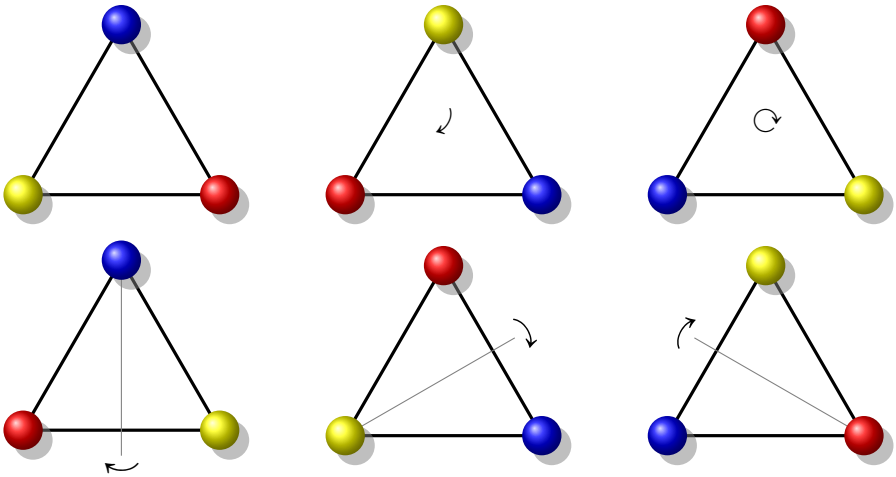
MAT 2250
Introduction à la théorie des groupes

(à partir de notes de Luc Bélair et Christophe Hohlweg)

François Bergeron

13 décembre 2015



UQÀM **Université du Québec à Montréal**
Département de mathématiques
Case postale 8888, Succursale Centre-Ville
Montréal (Québec) H3C 3P8

Table des matières

Page

Table des Figures **8**

Avant-propos **9**

1 Groupes **11**
1.1 Introduction à la notion de groupe . . . 11
1.2 Définition de groupes . . . 14
1.3 Exemples classiques . . . 18
1.4 Table de multiplication d'un groupe . . . 21
1.5 Règles de calcul . . . 22
1.6 Sous-groupes . . . 24
1.7 Ordre d'un groupe, ordre d'un élément . . . 27
1.8 Le groupe symétrique S_n . . . 31
1.9 Groupes engendrés par des réflexions . . . 37
1.10 Un groupe à la Galois . . . 38
1.11 Exercices . . . 40

2 Actions de groupes **49**
2.1 Groupes opérants sur des ensembles . . . 50
2.2 Actions de S_E . . . 54
2.3 Classes modulo un sous-groupe . . . 56
2.4 Orbites vs stabilisateurs . . . 59
2.5 Lemme de Burnside . . . 61
2.6 Morphismes d'actions, sommes d'actions, et actions transitives. . . . 63
2.7 Le système de cryptographie RSA . . . 66
2.8 Le groupe des isométries du cube . . . 69
2.9 Espaces homogènes . . . 72

2.10 Le groupe $\mathrm{SL}_2(\mathbb{Z})$ . . . 72
2.11 Actions linéaires . . . 75
2.12 Exercices . . . 78

3 Morphismes de groupes **83**
3.1 Définition . . . 83
3.2 Noyau d'un morphisme de groupes . . . 85
3.3 Isomorphismes de groupes . . . 87
3.4 Automorphismes intérieurs . . . 88
3.5 Théorème de Cayley . . . 88
3.6 Actions et morphismes de groupes . . . 90
3.7 Tous les groupes finis . . . 91
3.8 Exercices . . . 92

4 Groupes quotients et théorème d'isomorphie **97**
4.1 Groupes quotients . . . 97
4.2 Théorème d'isomorphisme . . . 99
4.3 Présentations (finies) de groupes . . . 101
4.4 Sous-groupes d'un groupe quotient . . . 102
4.5 Groupes monogènes et cycliques . . . 103
4.6 A_5 comme groupe des rotations du dodécaèdre . . . 105
4.7 Groupes résolubles . . . 108
4.8 Exercices . . . 108

5 Produits de groupes **113**
5.1 Le produit direct . . . 113
5.2 Le produit direct interne . . . 115
5.3 Produits semi-directs . . . 117
5.4 Exercices . . . 119

6 Groupes abéliens finis **121**
6.1 Groupes cycliques . . . 121
6.2 Groupes abéliens primaires . . . 122
6.3 Décomposition primaire . . . 123
6.4 Théorème principal . . . 127
6.5 Exercices . . . 128

7 Les p-groupes, et théorèmes de Sylow **129**
7.1 Les p-groupes . . . 129
7.2 Théorèmes de Sylow . . . 130

7.3 Exercices 132

A Théorie des groupes avec le calcul formel **135**

B Rappels sur les ensembles et fonctions **137**

Solutions de certains exercices **141**

Bibliographie commentée **157**

Index **161**

Table des figures

1.1 Symétries d'un triangle équilatéral . . . 12
1.2 Cube de Rubik . . . 12
1.3 Retournements de matelas. . . . 13
1.4 Forme de la molécule C_{60} . . . 14
1.5 Table de multiplication . . . 22
1.6 Permutoèdre. . . . 26
1.7 Deux graphes de Cayley pour S_3. . . . 27
1.8 Composition de permutations . . . 32
1.9 Un cycle. . . . 34
1.10 Décomposition en cycles disjoints . . . 36
1.11 Arrangement d'hyperplans dans $\mathbb{R}_3$, correspondant à S_4 . . . 37
1.12 Réflexions et arrangement de droites . . . 38

2.1 Orbites dans $\mathbb{C}$ pour les translations et rotations . . . 52
2.2 Colorations du tétraèdre . . . 62
2.3 Treillis des sous-groupes de S_4 . . . 65
2.4 Rotations du cube. . . . 69
2.5 Pavage du plan hyperbolique . . . 74
2.6 Portion de pavage de $\mathbb{R}^3$ par le permutoèdre. . . . 82

3.1 Isomorphisme entre les symétries du triangle et S_3. . . . 85
3.2 Graphe de Cayley de A_5 . . . 86

4.1 Graphe de Cayley du groupe libre . . . 101
4.2 Les cinq cubes inscrits dans le dodécaèdre. . . . 105
4.3 Rotation du dodécaèdre . . . 105
4.4 Version réaliste d'un cube inscrit dans le dodécaèdre. . . . 106
4.5 Permutation des 5 cubes d'un dodécaèdre . . . 107

5.1 Graphe de Cayley de $\mathbb{Z}_3 \times \mathbb{Z}_3$. . . . 114

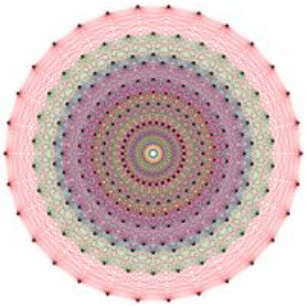
5.2 L'octaèdre. 118

Avant-propos

Ce recueil est en cours d'amélioration. Il est bien de consulter la page internet du cours pour les mises à jour. On remercie d'avance ceux qui prendront la peine de signaler les erreurs de toute nature. La version électronique est dynamique, avec des liens vers plusieurs ressources externes. En particulier, pour les quelques figures ou images provenant d'autres sources, un lien permet de retrouver cette source. Dans tous ces cas, les images sont du domaine public. Les notes contiennent aussi parfois des allusions à des sujets plus avancés, ou externes au cours. Lorsque cela est possible, il y a aussi des liens vers des pages qui expliquent (en partie) ces notions.

Chapitre 1

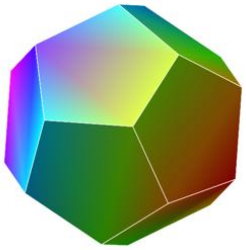
Groupes



La notion de groupe joue un rôle fondamental en mathématiques. C'est l'une des principales structures algébriques, avec celles d'anneau, de corps, modules, et espaces vectoriels. D'une part, elle formalise les propriétés de plusieurs des opérations bien connues entre des objets mathématiques divers comme les : nombres, vecteurs, matrices, fonctions, etc. D'autre part, elle donne un contexte clair pour discuter de transformations de toutes sortes : rotations, translations, symétries, etc. ; ou encore de manipulations d'objets. Elle est essentielle pour comprendre des aspects fondamentaux de la physique (théorie de la relativité, théorie des quantas), de la chimie (calcul des isomères), de la cristallographie (symétries des cristaux), de la cryptographie à clé publique (système RSA, courbes elliptiques), et de l'étude des codes correcteurs d'erreurs. Elle joue aussi un rôle fondamental en théorie de Galois [1] (qui étudie la résolution d'équations polynomiales), en théorie des nombres, en géométrie, et dans la théorie des invariants. Bref, c'est l'une des notions les plus intéressantes parmi celles élaborées par les mathématiciens.

1.1 Introduction à la notion de groupe

Souvent, un groupe décrit les transformations possibles d'un objet, ou les manipulations qu'on peut faire sur un objet. On suppose qu'appliquer à l'objet considéré une suite de transformations successives est aussi une transformation. On dira alors qu'on a « composé » les transformations pour en produire une nouvelle. On suppose aussi que défaire une transformation est une transformation. On dira que c'est



Le dodécaèdre.

1. Due à Évariste Galois, 1811-1832.

à la transformation « inverse ». Le groupe est l'ensemble des transformations possible. Pour fixer les idées, on considère par exemple les diverses rotations du dodécaèdre (voir figure ci-contre), ou encore les symétries possibles d'un triangle équilatéral, comme l'illustre la figure 1.1. On constate qu'il y a 3 manières de faire effectuer une symétrie de rotation du triangle, et 3 symétries axiales (de réflexions).

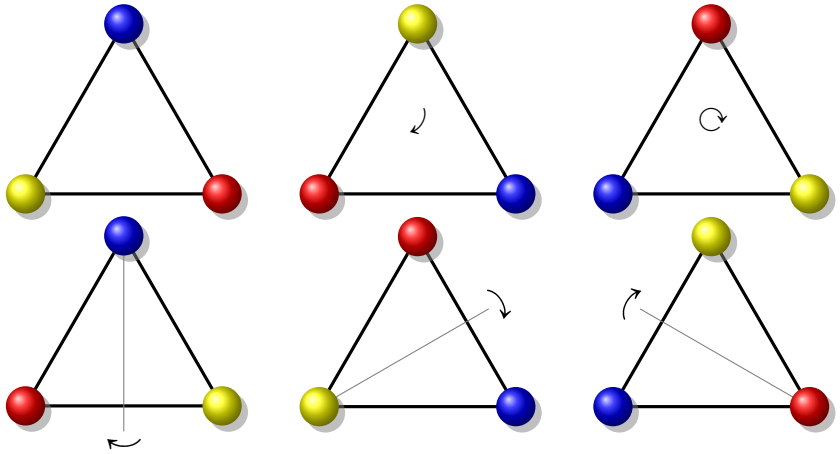


FIGURE 1.1 – Les symétries d'un triangle équilatéral.

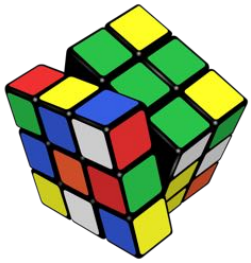


FIGURE 1.2 – Le Cube de Rubik.

Comme nous allons le voir dans ce cours, le fait d'en comprendre les transformations possibles permet de mieux saisir le rôle d'un objet, et d'en dégager les propriétés essentielles. Pour illustrer le sens de cette affirmation, considérons le fameux casse-tête qu'est le Cube de Rubik. Les mouvements possibles consistent à faire tourner une des 6 « faces » du cube de 90°, comme l'illustre la figure ci-contre. L'objectif est de ramener le cube à son état original (à savoir celui où les faces sont toutes d'une couleur uniforme), par une succession de tels mouvements. Dans ce contexte, on considère donc le « groupe » de toutes les suites possibles de rotation des faces. Comprendre ce groupe permet de comprendre comment résoudre le cube. Grâce à la théorie des groupes, on peut calculer [2] qu'il y a

$$(3^8 \times 2^{12} \times 12! \times 8!)/12 = 43252003274489856000$$

états (positions) possibles du cube, dont une seule est la bonne (la solution). Lorsqu'on manipule le cube, on s'aperçoit rapidement que le résoudre n'est pas facile. Par essai et erreur, on découvre (assez) vite comment rendre une des faces à son état de couleur uniforme ; puis, un peu moins rapidement, comment s'approcher de la solution. Malheureusement, quand on en est tout proche, on s'aperçoit qu'il

2. La théorie aide à trouver la bonne formule.

faut revenir en arrière (et défaire en partie ce que l'on a fait) pour arriver à la solution. C'est alors loin d'être évident.

Heureusement, si on la connaît, la théorie des groupes permet d'organiser les étapes nécessaires. Donc, en un certain sens, le problème du Cube de Rubik est un problème de théorie des groupes appliquée. La manipulation du Cube permet d'illustrer beaucoup des concepts de base de la théorie. Même à la maison, la théorie des groupes trouve application. Dans un article du New York Times, on décrit (sourire en coin) les diverses manières de retourner un matelas grâce à la théorie des groupes pour en éviter la déformation. On considère d'abord que les coins du matelas sont étiquetés comme l'illustre la figure ci-contre[3]. Il y a trois manipulations possibles du matelas, illustrées à la figure 1.3.

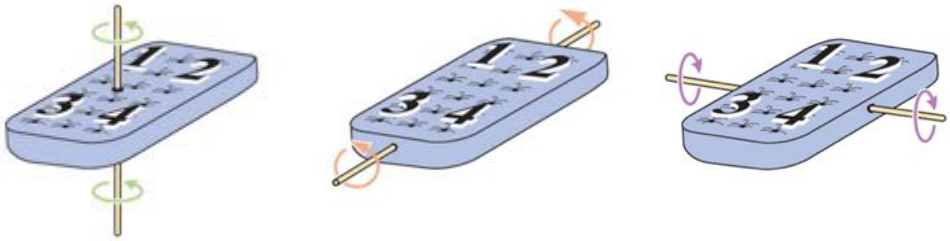
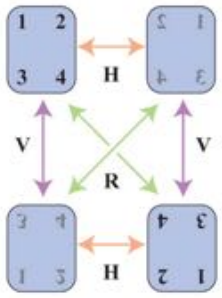


FIGURE 1.3 – Retournements de matelas.

