calculons le dernier chiffre en base 5 de 2018^{2017} . Cela revient à calculer $2018^{2017} \pmod{5}$. Comme $2018 \equiv 3 \pmod{5}$, cela revient à déterminer $3^{2017} \pmod{5}$. Or 3 et 5 sont premiers entre eux, donc le théorème d'Euler affirme que $3^{\varphi(5)} \equiv 1 \pmod{5}$ c'est-à-dire $3^4 \equiv 1 \pmod{5}$. On en déduit que, pour tout entier $a \in \mathbb{Z}$, $3^a \equiv 3^r$ où r désigne le reste de la division euclidienne de a par 4. On applique cela à $a = 2017$: son reste est 1 donc $3^{2017} \equiv 3^1 \equiv 3 \pmod{5}$. Le dernier chiffre cherché est 3.

Calculons les deux derniers chiffres de 2018^{2017} en base 10. Il s'agit de calculer $2018^{2017} \pmod{100}$ c'est-à-dire $18^{2017} \pmod{100}$. Noter qu'on ne peut pas appliquer le théorème d'Euler car 18 et 100 ne sont pas premiers entre eux. Cependant on a, modulo 100 : $18^2 \equiv 24$, $18^3 \equiv 32$, $18^4 \equiv 76$, $18^5 \equiv 68$ et $18^6 \equiv 24$. Une récurrence immédiate sur k donne $18^{2+4k} \equiv 24 \pmod{100}$

pour tout $k \geq 0$. Cherchons donc à écrire 2017 sous la forme $(2 + 4k) + \ell$ pour un petit entier ℓ . La division euclidienne de 2017 - 2 par 4 est $2017 - 2 = 503 \times 4 + 3$ d'où $2017 = (2 + 503 \times 4) + 3$. On obtient

$$18^{2017} \equiv 24 \times 18^3 \equiv 18^5 \equiv 68 \pmod{100}.$$

Les deux derniers chiffres recherchés sont 68.

- Il s'agit de calculer $79^{79^{79}} \pmod{100}$. Comme 79 et 100 sont premiers entre eux, le théorème d'Euler dit que $79^{\varphi(100)} \equiv 1 \pmod{100}$. Donc pour tout $a \in \mathbb{Z}$, on a $79^a \equiv 79^r \pmod{100}$ où r désigne le reste de la division euclidienne de a par $\varphi(100) (= 40)$. Or $79^{79} \equiv (-1)^{79} \equiv -1 \pmod{40}$. Donc $79^{79^{79}} \equiv 79^{-1} \pmod{100}$. De plus une relation de Bézout entre 100 et 79 est $(-15) \times 100 + 19 \times 79 = 1$ d'où $79^{-1} \equiv 19 \pmod{100}$. Les deux derniers chiffres recherchés sont 19.

Solution de l'exercice 6.18. 1. Si m n'est pas une puissance de 2 alors $m = 2^\ell q$ avec $\ell \geq 0$, q impair et $q \geq 3$. On en déduit, à l'aide d'une identité remarquable de type $a^n - b^n$,

$$2^m + 1 = (2^{2^\ell})^q - (-1)^q = (2^{2^\ell} + 1)(2^{2^\ell(q-1)} + \dots - 1).$$

Dans cette expression, $2^{2^\ell} + 1$ est un diviseur strict de $2^m + 1$. Donc si $2^m + 1$ est premier alors m est une puissance de 2.

- Posons $F_n = 2^{2^n} + 1$ pour tout $n \in \mathbb{N}$. Montrons par récurrence sur n que

$$\prod_{k=0}^{n-1} F_k = F_n - 2.$$

On a $F_0 = 3$ et $F_1 = 5$ donc $F_0 = F_1 - 2$. Supposons la propriété vraie au rang $n - 1$. On a alors

$$F_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) = (F_{n-1} - 2)F_{n-1}$$

d'où $F_n - 2 = \prod_{k=0}^{n-1} F_k$ en utilisant l'hypothèse de récurrence. Cela démontre la formule annoncée.

- Soit $m > n$. Supposons qu'il existe un nombre premier p divisant F_m et F_n . Alors p divise $\prod_{k=0}^{m-1} F_k$ donc divise $F_m - 2$. On en déduit que p divise 2. Or les nombres de Fermat sont clairement impairs. Donc le nombre premier p n'existe pas. Cela prouve que F_n et F_m sont premiers entre eux.
- Soit p_n le plus petit nombre premier divisant F_n . Alors la question précédente entraîne que les p_n sont deux à deux distincts. La suite $(p_n)_{n \in \mathbb{N}}$ est donc une suite infinie de nombres premiers.
- Soit p un nombre premier divisant F_n . Alors on a $2^{2^n} \equiv -1 \pmod{p}$ donc $2^{2^{n+1}} \equiv 1 \pmod{p}$. On en déduit que l'ordre de 2 dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ divise 2^{n+1} . Puisque $2^{2^n} \equiv -1 \pmod{p}$, cet ordre est exactement 2^{n+1} . Or par le théorème de Lagrange, cet ordre divise l'ordre du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$, qui vaut $\varphi(p) = p - 1$. On en déduit que $p - 1 = 2^{n+1}k$ pour un certain $k \in \mathbb{N}$.