Le matelas peut se retrouver dans l'un de quatre états, illustrés à la figure ci-contre, avec les diverses manipulations qui permettent de passer d'un état à l'autre. En un certain sens aussi, il y a une grande analogie avec la physique mathématique. Pour comprendre un objet physique (ou un phénomène), la clé consiste à comprendre le groupe des transformations de cet objet. Par exemple, dans la découverte du « buckminsterfullerène[4] », une molécule constituée de 60 atomes de carbone assemblés comme l'indique la figure 1.1, la théorie des groupes à permis de calculer le spectre de cette molécule avant même qu'on en ait trouvé des exemples dans la nature (autant sur Terre que dans l'espace). Cela détermine quelles sont les notions qu'on peut utiliser pour formuler les lois de la physique qui régissent le comportement de cet objet (ou phénomène). La théorie des groupes est donc cruciale pour dégager les théories de la physique. Ainsi, les lois de la relativité générale, les équations de Maxwell, et



États et transitions pour le matelas.

3. Les figures sont celles du New York Times
4. Ainsi appelé en l'honneur de Richard Buckminster Fuller (1895–1983), le concepteur de la biosphère.

les équations de Dirac décrivant les propriétés des électrons sont « invariantes » pour les transformations du groupe de Lorentz[5]. Grâce à ce fait, on peut fortement circonscrire leur formulation. Voilà pourquoi plusieurs livres de la physique moderne amorcent leurs exposés avec la théorie des groupes.

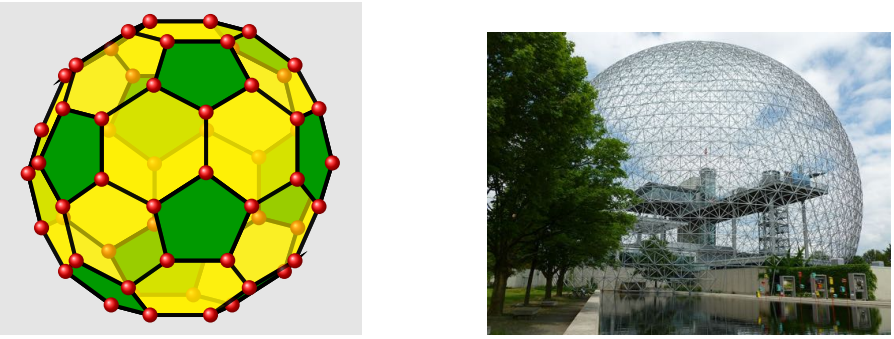
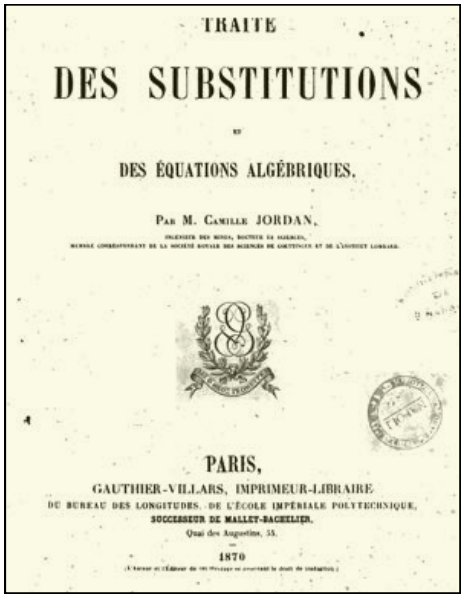


FIGURE 1.4 – Forme de la molécule C_{60}, la buckminsterfullerène, et la biosphère.

1.2 Définition de groupes


TRAITÉ

DES SUBSTITUTIONS

ET

DES ÉQUATIONS ALGÉBRIQUES,

PAR M. CAMILLE JORDAN,

PARIS,

GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE

DU BUREAU DES LONGITUDES, DE L'ÉCOLE IMPÉRIALE POLYTECHNIQUE,

SUCCESSEUR DE MALLET-BACHELIER,

1870

La théorie des groupes est née de la convergence de plusieurs domaines : théorie des nombres, géométrie, résolution d'équations algébriques, etc. Elle s'est dégagée dans la seconde moitié du 19e siècle. C'est à Galois qu'on doit le terme « groupe », qu'il a utilisé un peu au sens de « regroupement » pour des transformations. On s'est ensuite aperçu qu'elle permettait d'unifier plusieurs notions considérées à l'époque, pour autant qu'on en isole les propriétés correctement. On trouve beaucoup des notions modernes sur les groupes dans le *Traité des substitutions et des équations algébriques* publié en 1870 par Jordan[6]. Abstraitement donc, un groupe est simplement un ensemble muni d'une opération avec de bonnes propriétés. Dans un premier temps, nous allons en donner une description précise, pour ensuite donner corps à la notion en présentant une famille d'exemples typiques. En ce sens, on procède donc à l'inverse de ce qui s'est produit historiquement.

5. Hendrik Lorentz, (1853-1928). Pour plus de détails, voir groupe de Lorentz.
6. Camille Jordan, (1838-1922).

Loi de composition, ou opération. Pour la suite, on suppose que E est un ensemble non vide. On dit d'une fonction $* : E \times E \to E$ que c'est une **loi de composition** sur E, ou une **opération binaire** sur E. On note $(E, *)$ le fait que l'ensemble E est muni d'une opération binaire. Dans ce cas, on utilise souvent une notation **infixe**, c'est-à-dire que

$$* : E \times E \longrightarrow E, \qquad \text{avec} \qquad (x, y) \longmapsto x * y,$$

où l'image de (x, y) par la fonction « $*$ » est notée $x * y$.

Parmi les lois de composition, certaines possèdent des propriétés particulières qui les rendent plus intéressantes. Le choix de ces propriétés n'est pas arbitraire. En effet, c'est une vaste expérience mathématique qui a permis de dégager qu'elles sont les propriétés qui donnent à une loi de composition une structure suffisamment riche pour qu'elle ait un impact important sur l'étude d'un contexte dans lequel elle apparaît. Nous aurons maintes fois l'occasion de constater qu'une fois mises en évidence ces propriétés apparaissent toutes naturelles. On dit d'une loi de composition (opération) $*$, qu'elle est

(1) **associative** si $x * (y * z) = (x * y) * z$, pour tout $x, y, z \in E$.

(2) **commutative** si $x * y = y * x$ pour tout $x, y \in E$.

On remarque que, si $*$ est associative, alors on peut écrire $x * y * z$ au lieu de $(x * y) * z = (x * y) * z$, puisqu'il n'y a pas d'ambiguïté sur la façon de faire le calcul. Bien entendu, toutes les lois ne sont pas associatives.

Exemples. Par exemple, on a

(a) Les opérations usuelles d'addition « $+$ » et de multiplication « $\cdot$ » d'entiers (dans $\mathbb{Z}$) sont toutes deux commutatives et associatives. Il en est de même pour les entiers modulo n, c.-à-d. dans $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Dans ce qui suit, on suppose que l'ensemble $\mathbb{Z}_n$ est identifié [7] à $\{0, 1, \ldots, n\}$.

(b) La loi de composition $\star : (x, y) \mapsto xy + 1$ sur $\mathbb{N}$ est commutative, mais pas associative. En effet, pour $x, y, z \in \mathbb{N}$, on a

$$\begin{aligned} (x \star y) \star z &= (xy + 1) \star z = (xy + 1)z + 1 = xyz + z + 1, \quad \text{et} \\ x \star (y \star z) &= x \star (yz + 1) = x(yz + 1) = xyz + x + 1. \end{aligned}$$

Les résultats sont donc sont manifestement différent si $x \neq z$.

(c) On vérifie facilement que l'opération $x \star y := x^y$, pour x et y dans $\mathbb{N}$, n'est ni associative ni commutative.

(d) Dans l'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices $n \times n$ à coefficients réels, l'addition est une loi associative et commutative, tandis que la multiplication est une loi associative, mais pas commutative en général (voir Exercice 1.16).

7. C'est un léger abus de langage qui sera rediscuté au Chapitre 4.

Pour une opération $*$ sur E, et $A \subseteq E$, on dit que l'ensemble A est **stable** pour $*$, si pour tout $x, y \in A$ on a $x * y \in A$. On dit parfois que A **hérite** de l'opération [8] de E. Autrement dit, $*$ est aussi une opération sur A car la fonction

$$* : A \times A \longrightarrow A, \qquad \text{avec} \qquad (x, y) \longmapsto x * y$$

est bien définie. On peut donc considérer la structure algébrique $(A, *)$. L'associativité est **héréditaire**, c.-à-d.que si $*$ est associative dans E, et A est stable pour $*$, alors $*$ restreint à A est aussi associative. En effet, l'égalité $x * (y * z) = (x * y) * z$ est vraie pour tout $x, y, z \in E$, donc en particulier pour tout $x, y, z \in A$ sous-ensemble de E. On constate de la même manière que la commutativité est **héréditaire**. Nous aurons plusieurs exemples de cette situation dans ce qui suit. Considéré comme sous-ensemble de $\mathbb{Z}$, l'ensemble $\mathbb{Z}^*$ (des entiers non nuls) est stable pour la multiplication, mais $\mathbb{Z}^*$ n'est pas stable pour l'addition, puisqu'on observe que $1 + (-1) = 0 \notin \mathbb{Z}^*$.

Élément neutre, et monoïdes. Tout comme c'est le cas de 1 pour la multiplication usuelle, ou de 0 pour l'addition, plusieurs opérations admettent des « éléments neutres ». Plus généralement, pour $*$ une opération sur E, on dit que $(E, *)$ possède un **élément neutre** s'il existe un élément $e \in E$, tel que $x * e = e * x = x$ pour tout $x \in E$; . Un **monoïde** est un couple $(E, *)$, où $*$ est une opération associative qui admet un élément neutre. Un monoïde est dit **commutatif**, si l'opération est de plus commutative. Si $(E, *)$ possède un élément neutre e, alors cet élément neutre est **unique**. En effet, soit e et e' deux candidats, alors $e = e * e' = e' * e = e'$, et donc e et e' coïncident forcément. Il est clair que si $A \subseteq E$ est stable pour $*$ et $e \in A$, alors e est élément neutre pour $(A, *)$. Dès la petite école on apprend que les opérations de $(\mathbb{Z}, +)$ et $(\mathbb{Q}, \cdot)$ sont commutatives. En algèbre linéaire on est confronté (souvent pour la première fois) à une opération non commutative : la multiplication de matrices.

Éléments inversibles, et groupes. Une autre façon de concevoir la division de nombres x/y (resp. la soustraction $x - y$) et de penser qu'elle correspond à la multiplication de x par « l'inverse » multiplicatif $1/y$, de y (resp. l'addition de l'inverse additif $-y$). Cette approche est plus naturelle lorsqu'on cherche à généraliser, et on en arrive à la définition suivante. On dit que $x \in E$ est **inversible** dans $(E, *)$ s'il existe $y \in E$ tel que $x * y = y * x = e$. Dans $(\mathbb{Z}, +)$, l'inverse de x est $-x$. Dans $(\mathbb{Q}^*, \cdot)$, l'inverse de x est $1/x$. Dans un premier cours d'algèbre linéaire, on montre qu'une matrice $n \times n$ réelle est inversible pour la multiplication de matrices, si et seulement si son déterminant est non nul. On désigne habituellement par $\mathrm{GL}_n(\mathbb{R})$ l'ensemble des matrices réelles de déterminant non nul.

Nous sommes maintenant prêts à donner une définition précise de la notion de groupe. On dit que $(E, *)$ est **un groupe** si $(E, *)$ est un monoïde, et si tous les éléments de E sont inversibles. Un groupe $(E, *)$ est dit **abélien** [9], ou **commutatif**, si de plus l'opération $*$ est commutative. Par exemple, $(\mathbb{Z}, +)$ et $(\mathbb{Q}^*, \cdot)$ sont des groupes abéliens, mais $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ ne l'est pas.

8. Rigoureusement parlant, on devrait dénoter $\star|_{A \times A}$ la restriction de $\star$ à A, mais il n'y a pas risque de confusion.
9. Du mathématicien norvégien Niels H. Abel (1802-1829).

Notre définition de groupe est naturelle, mais légèrement redondante. Pour simplifier le travail de vérification qu'on a bien un groupe $(G, \star)$, il est parfois utile de la reformuler un peu. De façon équivalente, on constate que $(G, *)$ est un aussi groupe si et seulement si

(1) $*$ est associative ;

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

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

L'implication directe est une conséquence immédiate des définitions. Supposons maintenant que $(G, *)$ vérifie les trois conditions susmentionnées. Comme on sait déjà que $*$ est associative, il suffit de vérifier que $(G, *)$ possède un élément neutre (à droite autant qu'à gauche), et que tout élément de G est inversible (aussi à droite autant qu'à gauche). Par hypothèse, chaque $x \in G$ admet un inverse à gauche $y \in G$. Reste à vérifier que $x * y = e$. Or, comme $y \in G$, il existe également $z \in G$ tel que $z * y = e$. On calcule alors que

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

ce qui donne la propriété désirée. De façon très semblable, pour voir que e (l'élément neutre à gauche) est aussi élément neutre à droite, on calcule comme suit. Pour $x \in G$, on sait maintenant qu'il existe $y \in G$ tel que $y * x = x * y = e$, et on calcule que

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

On observe que dans tout monoïde $(E, *)$, où l'élément neutre est noté e, l'inverse d'un élément, s'il existe, est **unique**. En effet, pour $x \in E$, si $y, y' \in E$ deux inverses potentiels, alors

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

Il sont donc forcément égaux. On peut donc parler de **l'inverse**[10] de x, et on le note $\widetilde{x}$. On vérifie facilement (voir Exercice 1.3) que

$$\widetilde{\widetilde{x}} = x, \qquad \text{et} \qquad \widetilde{e} = e. \tag{1.1}$$

On dénote par $E^\times$ **l'ensemble des éléments inversibles** de E :

$$E^\times := \{x \in E \,|\, x \text{ est inversible}\}. \tag{1.2}$$

La proposition suivante fournit un outil général pour « construire » des groupes.

Proposition 1.1. *Si $(E, *)$ est un monoïde, alors $(E^\times, *)$ est un groupe dont l'élément neutre est e. De plus, $\widetilde{x * y} = \widetilde{y} * \widetilde{x}$.*

Démonstration. Il faut montrer que

10. La subtilité réside dans l'utilisation du « l »-apostrophe, qui souligne l'unicité.

(1) $*$ est une opération sur $E^\times$; en d'autres termes, que $E^\times$ est stable pour $*$;

(2) $(E, *)$ est un monoïde d'élément neutre e ;

(3) Tout élément de $E^\times$ est inversible.

Montrons d'abord (1). Il suffit de vérifier que si x, y sont inversibles dans E, alors $x * y$ l'est aussi dans E. On a

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

Donc $x * y$ est inversible et son inverse est $\widetilde{y} * \widetilde{x}$. En particulier, comme $\widetilde{x * y}$ est aussi inversible dans $E^\times$ (d'inverse $x * y$), tout élément de $E^\times$ est inversible, ce qui montre (iii).

Montrons maintenant (2). On sait que $E^\times$ est stable pour $*$ donc par hérédité, $*$ est associative sur $E^\times$. Puisque $\widetilde{e} = e$ car $e * e = e$, alors $e \in E^\times$ et donc $(E^\times, *)$ est un monoïde. ■

Un monoïde $(E, *)$ est donc un groupe si et seulement si $E = E^\times$.

Notation additive et multiplicative des groupes. Les **conventions** suivantes sont d'une utilisation généralisée, et pratique si on en comprend bien le sens. Cependant, elles mènent parfois à la confusion si on en ignore la portée. Lorsque le contexte est clair, on dit souvent que G est un « groupe » (sans mentionner l'opération), au lieu de $(G, \cdot)$. Sauf mention contraire, on note habituellement les opérations de groupes **multiplicativement** : $(x, y) \mapsto xy$, et on dit que ce sont des **produits**[11]. De plus, on écrit $x^{-1} = \widetilde{x}$ pour l'inverse de $x \in G$, et l'élément neutre est noté 1, ou 1_G. Dans le cas spécial où le groupe $(G, *)$ est un groupe abélien, on note plutôt l'opération additivement : $(x, y) \mapsto x + y$, et on dit que ce sont des **sommes**. On écrit alors $-x = \widetilde{x}$ pour l'inverse de $x \in G$, appelé aussi **opposé** de x, et l'élément neutre est noté 0, ou 0_G.

1.3 Exemples classiques

Les exemples classiques suivants (certains déjà mentionnés) apparaissent naturellement dans divers contextes des mathématiques. Leur variété souligne l'importance de la notion de groupe. Évidemment, les premiers exemples sont les plus simples.

L'addition de nombres. L'addition de nombres complexes $(a, b) \mapsto a + b$ est une loi de composition sur $\mathbb{C}$, et $(\mathbb{C}, +)$ est un groupe abélien d'élément neutre 0. De même

(a) $(\mathbb{N}, +)$, $(\mathbb{Z}^-, +)$, $(\mathbb{Q}^+, +)$, $(\mathbb{R}^-, +)$ et $(\mathbb{R}^+, +)$ sont des monoïdes commutatifs. En effet, ces sous-ensembles sont stables pour $+$, et ils héritent donc de l'associativité et de la commutativité.

11. Bien que la plupart du temps ce ne sont pas des produits usuels.

Cependant tous leurs éléments ne sont pas inversibles. Observons que l'opposé de 2 n'existe pas dans $(\mathbb{N}, +)$, ni $(\mathbb{Q}^+, +)$, ni dans $(\mathbb{R}^+, +)$;

(b) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sont des groupes : il est clair que ce sont des monoïdes, où tous les éléments ont des opposés ;

(c) Les ensembles $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, et $\mathbb{C}^*$ (dans chaque cas privé de 0) ne sont pas stables pour $+$, puisque (par exemple) $1 + (-1) = 0$ n'appartient à aucun de ces ensembles ;

(d) Pour tout $n \in \mathbb{N}$, on a que $(n\mathbb{Z}, +)$ est un groupe. En effet, on peut restreindre l'addition à $n\mathbb{Z}$ puisque $n\mathbb{Z}$ est stable pour l'addition. De plus, $0 \in n\mathbb{Z}$, et donc $(n\mathbb{Z}, +)$ est un monoïde. Enfin, $nk \in n\mathbb{Z}$ est inversible dans $n\mathbb{Z}$, car son opposé est $n(-k) \in n\mathbb{Z}$.

La multiplication de nombres. *La multiplication de nombres complexes* $(a, b) \mapsto ab$ est une loi de composition sur $\mathbb{C}$, et $(\mathbb{C}, \cdot)$ est un monoïde commutatif. Par ailleurs, puisque $\mathbb{C}^\times = \mathbb{C}^*$, on a le groupe abélien $(\mathbb{C}^*, \cdot)$, d'élément neutre 1. De plus,

(a) $(\mathbb{N}^*, \cdot)$ et $(\mathbb{Z}^*, \cdot)$ sont des monoïdes commutatifs, puisque les sous-ensembles correspondants sont stables pour $\cdot$. Ils héritent donc de l'associativité et de la commutativité. Cependant, tous leurs éléments ne sont pas inversibles. Par exemple, l'inverse de 2 n'existe pas, ni dans $\mathbb{N}$, ni dans $\mathbb{Z}$.

(b) $(\mathbb{Q}^*, \cdot)$ et $(\mathbb{R}^*, \cdot)$ sont des groupes. Puisque ce sont des sous-ensembles stables de $\mathbb{C}^*$, il est clair que ce sont des monoïdes. De plus, tous les éléments sont inversibles.

(c) $\mathbb{Z}^-$ n'est pas stable pour « $\cdot$ ». En effet, le produit de deux nombres négatifs est positif.

(d) pour $n \in \mathbb{N}^*$, on a que $(n\mathbb{Z}, \cdot)$ est un monoïde si et seulement si $n = 1$. En effet, on peut vérifier directement que $n\mathbb{Z}$ est stable pour la multiplication. Cependant, $1 \in n\mathbb{Z}$ si et seulement si $n = 1$.

Algèbre linéaire. Tout espace vectoriel est un groupe abélien pour l'addition de vecteurs (voir Exercice 1.6). De plus, pour $n \in \mathbb{N}$ on constate que

(a) $(\mathcal{M}_n(\mathbb{R}), +)$ est un groupe abélien ;

(b) $(\mathcal{M}_n(\mathbb{R}), \cdot)$ est un monoïde (non commutatif) dont l'élément neutre est la matrice identité I_n.

(c) Dans $(\mathcal{M}_n(\mathbb{R}), \cdot)$, l'ensemble des inversibles est

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

En vertu de la proposition 1.1, $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ est un groupe. On l'appelle le **groupe linéaire**. Il est non abélien si $n > 1$. De plus, $(AB)^{-1} = B^{-1}A^{-1}$ (attention, ici l'ordre de multiplication est important, car l'opération n'est pas commutative).

Ensembles quotients $\mathbb{Z}_n$. Les entiers modulo n joue un rôle important dans plusieurs contextes. Ils sont introduits dans les tout premiers cours universitaires. On montre que

(a) $(\mathbb{Z}_n, +)$ est un groupe abélien.

(b) $(\mathbb{Z}_n, \cdot)$ est un monoïde commutatif, mais pas un groupe.

(c) $((\mathbb{Z}_n)^\times, \cdot)$ est un groupe abélien.

On invite le lecteur à vérifier ces affirmations en exercice (voir Exer 1.5).

Fonctions et bijections. On désigne par $\mathrm{Fonct}(E, E)$ **l'ensemble des fonctions** de E vers E. Observons que cet ensemble est toujours non vide, même si E est vide[12]. Comme d'habitude la **composition** de fonction est dénotée $(f, g) \mapsto f \circ g$, avec $(f \circ g)(x) = f(g(x))$. On désigne par S_E l'ensemble des bijections de E vers E. Puisque, par définition, les **bijections** sont les fonctions qui admettent un inverse pour la composition de fonctions, c'est donc dire dire que

$$S_E = (\mathrm{Fonct}(E, E))^\times. \tag{1.3}$$

On dit aussi de σ dans S_E que c'est une **permutation** de E. Puisque la composition est une opération associative sur $\mathrm{Fonct}(E, E)$ (voir Exercice 1.10), il s'ensuit que $(\mathrm{Fonct}(E, E), \circ)$ est un monoïde (non commutatif en général). La fonction **identité** Id_E, telle que $\mathrm{Id}_E(x) := x$, est l'élément neutre dans $(\mathrm{Fonct}(E, E), \circ)$. C'est donc que $(\mathrm{Fonct}(E, E), \circ)$ est un monoïde. L'égalité (1.3) implique que $(S_E, \circ)$ est un groupe. On dit que c'est le **groupe symétrique**, ou **groupe des permutations**, de l'ensemble E. Lorsque $E = \{1 \dots, n\}$ on écrit traditionnellement S_n plutôt que S_E. Les éléments de S_n sont souvent représentés par des matrices $2 \times n$. Ainsi, pour $\sigma \in S_n$, on note

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

On écrit aussi souvent $\sigma = \sigma(1)\sigma(2)\dots\sigma(n)$. Nous allons voir que les groupes symétriques jouent un rôle fondamental en mathématiques. Dans S_n, on omet souvent le symbole de composition de fonctions, et on note multiplicativement la loi de composition. On écrit alors $\sigma\tau$, plutôt que $\sigma \circ \tau$, et l'identité est notée e (pour ne pas confondre avec le nombre 1, qui joue ici un autre rôle). Par exemple, les éléments de S_3 sont (dans les deux notations)

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 123, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = 213, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = 132,$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = 321, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = 231, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = 312.$$

12. Il y a une et une seule fonction de $\varnothing$ vers $\varnothing$, et c'est une bijection.

Transformations linéaires. Soit E un espace vectoriel, alors l'ensemble des transformations linéaires bijectives sur E, noté $\mathrm{GL}(E)$, est un sous-ensemble de S_E. Comme la composée d'applications linéaires est linéaire, on en déduit que $(\mathrm{GL}(E), \circ)$ est un groupe. C'est le **groupe général linéaire** sur E. On verra plus tard, via la notion **d'isomorphisme de groupes**, que c'est (presque) le « même » groupe que $\mathrm{GL}_n = \mathrm{GL}_n(\mathbb{R})$, quand E est un espace vectoriel réel de dimension n. Un autre groupe typique est le groupe **spécial linéaire** $\mathrm{SL}_n(\mathbb{R})$ des transformations linéaires de $\mathbb{R}^n$ vers $\mathbb{R}^n$, ayant déterminant 1. Ce sont des exemples de Groupes de Lie [13].

Le groupe affine. Un groupe plus général (ici décrit pour $\mathbb{R}^n$) que celui de la dernière section est le groupe $GA_n(\mathbb{R})$. Décrit en terme de matrices, c'est l'ensemble des transformations f de $\mathbb{R}^n$ vers $\mathbb{R}_n$, de la forme

$$X \mapsto f(X) := A\,X + B,$$

où A est une matrice $n \times n$ de déterminant non nul, et B est un vecteur (colonne) dans $\mathbb{R}^n$. Ici, X est aussi considéré comme vecteur colonne. L'inverse de f est $f^{-1}(X) := A^{-1}\,X - A^{-1}\,B$. Le groupe affine transforme des droites dans des droites, des plans dans des plans, etc. Il préserve le parallélisme, les points milieu de segments, ou même le proportions sur une droite, etc. La géométrie affine correspond à étudier les théorèmes qui restent « invariants » [14] par transformations affines. Ainsi, parce que les concepts intervenants dans son énoncé sont préservés par les transformations affines, on peut ramener la preuve du fait que les trois médianes d'un triangle se coupent en un et un seul point, au cas du triangle équilatéral. En effet, il existe une (et une seule) transformation affine de $\mathbb{R}^2$ qui transforme n'importe quel triangle en un triangle équilatéral, et cette transformation envoie forcément l'intersection des trois médianes d'un des triangles dans l'autre. La géométrie projective correspond à faire une même démarche analogue avec le groupe « projectif », de même pour d'autres géométries. C'est l'idée du Programme d'Erlangen de Felix Klein.

1.4 Table de multiplication d'un groupe

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

13. Sophus Lie (1842–1899).
14. Il y a une notion mathématique précise, que nous ne présentons pas ici.

de S_3 est

	e	132	213	231	312	321
e	e	132	213	231	312	321
132	132	e	312	321	213	231
213	213	231	e	132	321	312
231	231	213	321	312	e	132
312	312	321	132	e	231	213
321	321	312	231	213	132	e

On remarque que S_3 n'est pas abélien, car $231 \circ 132 = 213 \neq 321 = 132 \circ 231$. On peut clairement voir dans la table de multiplication les inverses de chaque élément. En effet, l'inverse de l'élément x est y si l'intersection de la ligne x avec la colonne y est e. Une façon de décrire un (petit) groupe fini consiste parfois à en donner la liste de ces éléments, puis à donner explicitement sa table de multiplication (en s'assurant qu'elle respecte l'associativité). Ainsi, on a le groupe dont les éléments sont

$$G = \{1, a, b, ab, ba, aba\},$$

avec la multiplication donnée par la table de la figure 1.5.

	1	a	b	ab	ba	aba
1	1	a	b	ab	ba	aba
a	a	1	ab	b	aba	ba
b	b	ba	aba	a	ab	1
ab	ab	aba	ba	1	b	a
ba	ba	b	a	aba	1	ab
aba	aba	ab	1	ba	a	b

FIGURE 1.5 – La table de multiplication du groupe G.

1.5 Règles de calcul

L'inverse d'un produit. On a déjà vu plus haut que si x, y sont dans un groupe G alors $(xy)^{-1} = y^{-1}x^{-1}$. Plus généralement,

$$(x_1 x_2 \dots x_n)^{-1} = x_n^1 \dots x_2^{-1} x_1^{-1}.$$

Comme le groupe n'est pas forcément abélien, on a en général

$$(xy)^{-1} = y^{-1}x^{-1} \neq x^{-1}y^{-1} = (yx)^{-1},$$

sinon $xy = yx$ car $(x^{-1})^{-1} = x$. Par exemple, dans $\mathrm{GL}_2(\mathbb{R})$, on a les matrices

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

pour lesquelles on a

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

Bien entendu, si G est un groupe abélien, noté additivement, alors l'opposé de $x+y$ est $-x-y = -y-x$.