Solution de l'exercice 6.19. 1. Soit

$$B = \{b \in \mathbb{N} \mid \forall a \in \mathbb{N}, s(a) + b = s(a + b)\}.$$

Montrons que $B = \mathbb{N}$ en utilisant le principe de récurrence. On a $0 \in B$: en effet, tout a dans \mathbb{N} vérifie $s(a) + 0 = s(a) = s(a + 0)$ par définition de $+$. Soit $b \in B$ et montrons que $s(b) \in B$. Par définition de $+$, on a pour tout $a \in \mathbb{N}$: $s(a) + s(b) = s(s(a) + b)$. Comme $b \in B$, on a par ailleurs $s(a) + b = s(a + b) = a + s(b)$, par définition de $+$. On en déduit $s(a) + s(b) = s(a + s(b))$ d'où $s(b) \in B$, ce qui conclut.

2. Fixons b et c dans \mathbb{N} . Posons $A = \{a \in \mathbb{N} \mid a + b = a + c \implies b = c\}$. Prouvons $A = \mathbb{N}$ en utilisant le principe de récurrence. On a $0 \in A$: en effet, par définition de $+$, on a $0 + b = 0 + c \implies b = c$. Soit $a \in A$ et montrons que $s(a) \in A$. Comme on a déjà montré la commutativité de $+$ (troisième point de la proposition 6.56), on peut écrire : $s(a) + b = b + s(a)$ puis, par définition de $+$, on a $b + s(a) = s(b + a)$. De même on a $s(a) + c = c + s(a) = s(c + a)$. Supposons maintenant $s(a) + b = s(a) + c$. Alors on a $s(b + a) = s(c + a)$ ce qui entraîne, par injectivité de s (deuxième axiome de Peano), $b + a = c + a$. Comme $a \in A$, on en déduit $b = c$. On a ainsi prouvé $s(a) + b = s(a) + c \implies b = c$ i.e. $s(a) \in A$. Cela conclut la preuve.

Solution de l'exercice 6.20. 1. Soit $\mathcal{P}(n)$ une propriété de l'entier $n \in \mathbb{N} - \{0\}$ telle que $\mathcal{P}(1)$ est vraie et, pour tout $n \in \mathbb{N}$, $\mathcal{P}(n)$ implique $\mathcal{P}(n + 1)$. Considérons le sous-ensemble

$$A = \{n \in \mathbb{N} - \{0\} \mid \mathcal{P}(n) \text{ est vraie}\} \cup \{0\}$$

de \mathbb{N} . Montrons que $A = \mathbb{N}$ en utilisant le principe de récurrence. On a évidemment $0 \in A$. De plus si $n \in A$ alors $s(n) = n + 1 \in A$: en effet c'est vrai si $n = 0$ car $\mathcal{P}(1)$ est vraie, et c'est vrai pour tout $n \neq 0$ car, par hypothèse, $\mathcal{P}(n)$ implique $\mathcal{P}(n + 1)$. On a donc $A = \mathbb{N}$. Il vient que l'ensemble $\{n \in \mathbb{N} - \{0\} \mid \mathcal{P}(n) \text{ est vraie}\}$ est égal à $\mathbb{N} - \{0\}$, ce qu'on voulait montrer.

2. Pour $n \in \mathbb{N} - \{0\}$, considérons la propriété suivante notée $\mathcal{P}(n)$: toute partie non vide finie de \mathbb{N} de cardinal n possède un plus grand élément. Montrons que pour tout n , $\mathcal{P}(n)$ est vraie en utilisant la forme de récurrence établie à la question précédente. Pour $n = 1$, toute partie de \mathbb{N} de cardinal 1 a un unique élément, qui est bien le plus grand. Supposons $\mathcal{P}(n)$ vraie. Soit A une partie finie de \mathbb{N} de cardinal $n + 1$. Alors A possède un plus petit élément, noté a , d'après la première partie du théorème 6.63. Posons $B = A - \{a\}$. C'est une partie de \mathbb{N} de cardinal n donc B admet un plus grand élément b . C'est aussi le plus grand élément de A . Donc la propriété $\mathcal{P}(n + 1)$ est vraie. Par récurrence, nous avons donc montré que toute partie non vide finie de \mathbb{N} possède un plus grand élément.