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

$$x^n := \begin{cases} x^{n-1}x & \text{si } n > 0, \\ 1 & \text{si } n = 0, \end{cases}$$

où 1 désigne l'élément neutre du groupe. En notation additive, on a plutôt

$$n \cdot x := \begin{cases} (n-1) \cdot x + x & \text{si } n > 0, \\ 0 & \text{si } n = 0. \end{cases}$$

De plus, on montre facilement (par récurrence) que

$$x^n x^m = x^{n+m}, \qquad (\text{ou encore} \quad n \cdot x + m \cdot x = (n+m) \cdot x \quad \text{en notation additive}). \tag{1.4}$$

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

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

Il est pratique de considérer aussi les puissances négatives, en posant pour $n > 0$, que

$$x^{-n} := (x^n)^{-1} = (x^{-1})^n.$$

En notation additive, on a $-(n \cdot x) = (-n) \cdot x$. On vérifie alors que, pour tout $m, n \in \mathbb{Z}$, on a encore la règle des exposants (1.4) (de même pour la version additive).

1.6 Sous-groupes

On a vu précédemment que pour montrer que $(A, \cdot)$ est un groupe, pour A un sous-ensemble de G, il suffisait de montrer que A est stable pour l'opération, contient le neutre e de G, et que les inverses des éléments de A sont aussi dans A. C'est une notion qui mérite d'être explorée, et on pose la définition suivante. Soit H, un sous-ensemble stable de G, qui contient l'élément neutre e de G, et tel que l'inverse x^{-1} soit aussi dans H pour tout $x \in H$. On dit alors que H est un **sous-groupe** de G. Si H est un sous-groupe de G, on écrit $H \leqslant G$.

On voit facilement que $H = \{e\}$ et G sont des sous-groupes de G. Un sous-groupe différent de G et de $\{e\}$ est dit sous-groupe **propre**. Pour montrer que $(E, *)$ est un groupe, il est souvent plus facile de montrer que c'est un sous-groupe d'un groupe déjà connu. On a les (chaînes de) sous-groupes suivants :

$$(n\mathbb{Z}, +) \leqslant (\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +) \leqslant (\mathbb{C}, +);$$
$$(\mathbb{Q}^*, \cdot) \leqslant (\mathbb{R}^*, \cdot) \leqslant (\mathbb{C}, \cdot).$$

De plus, pour tout espace vectoriel, $\mathrm{GL}(E) \leqslant S_E$. Pour un groupe G, l'ensemble

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

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

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

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

Proposition 1.2. *Les seuls sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$, pour $n \in \mathbb{N}$.*

Démonstration. Voir exercice 1.11. ∎

Proposition 1.3. *Soit G un groupe.*

(1) *Soit $H \subseteq G$, alors H est un sous-groupe de G si et seulement si $e \in H$ et pour tout $x, y \in H$ on a $xy^{-1} \in H$.*

(2) *Si $H \leqslant G$ et $K \leqslant H$ alors $K \leqslant G$ (la relation $\leqslant$ est transitive).*

(3) *L'intersection non vide d'une famille de sous-groupes de G est un sous-groupe de G.*

Démonstration. Voir exercice 1.12. ∎

Sous-groupes engendrés. Dans le groupe $\mathbb{Z}$, avec l'addition, tout élément s'écrit sous la forme

$$x = \underbrace{1 + 1 + \ldots + 1}_{n\text{-fois}}.$$

Autrement dit $\mathbb{Z}$ est **engendré** par 1. C'est le plus petit sous-groupe de $\mathbb{Z}$ qui contient 1, en vertu de la proposition 1.2. Plus généralement, pour G un groupe et $S \subseteq G$, on note $\langle S \rangle$ l'intersection de tous les sous-groupes de G qui contiennent S. C'est un sous-groupe de G (proposition 1.3) appelé **sous-groupe engendré** par S. Si $G = \langle S \rangle$, alors on dit que G est engendré par S, et que S est une **partie génératrice de** G. On dit des éléments de S que ce sont des **générateurs** de G. Lorsque $S = \{s\}$, alors on dénote plus simplement [15] par $\langle s \rangle$ le sous-groupe engendré par $s \in G$. Si $G = \langle s \rangle$ on dit que G est **monogène**. La proposition suivante clarifie certains aspects de ces définitions.

Proposition 1.4. *Soit G un groupe et $S \subseteq G$.*

(1) *Dans $\mathcal{P}(G)$ ordonné par l'inclusion, $\langle S \rangle$ est le plus petit sous-groupe de G contenant S.*

(2) *Pour $S = \varnothing$ alors $\langle S \rangle = \{e\}$. Sinon,*

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

Les éléments de $\langle S \rangle$ sont les produits [16] constitués de générateurs ou de leurs inverses. En notation additive, on a

$$\langle S \rangle = \{x_1 + \cdots + x_n \,|\, n \in \mathbb{N},\ x_i \in S \text{ ou } -x_i \in S,\ \text{pour tout } 1 \leqslant i \leqslant n\}.$$

Démonstration.

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

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

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

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

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

15. Au lieu d'écrire $\langle \{s\} \rangle$.
16. Rappelons qu'un produit vide ($n = 0$) est égal à 1, et qu'une somme vide est égale à 0.

Puisque $y_i z_j \in S$ ou $z_i^{-1}, z_j^{-1} \in S$, yz^{-1} est bien le produit d'élément de S ou de leurs inverses. Ainsi $xy^{-1} \in H$. On en déduit en vertu de la proposition 1.3 que $H \leqslant G$, d'où $H \in \Lambda$. En vertu de (1) on sait donc que $\langle S \rangle \subseteq \Lambda$. Montrons maintenant l'inclusion inverse. Soit $K \in \Lambda$ et $x = x_1 \dots x_n \in H$ avec $x_i \in S \subseteq K$ ou $x_i^{-1} \in S \subseteq K$. Donc, puisque K est un groupe, $x_i = (x_i^{-1})^{-1} \in K$ pour tout $1 \leqslant i \leqslant n$. D'où $x = x_1 \dots x_n \subseteq K$. On en conclut que $H \subseteq K$. Donc H est le plus petit élément de Λ pour l'inclusion. Autrement dit, $H = \langle S \rangle$ par (1). ■

Exemples.

(a) $\mathbb{Z} = \langle 1 \rangle$ est un groupe monogène pour l'addition. En effet, si $n \in \mathbb{Z}$ est positif, alors $n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ fois}}$; et si $n \in \mathbb{Z}$ est négatif, on a $n = \underbrace{(-1) + (-1) + \cdots + (-1)}_{|n| \text{ fois}}$.

(b) $n\mathbb{Z} = \langle n \rangle$ est aussi un groupe monogène pour l'addition.

(c) $\mathbb{Z}_n = \langle 1 \rangle$ est encore un groupe monogène (pour l'addition).

(d) Posons $\tau_1 := 213$ et $\tau_2 := 132$. Alors $S_3 = \langle \tau_1, \tau_2 \rangle$, car $321 = \tau_1\tau_2\tau_1 = \tau_2\tau_1\tau_2$; $312 = \tau_1\tau_2$ et $132 = \tau_2\tau_1$. D'où $S_3 = \{e, \tau_1, \tau_2, \tau_1\tau_2, \tau_2\tau_1, \tau_1\tau_2\tau_1\}$.

(e) Posant $\sigma := 231$, on vérifie que $S_3 = \langle \tau_1, \sigma \rangle$. En effet, $\tau_2 = \sigma\tau_1$, $321 = \tau_1\sigma$ et $\sigma = \sigma^2 = \sigma^{-1}$.

Ces exemples permettent d'observer que l'expression d'un élément comme produit de générateurs n'est pas unique. Ainsi on a, $321 = \tau_1\tau_2\tau_1 = \tau_2\tau_1\tau_2$ dans S_3 ; et $1 = 1 + 1 + 1 + 1$ dans $\mathbb{Z}_3$ (noté additivement). On dit de telles expressions que ce sont des **relations** dans le groupe. D'autre part, les deux derniers exemples montrent que la partie génératrice d'un groupe n'est pas nécessairement unique (ici on donne deux façons de décrire S_3). Une façon de visualiser comment un graphe se décrit en terme de générateurs est de construire le **graphe de Cayley** associé à ces générateurs. Les sommets du graphe sont les éléments du groupe. Pour chaque générateur s, on a un arc de g à h :

$$g \xrightarrow{s} h, \qquad \text{ssi} \qquad s\,g = h.$$

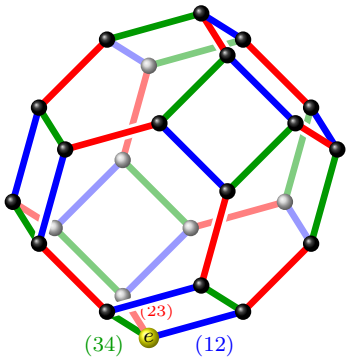


FIGURE 1.6 – Permutoèdre.

On donne souvent des couleurs différentes aux arcs, selon les générateurs auxquels ils correspondent. Une autre habitude courante est de remplacer les arcs aller-retour qui correspondent à des involutions par une seule arête non orientée. Par exemple, on dit du graphe de Cayley du groupe S_4, pour les générateurs $\tau_i = (i, i+1)$, que c'est le **permutoèdre**. Les arêtes bleues, rouges et vertes correspondent respectivement à la multiplication par les transpositions (12), (23) et (34). Les hexagones viennent de ce que

$$(12)(23)(12)(23)(12)(23) = e, \qquad \text{et} \qquad (23)(34)(23)(34)(23)(34) = e,$$

et les carrés de $(12)(34)(12)(34) = e$. Bien entendu, un même groupe donne lieu à plusieurs graphes de Cayley différents, selon que l'on considère des systèmes de générateurs différents. Ainsi, le graphe

de Cayley pour S_3, avec les générateurs $\tau_1 = (12)$ et $\tau_2 = (23)$ donne le graphe de gauche dans la figure 1.7 ; tandis qu'avec les générateurs $\tau_1 = (12)$ et $\sigma = (123)$, on obtient plutôt le graphe de droite de cette même figure.

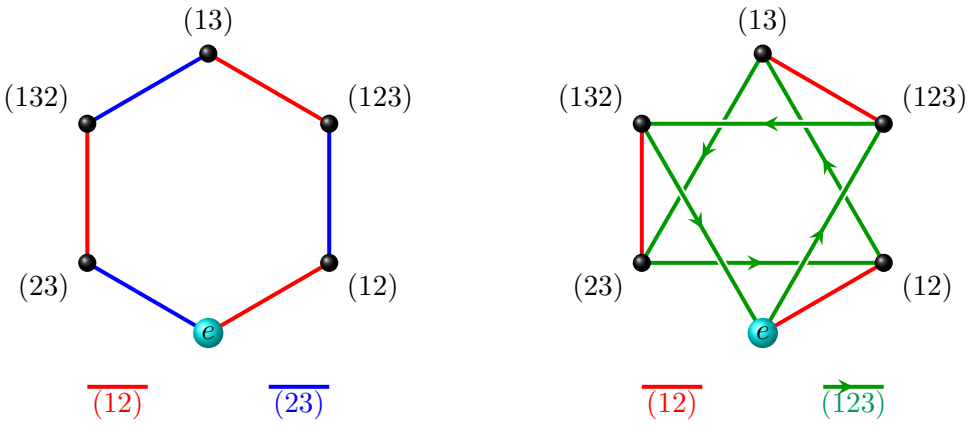


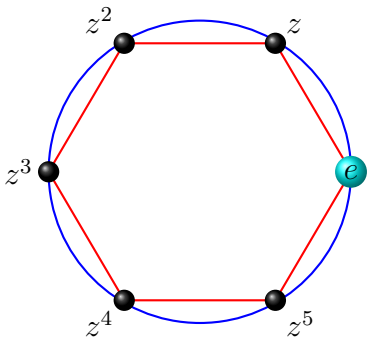
FIGURE 1.7 – Deux graphes de Cayley pour S_3.

Proposition 1.5. *Soit $G = \langle s \rangle = \{s^n \,|\, n \in \mathbb{Z}\}$ un groupe monogène, alors G est abélien. De plus, la fonction $f : \mathbb{Z} \to \langle x \rangle$ définie en posant $f(k) := x^k$ est surjective, et vérifie $f(k+\ell) = f(k)f(\ell)$; et l'ensemble $\{k \in \mathbb{Z} |\ f(k) = e\}$, est un sous-groupe de $\mathbb{Z}$.*

Démonstration. Voir exercice 1.15. ■

1.7 Ordre d'un groupe, ordre d'un élément

On dit que G est un **groupe fini**, si G est fini en tant qu'ensemble. On dit alors du cardinal $|G|$ que c'est l'**ordre** de G. L'**ordre d'un élément** $x \in G$ est l'ordre du groupe (monogène) $\langle x \rangle$. On le note $\mathrm{ord}(x)$. Si le groupe $\langle x \rangle$ est infini, on dit que l'ordre de x est infini, et on écrit $\mathrm{ord}(x) := \infty$. S'il est fini, on pose $\mathrm{ord}(x) := |\langle x \rangle|$. Le groupe monogène fini $\langle x \rangle$ est alors appelé **groupe cyclique**. Pour un groupe G fini, il est clair que $\mathrm{ord}(x) \leqslant |G|$, pour chaque élément x de G, puisque $\langle x \rangle \subseteq G$. L'élément neutre e est le seul élément de G d'ordre 1. En effet, on a d'abord clairement $|\langle e \rangle| = |\{e\}| = 1$. Réciproquement, si $\mathrm{ord}(x) = 1 = |\langle x \rangle|$, alors $\langle x \rangle = \{x\}$. Comme tout sous-groupe de G contient e, on a $e \in \langle x \rangle$, et donc $x = e$.



Groupe cyclique, $z^6 = e$.

Évidemment, G est infini s'il contient un élément d'ordre infini x, puisqu'il contient l'ensemble infini $\langle x\rangle$. On a (exercice) $\mathrm{ord}(x) = \mathrm{ord}(x^{-1})$. On dit des éléments d'ordre 2 dans G, que ce sont des **involutions**. Les involutions sont donc telles que $x^{-1} = x$. Observons que dans $(\mathbb{Z}, +)$, tous les éléments non nuls sont d'ordre infini et $\mathrm{ord}(0) = 1$! En effet si $n \neq 0$, alors $n\mathbb{Z} = \langle n\rangle$ est en bijection avec $\mathbb{Z}$ et est donc, de ce fait, infini. Parmi les groupes finis dits exceptionnels (voir Section 3.7), le plus grand est le groupe M, qu'on appelle le « Monstre ». Une des raisons est que son ordre est « assez » grand

$$\begin{aligned} 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 49 \cdot 71 \\ = \ 808017424794512875886459904961710757005754368000000000. \end{aligned}$$

Le résultat suivant est une caractérisation importante de l'ordre d'un élément, qui met en évidence une propriété importante des groupes finis.

Proposition 1.6. *Dans un groupe G fini, l'ordre d'un élément x est la plus petite puissance de x qui donne l'élément neutre, c.-à-d.*

$$\mathrm{ord}(x) = \min\{n \in \mathbb{N} \mid x^n = e\}. \tag{1.5}$$

Le groupe cyclique $\langle x\rangle$ s'écrit alors comme

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

Démonstration. On sait que

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

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

$$\mathbb{Z} \to \langle x\rangle, \qquad \text{avec} \qquad k \mapsto x^k,$$

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

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

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

et donc que $\mathrm{ord}(x) = |\langle x\rangle| = n$. ∎

Par exemple, l'ordre de S_3 est $|S_3| = 6$. On constate que dans S_3, on a $\mathrm{ord}(e) = 1$, $\mathrm{ord}(213) = \mathrm{ord}(132) = \mathrm{ord}(321) = 2$ (ce sont des involutions) et $\mathrm{ord}(231) = \mathrm{ord}(312) = 3$. Comme autre exemple, dans $\mathbb{Z}_6$, on a $\mathrm{ord}(0) = 1$, $\mathrm{ord}(1) = \mathrm{ord}(5) = 6$, $\mathrm{ord}(2) = \mathrm{ord}(4) = 3$, et $\mathrm{ord}(3) = 2$ (donc 3 est une involution). Notez que, dans tous ces exemples, l'ordre d'un élément divise (sans reste) l'ordre du groupe ! On montrera plus tard que c'est un phénomène général. Dans le cas où les éléments

d'un groupe correspondent à des transformations d'un objet, comme les manipulations d'un cube de Rubik, le phénomène décrit par la Proposition 1.6 correspond à dire qu'on revient inévitablement à la configuration de départ en répétant une même transformation un nombre suffisant de fois. Ainsi, on doit répéter 105 fois la séquence qui consiste à tourner la face gauche d'un quart de tour dans le sens horaire puis la face avant d'une même façon, avant de revenir au cube dans sa position originale. Il y a une (autre) séquence de mouvements qui nécessite d'être répétée 1260, et c'est l'ordre le plus grand d'un élément du groupe du cube.

Proposition 1.7. *Soit $n \in \mathbb{N}^*$, alors $|S_n| = n!$. Plus généralement, si E et F sont deux ensembles de cardinal n, alors l'ensemble $\mathcal{B}(E,F)$ des bijections de E dans F est de cardinal $n!$.*

Démonstration. On montre l,'énoncé par récurrence sur n. Si $n = 1$ il y a une et une seule fonction $E = \{x\} \to F = \{y\}$, qui est clairement bijective. Donc $\mathcal{B}(E,F) = 1 = 1!$ dans ce cas. Supposons maintenant la propriété vraie pour $n - 1 \geqslant 1$: si E' et F' sont deux ensembles de cardinal $n-1$, alors $|\mathcal{B}(E',F')| = (n-1)!$. Soit $x \in E$. Alors, pour tout $y \in F$, on a $|E\backslash\{x\}| = |F\backslash\{y\}| = n-1$. Donc par récurrence, $|\mathcal{B}(E\backslash\{x\}, F\backslash\{y\})| = (n-1)!$ pour tout $y \in F$. Si $\alpha \in \mathcal{B}(E\backslash\{x\}, F\backslash\{y\})$ alors la fonction $f : E \to F$ telle que $f|_{E\backslash\{x\}} = \alpha$ et $f(x) = y$ est une bijection de E dans F (à vérifier). Donc pour tout $y \in F$, il y a $(n-1)!$ bijection de E dans F tel que $f(x) = y$. C'est-à-dire que l'ensemble $A_y = \{f \in \mathcal{B}(E,F) \mid f(x) = y\}$ est de cardinal $(n-1)!$ pour tout $y \in F$. On peut vérifier que $\{A_y \mid y \in F\}$ est une partition de l'ensemble $\mathcal{B}(E,F)$ (exercice). D'où

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

Donc la propriété est vraie au rang n, et le lemme s'ensuit pour tout $n \in \mathbb{N}^*$. ∎

Observons que, dans un groupe G, si $\mathrm{ord}(x) = n$ alors $x^{-1} = x^{n-1}$. En effet,

$$x^{n-1}x = x^n = e = x\,x^{n-1}.$$

En particulier, si G est un groupe fini engendré par S, alors tous les générateurs sont d'ordre fini et $s^{-1} = s^{d-1}$, avec $d = \mathrm{ord}(s)$ pour $s \in S$. En vertu de la proposition 1.4, $x \in G$ s'écrit donc comme un produit de générateurs : $x = x_1 \dots x_m$ (avec $x_i \in S$), et on n'a nul besoin de considérer les inverses. En effet, pour obtenir une telle expression à partir d'un produit constitué de générateurs et de leurs inverses, il suffit de remplacer chaque inverse s^{-1} (pour $s \in S$) par le mot s^{d-1}, où $d = \mathrm{ord}(s)$. Par exemple, S_3 est engendré par $\tau = (12)$ et $\sigma = (123)$, et $(13) = \tau\sigma^{-1}$. Mais σ est d'ordre 3, et donc $\sigma^{-1} = \sigma^2$. On obtient donc $(13) = \tau\sigma\sigma$.

Le groupe $(\mathbb{Z},+)$ et $(\mathbb{Z}_n,+)$. Le groupe $\mathbb{Z}$ muni de l'addition est un groupe abélien d'ordre infini. Les seuls générateurs de $\mathbb{Z}$ sont 1 et -1, puisqu'on ne peut avoir $\mathbb{Z} = \langle n\rangle = n\mathbb{Z}$ que si tout entier

est multiple de n, ce qui force $n = \pm 1$. $\mathbb{Z}$ est d'ordre infini, tout entier non nul est d'ordre infini. Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$. Ce sont des sous-groupes monogènes, et les seuls générateurs de $n\mathbb{Z}$ sont $\pm n$. L'ensemble des sous-groupes de $\mathbb{Z}$ est donc en bijection avec $\mathbb{N}$. Pour chaque $n \in \mathbb{N}$, l'ensemble $\mathbb{Z}_n$, muni de l'addition, est un groupe abélien d'ordre n.

Proposition 1.8. *Soit $x \in \mathbb{Z}_n$ et $d = \text{pgcd}(x, n)$, alors $\text{ord}(x) = n/d$.*

Démonstration. Considérons les deux entiers $k := n/d$ et $\ell := x/d$, pour lesquels on a $\text{pgcd}(k, \ell) = 1$. En effet, si d' divise k et ℓ, alors $d'd$ divise x et n. Or $d = \text{pgcd}(x, n)$, donc $d' = 1$. Calculant dans $\mathbb{Z}_n$, on a (en notation additive)

$$k \cdot x = k(dq) = n\, d = 0.$$

En vertu de la proposition 1.6, il suffit donc de montrer que k est minimum pour cette propriété. Si $k' \leqslant k$ est tel que $k' \cdot x = 0$, alors $k'x = k'\ell d = bn = bkd$, pour un certain $b \in \mathbb{Z}$. Il s'ensuit que $k'\ell = bk$. Comme k et l sont premiers entre eux, le lemme de Gauss entraîne que k divise k', et donc $k = k'$ car $k' \leqslant k$. ■

On observe que l'ordre des éléments de $\mathbb{Z}_n$ divise l'ordre de $\mathbb{Z}_n$. Par exemple, l'ordre de 30 dans $(\mathbb{Z}_{42}, +)$ est $42/\text{pgcd}(30, 42) = 7$. En fait, comme on le verra au Chapitre 4, cette propriété est vraie pour tout groupe fini. C'est le théorème de Lagrange (voir Théorème 2.4).

Proposition 1.9. *Les seuls sous-groupes de $(\mathbb{Z}_n, +)$ sont les $\langle k \rangle$ tel que k divise n (et d'ordre n/k). En particulier, la fonction $k\mathbb{Z} \mapsto \langle k \rangle$ est une bijection entre l'ensemble des sous-groupes $k\mathbb{Z}$ de $\mathbb{Z}$ tel que k divise n et l'ensemble des sous-groupes de $(\mathbb{Z}_n, +)$.*

Démonstration. Soit H un sous-groupe de $(\mathbb{Z}_n, +)$. Considérons $K = \{x \in \mathbb{Z} \,|\, (x \bmod n) \in H\}$. Montrons que K est un sous-groupe de $(\mathbb{Z}, +)$ contenant $n\mathbb{Z}$. Observons que K est non vide, car $0 \in K$, car $(0 \bmod n) \in H$. De même, puisque $(n \bmod n) = 0$, on obtient que $n \in K$. Soit $x, y \in K$ alors $(x - y \bmod n) = (x \bmod n) - (y \bmod n) \in H$, car H est un sous-groupe de $\mathbb{Z}_n$. Donc $K \leqslant \mathbb{Z}$. Comme K est un sous-groupe de $\mathbb{Z}$, on sait qu'il existe $k \in \mathbb{N}$ tel que $K = k\mathbb{Z}$. Puisque $n \in K = k\mathbb{Z}$ et $n\mathbb{Z} = \langle n \rangle$ est le plus petit sous-groupe contenant n, on a $n\mathbb{Z} \subseteq k\mathbb{Z}$. Donc tout élément de $y \in K$ s'écrit $y = qk$ et donc tout élément de H s'écrit sous la forme $(y \bmod n) = q \cdot (k \bmod n)$. D'où $K = \langle (k \bmod n) \rangle$. Puisque $n\mathbb{Z} \subseteq k\mathbb{Z}$, on a que k divise n et donc $\text{pgcd}(n, k) = k$. En vertu de la proposition 1.8, on conclut que

$$|H| = |\langle (k \bmod n) \rangle| = n/k.$$

On laisse en exercice la dernière partie de la proposition. ■

Corollaire 1.10. *Soit $n \in \mathbb{N}$, alors*

(1) *$x \in \mathbb{Z}_n$ engendre $(\mathbb{Z}_n, +)$ si et seulement si $\text{pgcd}(x, n) = 1$.*

(2) *$(\mathbb{Z}_n)^\times$ est l'ensemble des générateurs de $\mathbb{Z}_n$.*

Démonstration. Exercice. ∎

1.8 Le groupe symétrique S_n

Considérons plus en détail le groupe symétrique S_E, des permutations d'un ensemble E de cardinal n. Pour faciliter la présentation, on choisit de prendre $E = \{1, 2, \ldots, n\}$, mais certaines de nos observations s'appliquent au cas général [17]. On a déjà montré que S_n, muni de la composition de fonctions, est un groupe d'ordre $n!$, qui est non abélien en général. C'est notre premier exemple de groupe fini non abélien (le groupe linéaire est un groupe infini non abélien). Comme nous allons le voir plus tard, tout groupe fini est une copie d'un sous-groupe d'un groupe symétrique (théorème de Cayley [18]). La question de trouver tous les sous-groupes d'un groupe symétrique est donc étroitement liée à la classification de tous les groupes finis ! Voici quelques propriétés combinatoires du groupe symétrique.

Une **inversion** [19] d'une permutation $\sigma \in S_n$ est un couple (i, j) tel que :

$$1 \leqslant i < j \leqslant n \quad \text{et} \quad \sigma(i) > \sigma(j).$$

On dit du nombre d'inversions de la permutation $\sigma \in S_n$ que c'est la **longueur** de σ. Ce nombre est noté :

$$\ell(\sigma) = \{(i, j) \,|\, 1 \leqslant i < j \leqslant n \text{ et } \sigma(i) > \sigma(j)\}.$$

On établie facilement que $\ell(\sigma) = 0$ si et seulement si $\sigma = e$. En effet, il est clair que la longueur de e est 0, puisque e n'a pas d'inversion. Inversement, si $\ell(\sigma) = 0$ alors on doit avoir $\sigma(1) < \sigma(2) < \cdots < \sigma(n)$, d'où $\sigma = 12 \ldots n = e$. Par exemple, l'ensemble des inversions de $\sigma = 24513$ est

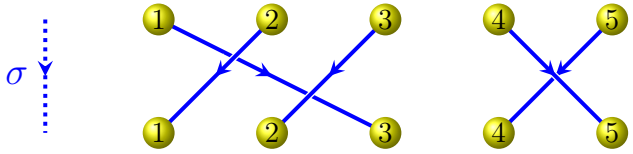
$$\{(1, 4),\ (2, 4),\ (2, 5),\ (3, 4),\ (3, 5)\},$$

et donc $\ell(\sigma) = 5$. Dans S_3, on a

$$\ell(123) = 0, \quad \ell(213) = 1, \quad \ell(132) = 1, \quad \ell(231) = 2, \quad \ell(312) = 2, \quad \text{et} \quad \ell(321) = 3.$$

Une manière agréable de visualiser les inversions d'une permutation est d'utiliser la représentation suivante. On dispose sur chacune de deux lignes superposées les nombres de 1 à n, et on joint par une flèche le i apparaissant sur la ligne du haut à $\sigma(i)$ sur celle du bas. Ainsi, la permutation $\sigma = 31254$ se représente comme suit :

17. Les exceptions à ce principe concernent les cas où on exploite l'ordre entre les entiers. Bien entendu, il n'y a pas d'ordre particulier qu'on puisse ainsi exploiter pour un ensemble E en général.
18. Arthur Cayley (1821-1895).
19. Observons que cette notion utilise l'ordre sous-jacent sur les entiers.



Le nombre d'inversions d'une permutation est alors le nombre de croisements dans la figure. La composition $\tau\sigma$, de deux permutations σ et τ de S_n, correspond à superposer deux tels diagrammes de flèches, plaçant celui de σ au-dessus de celui de τ. Ainsi, le composé de $\tau = 12435$ et $\sigma = 31254$ s'obtient en « suivant » les flèches dans la figure obtenue par cette superposition. Pour, $1 \leqslant i < n$,

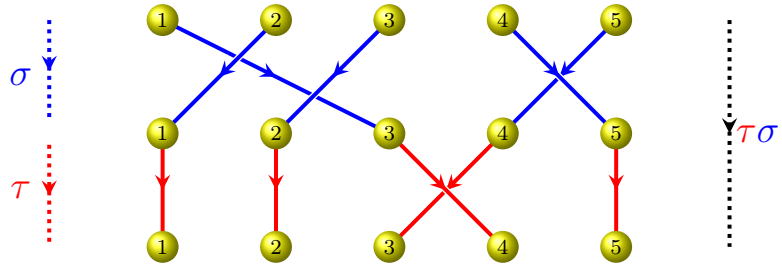


FIGURE 1.8 – Composition de permutations

la **transposition adjacente** τ_i est la permutation qui échange i et $i+1$ et laisse fixe tout autre $j \in \{1 \dots n\} \backslash \{i, i+1\}$. En formule,

$$\tau_i(j) = \begin{cases} i+1 & \text{si } j = i, \\ i & \text{si } j = i+1, \\ j & \text{autrement.} \end{cases}$$

Les transpositions sont des involutions, c'est-à-dire que $\tau_i^2 = e$, ou encore que $\tau_i^{-1} = \tau_i$. Multiplier à droite par τ_i revient à échanger $\sigma(i)$ et $\sigma(i+1)$ dans σ, c.-à-d.

$$\sigma\,\tau_i = \sigma(1)\sigma(2)\cdots\sigma(i-1)\,\underbrace{\sigma(i+1)\sigma(i)}\,\sigma(i+2)\cdots\sigma(n).$$

Cela se voit bien sur un diagramme de flèches. Ainsi, on a

$$24513 = 24153\ \tau_3 = 21453\ \tau_2\tau_3 = 12453\ \tau_1\tau_2\tau_3 = 12435\ \tau_4\tau_1\tau_2\tau_3 = \tau_3\tau_4\tau_1\tau_2\tau_3.$$

Observons ici que multiplier par τ_i revient à augmenter ou diminuer la longueur par 1 ! Ce phénomène est général, comme le montre le lemme suivant.

Lemme 1.11. *Soit $\sigma \in S_n$ et $1 \leqslant i < n$, alors $\ell(\sigma\tau_i) = \ell(\sigma) \pm 1$. Plus précisément,*

$$\ell(\sigma\tau_i) = \begin{cases} \ell(\sigma) + 1 & \text{si } \sigma(i) < \sigma(i+1), \\ \ell(\sigma) - 1 & \text{si } \sigma(i) > \sigma(i+1). \end{cases}$$

Démonstration. Posons $\sigma = a_1 a_2 \dots a_n$ où $a_i = \sigma(i)$. Comme on l'a déjà observé, $\alpha = \sigma\tau_i = a_1 \dots a_{i-1} a_{i+1} a_i a_{i+2} \dots a_n$ s'obtient à partir de σ en échangeant la i-ème et la $i+1$-ème lettre. On observe d'abord que toute inversion $(k,l) \neq (i, i+1)$ de σ correspond à une inversion $(k', l') \neq (i, i+1)$ de α et vice versa. Donc, si (i,k) est une inversion de α alors $(i+1, k)$ est une inversion de α car $a_i = \sigma(i) = \alpha_{i+1}$ et $\sigma(k) = \alpha_k$. En d'autres termes, le nombre d'inversions de σ différentes de $(i, i+1)$ est égal au nombre d'inversions de α différentes de $(i, i+1)$. Si $a_i = \sigma(i) < \sigma(i+1) = a_{i+1}$, alors $(i, i+1)$ n'est pas une inversion de σ. Mais puisque $\alpha(i) = a_{i+1} > a_i = \alpha(i+1)$, alors $(i, i+1)$ est une inversion de α. Dans ce cas, α a une inversion de plus que σ. Si par contre $a_i = \sigma(i) > \sigma(i+1) = a_{i+1}$, alors $(i, i+1)$ est une inversion de σ. Mais puisque $\alpha(i) = a_{i+1} < a_i = \alpha(i+1)$, alors $(i, i+1)$ est une inversion de α. Dans ce cas, α a une inversion de moins que σ. ∎

Nous sommes maintenant en mesure de démontrer la proposition suivante, qui permet de donner un système de générateurs pour S_n. Nous allons aussi voir qu'elle permet de comprendre d'une autre manière la longueur $\ell(\sigma)$.

Proposition 1.12. *Toute permutation $\sigma \in S_n$ est un produit de $\ell(\sigma)$ transpositions adjacentes.*

Démonstration. Par récurrence sur $\ell(\sigma)$. Si $\ell(\sigma) = 0$, alors $\sigma = e$ est l'identité, qui correspond au produit vide. Supposons $\ell(\sigma) > 0$, alors $\sigma \neq e$. Il existe donc i tel que $\sigma(i) > \sigma(i+1)$. Ainsi en vertu du lemme 1.11, $\ell(\sigma\tau_i) = \ell(\sigma) - 1 < \ell(\sigma)$. Par hypothèse de récurrence, $\sigma\tau_1$ est égal à un produit de $\ell(\sigma\tau_i)$ transpositions adjacentes. Donc $\sigma = \sigma\tau_i\tau_i^{-1} = (\sigma\tau_i)\tau_i$ (car τ_i est une involution) est un produit de $\ell(\sigma)$ transpositions adjacentes. ∎

Une autre utilité de la longueur est de permettre la définition suivante. On considère la fonction

$$\varepsilon : S_n \to \{\pm 1\}, \qquad \text{avec} \qquad \varepsilon(\sigma) := (-1)^{\ell(\sigma)}.$$

On dit de $\varepsilon(\sigma)$ que c'est le **signe** de la permutation σ. Dans un cours d'algèbre linéaire, on montre que

$$\det(a_{ij})_{1 \leqslant i,j \leqslant n} = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}, \tag{1.6}$$

pour toute matrice $(a_{ij})_{1 \leqslant i,j \leqslant n}$.

Corollaire 1.13. *Pour tout σ, et τ dans S_n, on a*

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau).$$

Démonstration. Il suffit de montrer que

$$\ell(\sigma\tau) \equiv \ell(\sigma) + \ell(\tau) \ (\mathrm{mod}2). \tag{1.7}$$

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

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

L'égalité (1.7) est laissée en exercice. ■

Ordre et cycles d'une permutation. La notion de cycle[20] est fondamentale dans le groupe symétrique. Elle rend possible une nouvelle décomposition des permutations. Cette permet décomposition, entre autres, de calculer différemment l'ordre. De plus, elle joue un rôle crucial dans plusieurs constructions. Pour $1 < p \leqslant n$, on dit d'une permutation $\gamma \in S_n$ que c'est un un **p-cycle** (ou simplement que c'est un **cycle**) s'il existe p entiers distincts $1 \leqslant a_1, a_2, \ldots, a_p \leqslant n$ tels que

$$\gamma(a_1) = a_2, \quad \gamma(a_2) = a_3, \quad \ldots \quad \gamma(a_j) = a_{j+1}, \quad \ldots \quad \text{et} \quad \gamma(a_p) = a_1;$$

avec de plus $\gamma(b) = b$ pour tout $b \notin \{a_1 \ldots, a_p\}$. On dit de ces derniers b, que ce sont des points fixes de γ. La figure 1.9 représente un cycle de façon plus imagée.

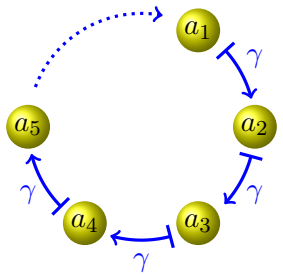


FIGURE 1.9 – Un cycle.

On dénote habituellement par $(a_1, a_2 \ldots, a_p)$ un tel cycle γ. Les parenthèses soulignent qu'on parle d'un cycle. Pour alléger la notation, on omet les virgules lorsque c'est possible. Notons que les points laissés fixes par γ n'apparaissent pas dans cette notation. On dit de p que c'est la **longueur** du cycle γ. Par définition, une **transposition** est un 2-cycle, et elle est de la forme (i, j), pour $i \neq j$. La transposition adjacente τ_i, déjà vue, s'écrit donc aussi $\tau_i = (i, i+1)$. Enfin, si $p = n$, on dit qu'on a une permutation **circulaire**. Comme nous allons le constater, les permutations circulaires dans S_n, pour $n > 1$, sont les seules qui n'ont pas de point fixe. Par exemple, la permutation

$$\gamma = 24351 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = (1245)$$

20. Cette notion est générale, et s'applique aux permutations de tout ensemble fini E.

est un 4-cycle dans S_5, car $\gamma(1) = 2$, $\gamma(2) = 4$, $\gamma(4) = 5$ et $\gamma(5) = 1$. Son seul point fixe est $\gamma(3) = 3$. De plus, l'inverse de γ est aussi un 4-cycle. En effet, $\gamma^{-1} = 51324 = (1542)$ s'obtient en « lisant le cycle γ à l'envers ». Notons d'autres parts que $\gamma^2 = 45312$ n'est pas un cycle, car $\gamma^2(1) = 4$, $\gamma^2(4) = 1$, $\gamma^2(2) = 5$ et $\gamma^2(5) = 2$. En général, le produit de cycles n'est pas un cycle. Plus généralement, on a la propriété suivante.

Proposition 1.14. *Si $\gamma = (a_1 \dots, a_p) \in S_n$ un p-cycle, alors*

(1) $\gamma^{-1} = (a_1, a_p, a_{p-1} \dots a_2)$ *est un p-cycle ;*
(2) $\mathrm{ord}(\gamma) = p$.
(3) *le signe de γ est $(-1)^{p-1}$.*

Démonstration. Voir exercice 1.32. ∎

Pour deux entiers p et q, plus grands ou égaux à 2, on dit que des cycles $(a_1 \dots, a_p)$ et $(b_1 \dots, b_q)$ sont **à support disjoint**, ou plus simplement **disjoints**, si $\{a_1 \dots, a_p\} \cap \{b_1 \dots, b_q\} = \varnothing$. Par exemple, les cycles $(1, 5, 4)$ et $(2, 3)$ sont à support disjoint ; tandis que les cycles $(1, 5, 2)$ et $(2, 6, 3)$ ne le sont pas. Deux cycles à support disjoint commutent, c.-à.d. si σ et τ sont des cycles à support disjoint, alors $\sigma\tau = \tau\sigma$. Le but de toute cette discussion est la proposition suivante.

Proposition 1.15. *Toute permutation (différente de l'identité) s'écrit de manière unique, à l'ordre des facteurs près, comme produit de cycles à support disjoint (et donc qui commutent).*

Plutôt que de démontrer cette proposition, nous allons illustrer le processus qui mène à cette décomposition pour une permutation particulière. La démonstration générale est laissée en exercice (ou voir [3]). Prenons $\sigma = 729158436 \in S_9$, et débutons avec 1. En calculant les images successives $\sigma(1) = 7$, $\sigma^2(1) = 4$, et $\sigma^3(1) = 1$, on trouve que σ contient le cycle $\gamma_1 := (174)$. La plus petite valeur qui n'est pas couverte par ce cycle est 2, et on constate que c'est un point fixe de σ. Puis viens 3, qui « engendre » le cycle $\gamma_2 := (3968)$. Le seul nombre qui reste est maintenant 5, qui est un point fixe. La décomposition résultante est donc

$$\sigma = \gamma_1\gamma_2 = (174)(3968) = \gamma_2\gamma_1 = (3968)(174).$$

L'unicité de la décomposition provient de l'unicité des cycles qui la compose. On observe que les cycles de σ sont de la forme

$$(x, \sigma(x), \sigma^2(x), \sigma^3(x), \dots, \sigma^{d-1}(x)),$$

où d est l'ordre de x.

Une façon agréable de mettre en évidence la décomposition d'une permutation en cycles disjoints est de représenter la permutation comme à la figure 1.10. Dans celle-ci, on joint les éléments de l'ensemble sous-jacent par une flèche $i \to j$, si $\sigma(i) = j$. On voit bien ainsi apparaître les cycles disjoints, pour le moins que le dessin soit fait correctement.

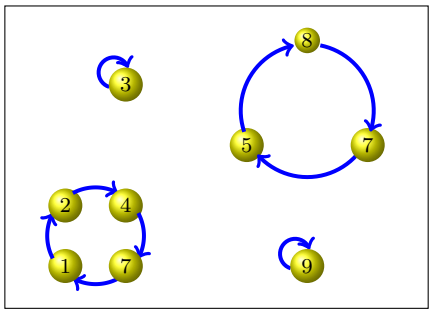


FIGURE 1.10 – La décomposition de la permutation 248736159 en cycles disjoints.

Corollaire 1.16. *Soit $\sigma = \gamma_1 \dots \gamma_k \in S_n$ une permutation en cycle décomposée en cycles disjoints, alors* $\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(\gamma_1), \mathrm{ord}(\gamma_2), \mathrm{ord}(\gamma_3) \dots, \mathrm{ord}(\gamma_k))$. *De plus le signe de σ est $(-1)^{n-c(\sigma)}$, où $c(\sigma)$ est le nombre de cycles de σ.*

Démonstration. Exercice. ■

Par exemple, avec la permutation $\sigma = 729158436 \in S_9$ de l'exemple précédent, on trouve de cette manière que $\mathrm{ord}(\sigma) = 12$, puisque c'est le plus petit commun multiple de 3 et 4, les longueurs des cycles de la décomposition de σ. Un problème amusant, et pas trivial, est de déterminer quel est le plus grand ordre possible pour un élément de S_n.

1.9 Groupes engendrés par des réflexions

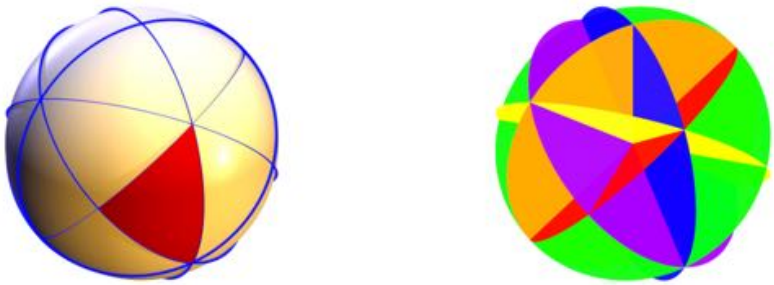


FIGURE 1.11 – Arrangement d'hyperplans dans $\mathbb{R}_3$, correspondant à S_4

Le groupe symétrique fait partie (à isomorphisme[21] près) d'une famille de groupes de grand intérêt en recherche mathématique contemporaine. Ce sont des sous-groupes de GL_n qui s'obtiennent en composant des **réflexions**[22], c.-à-d. des matrices $n \times n$, à coefficients réels, dont le carré est l'identité et le déterminant est -1. Autrement dit, les générateurs du groupe sont des réflexions dans des hyperplans (sous espaces vectoriels de dimension $n-1$). On observe qu'une réflexion est son propre inverse. C'est le cas des matrices suivantes :

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

qui engendrent le groupe S_4, des matrices de permutations. On s'aperçoit que ces matrices laissent fixes les vecteurs de la forme (a, a, a, a). On peut donc considérer la trace de l'action de S_4 sur le sous-espace vectoriel de dimension 3, orthogonal à ces vecteurs. Cette action est représentée à la figure 1.11. Dans la partie de droite de cette figure, les plans sont obtenus comme intersection[23] avec les hyperplans de réflexion. Il y a un plan pour chaque réflexion[24] dans le groupe. Pour que le groupe engendré soit fini, il y a de fortes contraintes sur les angles entre les hyperplans correspondant aux générateurs, comme on le voit à la figure 1.11, ainsi qu'à la figure 1.12. Dans la partie de gauche de la figure ci-haut, on voit l'intersection des plans avec la sphère de rayon 1. Les angles entre les plans sont ainsi mis en évidence, et le triangle rouge contient un angle de $\pi/2$ et deux angles de $\pi/3$. Ces contraintes sur les angles

21. Voir Section (3.3).
22. On en donne ici une définition un peu simplifiée.
23. Pour plus de détails, voir Swallowtail on the shore, dans la série de textes *Snapshots of modern mathematics from Oberwolfach*, No7/2014.
24. Attention, le groupe contient aussi d'autres éléments.

permettent de déterminer quels sont tous les groupes finis de ce genre. Un autre exemple que nous verrons plus tard (Voir Section 2.1) est le groupe « diédral ». Plus généralement, parmi les groupes engendrés par les réflexions, on retrouve les groupes de Coxeter [25] qui jouent un rôle fondamental dans plusieurs domaines des mathématiques, de la physique, et en cristallographie.

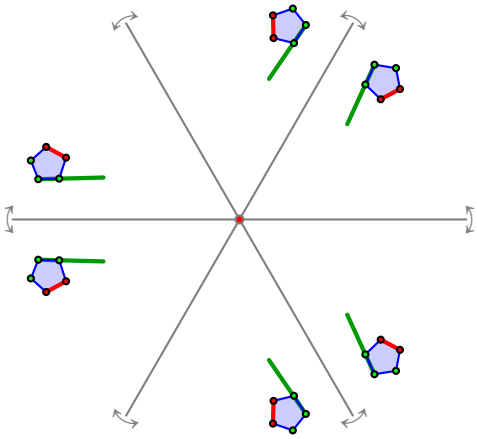


FIGURE 1.12 – Réflexions selon des droites d'angles $2\,k\,\pi/6$, avec $0 \leqslant k \leqslant 2$.

1.10 Un groupe à la Galois

Sur l'ensemble des expressions de la forme

$$a + b\,\zeta + c\,\zeta^2 + d\,\zeta^3 + e\,\zeta^4, \qquad \text{pour} \qquad \zeta = \exp(2\,i\,\pi/5),$$

avec a, b, c, d, et e des nombres réels ; on considère les « transformations » $f : \mathbb{C} \to \mathbb{C}$ telles que :

(1) $f(x+y) = f(x) + f(y)$, pour tout $x, y \in \mathbb{C}$,

(2) $f(x\,y) = f(x)\,f(y)$, pour tout $x, y \in \mathbb{C}$,

(3) $f(r) = r$, si et seulement si $r \in \mathbb{R}$.

L'ensemble de ces transformations forme un groupe G pour la composition. En effet, les conditions ci-dessus entraînent que

$$f(a + b\,\zeta + c\,\zeta^2 + d\,\zeta^3 + e\,\zeta^4) = a + b\,f(\zeta) + c\,f(\zeta)^2 + d\,f(\zeta)^3 + e\,f(\zeta)^4,$$

avec

$$f(\zeta)^5 = f(\zeta^5) = f(1) = 1.$$

25. Les travaux de H.S.M. Coxeter, (1907-2003), ont inspiré plusieurs des oeuvres artistiques de M.C. Escher (1898-1972).

Autrement dit, la transformation f est entièrement caractérisée par la valeur de $f(\zeta)$. Il n'y a que 4 choix possibles pour $f(\zeta)$, ce sont les quatre **racines 5^{e} de l'unité** différentes [26] de 1 :

$$f_k(\zeta) = \zeta^k, \qquad 1 \leqslant k \leqslant 4,$$

avec la propriété $f_k \circ f_j = f_{kj}$ (loi des exposants). On observe que f_1 est l'identité, et le groupe G est donc constitué de $\{e, f_2, f_3, f_4\}$. On trouve, par un calcul direct qui exploite le fait que

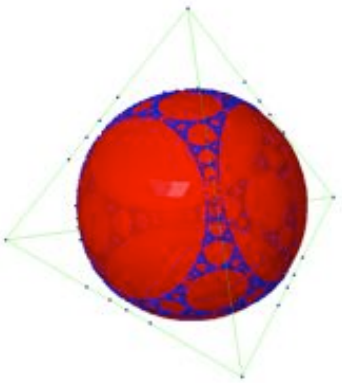
$$\zeta^5 = 1, \quad \zeta^6 = \zeta, \quad \zeta^7 = \zeta^2, \quad \dots$$

que la table de multiplication de G est

	e	f_2	f_3	f_4
e	e	f_2	f_3	f_4
f_2	f_2	f_4	e	f_3
f_3	f_3	e	f_4	f_2
f_4	f_4	f_3	f_2	e

Ce qui permet de constater que c'est bien un groupe. Sous une forme « déguisée » [27], c'est en fait le groupe cyclique $\mathbb{Z}_4$. La théorie de Galois ramène l'étude des racines de polynômes à l'étude d'un groupe de Galois qui lui est associé en généralisant la construction que l'on vient de considérer. Dans notre cas, nous avons calculé le groupe de Galois du polynôme $p(z) = a + bz + cz^2 + dz^3 + ez^4$.

Conclusion



Pour de nombreuses utilisations en mathématique, en physique, et dans d'autres domaines, il importe de mieux comprendre la structure des groupes, et leurs propriétés. Parmi les problèmes centraux et encore de grande actualité : la recherche des plus petits ensembles de générateurs d'un groupe, où la détermination de tous ses sous-groupes, sont deux problèmes difficiles de la théorie générale des groupes. Un autre axe très important est la recherche en théorie de la représentation des groupes. Enfin, une des grandes réalisations des algébristes du XXe siècle a été de classifier tous les groupes finis (voir l'atlas des groupes finis Atlas des groupes finis).

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

26. Ceci résulte de la condition (3).
27. À ce sujet, voir la notion d'isomorphisme, Section 3.3.

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

1.11 Exercices

Exercice 1.1. Soit la loi de composition $\star : (a, b) \mapsto ab + a + b$ sur $\mathbb{R}$. Est-ce que $\star$ est associative ? Commutative ?

Exercice 1.2. Soit la loi de composition $\star : (A, B) \mapsto AB + \mathrm{Id}$ sur $\mathcal{M}_n(\mathbb{R})$ l'ensemble des matrices carrées $n \times n$. Est-ce que $\star$ est associative ? Commutative ?

Exercice 1.3. Montrer que l'inverse de l'élément neutre d'un groupe est égal à lui-même, et montrer que l'inverse de l'inverse de x est égal à x.

Exercice 1.4. Soit E un ensemble muni d'une multiplication et d'une addition. On considère dans E la loi de composition $\star : (a, b) \mapsto ab + a + b$.

(a) Posons $E = \mathbb{R}$. Est-ce que $(\mathbb{R}, \star)$ possède un élément neutre ? (justifier). Lesquels des sous-ensembles de $\mathbb{R}$ suivants sont stables pour $\star$:

$$\mathbb{N}, \quad \mathbb{Q}^-, \quad \mathbb{Q}^{+*}, \quad \mathbb{R}, \quad \text{et} \quad n\mathbb{Z}.$$

(b) Mêmes questions avec $E = \mathcal{M}_n(\mathbb{R})$ et $E = \mathrm{GL}_n(\mathbb{R})$.

Exercice 1.5. On considère les ensembles $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{Z}^*$, $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{Q}^+$, $\mathbb{Q}^{+*}$, $\mathbb{R}^*$, $\mathbb{R}^+$, $\mathbb{R}^{+*}$, $\mathbb{Z}^-$, $\mathbb{Q}^-$ et $\mathbb{R}^-$. Parmi ces ensembles, lesquels sont des groupes ou des monoïdes pour : (a) l'addition sur $\mathbb{R}$; (b) la multiplication sur $\mathbb{R}$. Justifier et préciser l'ensemble de leurs éléments inversibles.

Exercice 1.6. Pour tout espace vectoriel V, déduire de la définition d'espace vectoriel que $(V, +)$ est un groupe. En conclure que $(\mathcal{M}_n, +)$ est un groupe.

Exercice 1.7. Soit G un ensemble muni d'une loi de composition $*$. Montrer que $(G, *)$ est un groupe si et seulement si

(a) $*$ est associative ;

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

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

Exercice 1.8. Soit E un ensemble.

(a) Montrer que $(\mathcal{P}(E), \cup)$ et $(\mathcal{P}(E), \cap)$ sont des monoïdes. Sont-ils des groupes ?

(b) On considère dans $\mathcal{P}(E)$ la loi de composition

$$(A, B) \mapsto A \vartriangle B = (A \cup B) \backslash (A \cap B) \quad (\textbf{Différence symétrique}).$$

Montrer que $(\mathcal{P}(E), \vartriangle)$ est un groupe. Quel est son élément neutre ? Quel est l'inverse de A ? Est-ce un groupe abélien ?

Exercice 1.9. Soit $n \in \mathbb{N}^*$.

(a) Montrer que $(\mathbb{Z}_n, +)$ est un groupe abélien de cardinal n.

(b) Montrer que $(\mathbb{Z}_n, \cdot)$ est un monoïde commutatif. Est-ce un groupe ? (Justifier.)

(c) Montrer que $((\mathbb{Z}_n)^\times, \cdot)$ est un groupe abélien de cardinal $\varphi(n)$ (la **fonction d'Euler**, dont la valeur est le nombre d'entiers relativement premiers à n, entre 1 et $n-1$.)

(d) Soit la loi de composition $\star : (a, b) \mapsto ab + a + b$ dans $\mathbb{Z}_n$. Est-ce que $\star$ possède un élément neutre ? (Justifier.) Est-ce que $(\mathbb{Z}_n)^\times$ est stable pour $\star$?

Exercice 1.10. Soit E un ensemble. Montrer que la composition de fonction munie l'ensemble $\mathrm{Fonct}(E, E)$ d'une structure de monoïde.

Exercice 1.11. (voir Proposition 1.2) Montrer que pour chaque n, l'ensemble $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Si H est un sous-groupe de $\mathbb{Z}$, montrer que $H = n\mathbb{Z}$, avec n égal au plus petit entier positif non null dans H.

Exercice 1.12. (voir Proposition 1.3) Pour un groupe G, soit H un sous-ensemble de G contenant l'élément neutre e de G, et tel que xy^{-1} est dans H pour tout x et y dans H. En choisissant x et y judicieusement, montrer que H contient l'inverse de tous ces éléments. Montrer que la notion de sous-groupes est transitive, et vérifier que l'intersection d'une famille quelconque de sous-groupes est un sous-groupe. Est-il vrai que l'union de sous-groupes est un sous-groupe ? Justifier votre réponse.

Exercice 1.13. Soit G un groupe. On suppose que pour tout $x \in G$ on a $x^2 = e$. Montrer que G est abélien.

Exercice 1.14. Soit G un groupe et soit $a, b \in G$ tel que $a^5 = e$ et $a^3 b = ba^3$.

(a) Montrer que $a^6 b = ba^6$;

(b) en déduire que $ab = ba$.

Exercice 1.15. (voir Proposition 1.5) Pour x élément de G un groupe, montrer par récurrence que $x^{k+\ell} = x^k x^\ell$, pour tout k et ℓ dans $\mathbb{N}$. En déduire ensuite que cette propriété s'étend à tout $\mathbb{Z}$. Puis, montrer que $\langle x \rangle$ est abélien, et que la fonction $f(k) := x^k$ est surjective sur $\langle x \rangle$. Verifier que $f(k+\ell) = f(k)f(\ell)$, puis que $\{k \mid f(k) = e\}$ est un sous-groupe de $\mathbb{Z}$. En conclure que $f(k) = e$ si et seulement si $(k \bmod n) = 0$ pour un certain $n \in \mathbb{Z}$ (voir Exercice 1.11).

Exercice 1.16. Montrer que le centre $Z(G)$ d'un groupe est un sous-groupe de G. Calculer le centre de GL_n, et en conclure que GL_n n'est pas commutatif.

Exercice 1.17. Soit $n \in \mathbb{N}^*$.

(a) Montrer que l'ensemble $O(n) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^tMM = \mathrm{Id}_n\}$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$. C'est le **groupe orthogonal**. Rappelons que ${}^tM$ désigne la transposée de M.

(b) Montrer que l'ensemble $SO(n) = \{M \in O(n) \,|\, \mathrm{dét}(M) = 1\}$ est un sous-groupe de $O(n)$. C'est le **groupe spécial orthogonal**. Rappelons que

$$SO(2) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \mid \theta \in \mathbb{R} \right\}.$$

Exercice 1.18. Soit G un groupe et $A \subseteq G$. Pour $g \in G$ on note $gAg^{-1} = \{gxg^{-1} \,|\, x \in A\}$.

(a) Montrer que $Z(A) = \{g \in G \,|\, gx = xg, \text{ pourtout } x \in A\}$ est un sous-groupe de G.

(b) Montrer que gAg^{-1} et A sont en bijection.

(c) Montrer que $N(A) = \{g \in G \,|\, gAg^{-1} = A\}$ est un sous-groupe de G.

(d) Montrer que $Z(A) \leqslant N(A)$.

Exercice 1.19.

(a) Quel est le centre du groupe S_n, pour $n \in \mathbb{N}^*$?

(b) Montrer que G est un groupe abélien si et seulement si G est égal à son centre.

Exercice 1.20. Montrer que les seuls sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $(n\mathbb{Z}, +)$, pour $n \in \mathbb{N}$.

Exercice 1.21. Soit G un groupe. Montrer que

(a) Soit $H \subseteq G$, alors H est un sous-groupe de G si et seulement si $e \in H$ et pour tout $x, y \in H$, $xy^{-1} \in H$.

(b) Si $H \leqslant G$ et $K \leqslant H$ alors $K \leqslant G$ (la relation $\leqslant$ est transitive).

(c) L'intersection non vide d'une famille de sous-groupes de G est un sous-groupe de G.

Exercice 1.22. Soit G un groupe et H, H' deux sous-groupes de G. Montrer que $H \cup H'$ est un sous-groupe de G si et seulement si $H \subseteq H'$ ou $H' \subseteq H$.

Exercice 1.23. Soit G un groupe. On dit que x et y sont **conjugués** dans G s'il existe $g \in G$ tel que $x = gyg^{-1}$. On notera $x \sim y$.

(a) Montrer que $\sim$ est une relation d'équivalence sur G. La classe d'équivalence de $x \in G$ est appelée **classe de conjugaison de** x.

(b) Soit $x \in G$, montrer que l'ensemble $G_x = \{g \in G \,|\, gxg^{-1} = x\}$ est un sous-groupe de G, appelé sous-groupe stabilisateur de $x \in G$.

Exercice 1.24. Soit $G = \langle s \rangle$ un groupe monogène. Montrer que

(a) G est un groupe abélien.

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

(c) La fonction $f : \mathbb{Z} \to \langle x \rangle$, définie par $f(k) = x^k$, est surjective et que $f(k + l) = f(k)f(l)$.

(d) Si G est noté additivement, montrer que $G = \{ns \,|\, n \in \mathbb{Z}\}$.

Exercice 1.25. Soit G un groupe et $g \in G$. Montrer que

(a) Si $\text{ord}(g) = \infty$ alors $\text{ord}(g^k) = \infty$ pour tout $k \in \mathbb{N}^*$.

(b) Si $\text{ord}(g) = n$ est fini et $k \in \mathbb{N}^*$, alors $\text{ord}(g^k) = n/\text{pgcd}(n, k)$.

(c) $\text{ord}(g^{-1}) = \text{ord}(g)$.

Exercice 1.26. Soit le groupe $G = \mathbb{Z}_{12}$.

(a) Déterminer le sous-groupe H de G engendré par 6 et 8. Déterminer son ordre.

(b) Caractériser les générateurs de G.

(c) Quel est l'ordre de l'élément 9 ?

Exercice 1.27. Soit $n \in \mathbb{N}^*$, montrer que

(a) La fonction $k\mathbb{Z} \mapsto \langle k \rangle$ est une bijection entre l'ensemble des sous-groupes $k\mathbb{Z}$ de $\mathbb{Z}$ tel que k divise n, et l'ensemble des sous-groupes de $\mathbb{Z}_n$.

(b) $\mathbb{Z}_n = \langle x \rangle$ si et seulement si $\text{pgcd}(x, n) = 1$.

(c) $(\mathbb{Z}_n)^\times$ est l'ensemble des générateurs de $\mathbb{Z}_n$.

Exercice 1.28. On considère dans cet exercice le groupe symétrique S_4. Avec nos conventions, on a les transpositions adjacentes

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = 2134 \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = 1324 \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = 1243.$$

(a) Écrire tous les éléments de S_4 comme un produit des transpositions adjacentes τ_i ;

(b) Calculer les ordres et les longueurs des éléments de S_4.

(c) On considère les sous-groupes

$$H = \langle \tau_1, \tau_2 \rangle ; \quad K = \langle \tau_2, \tau_3 \rangle \quad \text{et} \quad L = \langle \tau_1, \tau_3 \rangle .$$

(1) Quels sont les ordres de H, K et L ?

(2) Écrire la table de multiplication de ces sous-groupes. Sont-ils abéliens ?

(c) Que remarquez-vous ?

Exercice 1.29. (**Relations de tresse**) Dans S_n, avec $\tau_i := (i, i+1)$, montrer que pour tout $1 \leqslant i, j \leqslant n$, on a

$$\tau_i \tau_j = \tau_j \tau_i, \qquad \text{si} \qquad |i - j| > 1,$$

et

$$\tau_i \tau_j \tau_i = \tau_j \tau_i \tau_j, \qquad \text{si} \qquad |i - j| = 1.$$

Exercice 1.30. On considère la fonction

$$\gamma : S_n \to \mathbb{Z}_2 \qquad \text{avec} \qquad \gamma(\sigma) := (\ell(\sigma) \bmod 2).$$

(a) Montrer que $\gamma(e) = 0$, et que $\gamma(\tau_i) = 1$ pour tout $1 \leqslant i < n$.

(b) Soit $\sigma\tau \in S_n$. Par récurrence sur $\ell(\sigma)$, montrer que $\ell(\sigma\tau) = (\ell(\sigma) + \ell(\tau) \bmod 2)$.

(c) Montrer que $\gamma(\sigma\tau) = \gamma(\sigma)\gamma(\tau)$, pour tout $\sigma, \tau \in S_n$.

Exercice 1.31. (a) Décomposer en cycles disjoints les permutations dans S_3 et dans S_4.

Exercice 1.32. [**Démonstration de la Proposition 1.14**] Soit $\gamma = (a_1, \ldots, a_p) \in S_n$ un p-cycle, alors

(a) $\gamma^{-1} = (a_1, a_p, a_{p-1}, \ldots a_2)$ est un p-cycle ;

(b) $\mathrm{ord}(\gamma) = p$.

(c) le signe de γ est $(-1)^{p-1}$.

Exercice 1.33. Considérons les deux permutations suivantes de S_9 : $\sigma = 492517683$ et $\tau = 719238465$.

(a) Écrire σ et τ comme produits de cycles disjoints.

(b) Trouver l'ordre de σ et de τ.

(c) Écrire σ et τ comme produits de transpositions adjacentes.

Exercice 1.34. (**Décomposition en cycles**) Soit $\sigma \in S_n$, montrer que σ s'écrit de manière unique comme produit de cycles disjoints (à l'ordre des facteurs près).

Exercice 1.35. (**Classe de conjugaison de S_n**)

(a) Soit $\sigma \in S_n$ et $\alpha = (a_1, \ldots, a_k)$ un k-cycle. Montrer que $\sigma\alpha\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))$ est un k-cycle.

(b) Montrer que $\alpha, \beta \in S_n$ sont conjugués si et seulement si pour tout k, α et β ont le même nombre de k-cycles dans leur décomposition en cycles disjoints.

Exercice 1.36. Soit σ une permutation dans S_n et $\sigma = \gamma_1 \ldots \gamma_k$ sa décomposition de σ en cycles disjoints, alors on a

$$\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(c_1), \mathrm{ord}(c_2), \mathrm{ord}(c_3), \ldots, \mathrm{ord}(c_k)).$$

Montrer de plus que le signe de σ est $(-1)^{n-k}$.

Exercice 1.37. Montrer qu'on peut exprimer les transpositions $\tau_i = (i, i+1)$ comme produit de transpositions de la forme $(1a)$, pour $2 \leqslant a \leqslant n$. En conclure que le groupe S_n est engendré par ces transpositions.

Exercice 1.38. Établir la table de multiplication du groupe diédral D_3. Comparer avec la table du groupe S_3 : que remarque-t-on ?

Exercice 1.39. Soit $D_m = \langle s, r \rangle$ le groupe diédral d'ordre $2m$ engendré par la rotation r d'angle $2\pi/m$, et la symétrie s verticale. Soit $t = sr$, montrer que t est une involution et que $D_m = \langle s, t \rangle$.

Exercices exploratoires

Exercice 1.40 (Le jeu de taquin). Le **jeu de taquin** est constitué d'un damier 4×4 sur les cases duquel sont disposées 15 tuiles carrées, avec une case vide. Les tuiles sont numérotées de 1 à 15. Un mouvement consiste à glisser une tuile voisine de l'emplacement vide, pour remplir cet emplacement.

Les glissements se font verticalement ou horizontalement. La figure suivante illustre une succession de tels mouvements, avec la tuile déplacée marquée en jaune.

À partir d'une configuration donnée, le jeu consiste à se ramener à la configuration de départ ; qui est celle où les tuiles sont rangées dans l'ordre croissant quand on les parcourt selon l'ordre habituel de lecture, avec la case vacante dans le coin inférieur droit. C'est la première configuration dans la figure ci-haut. Ce jeu a apparemment été introduit dans les années 1870, et ses aspects mathématiques sont discutés dans un article de l'American Journal of pure and applied mathematics en 1879. En 1891, Sam Loyd, un concepteur de casse-tête numériques et logiques, a proposé comme défi de trouver comment ramener la configuration suivante à la configuration de départ

Chaque configuration, qui laisse le coin inférieur droit vacant, correspond à une permutation de l'ensemble $\{1, 2, \ldots, 15\}$, qui consiste à lire (dans l'ordre usuel) le numéro des cases. Le groupe G, des transformations (suites de glissements) qui laissent le coin inférieur droit vacant, peut ainsi être considéré comme sous-groupe de S_{15}.

(a) Montrer que G est constitué de permutations paires.

(b) En trouvant assez de générateurs de G, montrer que $G = A_{15}$.

(c) En déduire que le problème de Sam Loyd (voir ci-haut) est impossible à résoudre.

(d) Pour chaque n, déterminer le groupe des transformations de la généralisation au damier $n \times n$ du jeu de taquin.

Pour démontrer plusieurs propriétés fondamentales de la théorie des fonctions symétriques, Schutzenberger [28] à introduit une adaptation du jeu de taquin à la combinatoire des tableaux de Young, ainsi

28. Marcel Paul Schutzenberger (1920-1996), est le grand-père mathématique de deux professeurs du Lacim : le centre de recherche en algèbre, combinatoire, et informatique mathématique de l'UQAM, fondé en 1990.

nommé en l'honneur d'un des pionniers[29] de la théorie de la représentation des groupes.

Exercice 1.41. Soit $\mathcal{A}$ un ensemble fini quelconque, qu'on va ici appeler **alphabet**, dont les éléments sont appelé **lettres**. On dit d'une suite arbitraire $a_1a_2\cdots a_n$, avec $n \in \mathbb{N}$, de lettres dans $\mathcal{A}$, que c'est un **mot** de **longueur** n sur $\mathcal{A}$. On désigne par $\mathcal{A}^*$ l'ensemble des mots de longueur quelconque sur $\mathcal{A}$, et le mot de longueur 0 (ou **mot vide**) est dénoté par 1 ou ε. On munit $\mathcal{A}^*$ de l'opération de **concaténation**, c.-à-d.

$$(a_1a_2\cdots a_n)\cdot(b_1b_2\cdots b_k) := a_1a_2\cdots a_nb_1b_2\cdots b_k,$$

qui consiste simplement à coller ensemble les mots considérés.

(a) Montrer que la concaténation est associative, avec le mot vide comme élément neutre.

(b) Calculer le nombre de mots de longueur n sur un alphabet de longueur de k lettres.

Avec cette opération, on dit que $\mathcal{A}^*$ est le **monoïde libre** sur $\mathcal{A}$.

Exercice 1.42 (Anneaux). La donnée d'une structure **d'anneau** sur un ensemble A, est la donnée de deux opérations sur A. La première est habituellement notée additivement, et elle fait de $(A,+)$ un groupe commutatif, avec neutre noté 0 ; et la seconde est notée multiplicativement et fait de $(A,\cdot)$ un monoïde, avec neutre noté 1. On dit que l'anneau est **commutatif** si ce monoïde est commutatif. Vérifier que chacune des structures suivantes forme bien un anneau.

(a) On fixe X un ensemble non vide, et soit

$$\mathbb{R}^X = \{f \mid f : X \to \mathbb{R}\}$$

Rappelons qu'on dénote habituellement par 0, et 1 les fonctions constantes de valeur 0 et 1 respectivement ; et que les opérations usuelles sur les fonctions $f+g$, $f\cdot g$, et $(-f)$ sont caractérisées par les égalités

$$\begin{aligned}(f+g)(x) &:= f(x)+g(x),\\ (f\cdot g)(x) &:= f(x)g(x),\\ (-f)(x) &:= -f(x).\end{aligned}$$

On considère sur $\mathbb{R}^X$ la structure d'anneau correspondante.

(b) Avec les mêmes définitions, on considère la structure d'anneau sur $\mathcal{C}(\mathbb{R})$, l'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$.

(c) Pour un anneau unitaire A, et $n \geqslant 1$, on considère la structure d'anneau sur l'ensemble $M_n(A)$ des matrices carrées $n\times n$ à coefficients dans A, avec les opérations habituelles sur les matrices. Bien entendu, la matrice nulle et la matrice identité s'obtiennent en considérant que leurs coefficients correspondent aux éléments 0 et 1 de A, de la manière usuelle.

29. Alfred Young (1863-1942).

(d) Pour A un anneau unitaire commutatif, et n variables $x_1, \ldots, x_n$, on considère l'anneau $A[x_1, \ldots, x_n]$ des polynômes en les variables $x_1, \ldots, x_n$, à coefficients dans A. Les polynômes constants (incluant 0 et 1) correspondent aux éléments de A. Les opérations se définissent de la manière habituelle.

Exercice 1.43. Soit A un anneau commutatif. Montrer que les éléments inversibles de $M_n(A)$ sont les matrices dont le déterminant donne un élément inversible de A. (N.B. Le déterminant est défini de la même façon que pour les matrices réelles.)

Exercice 1.44. Soit $\mathbb{G} = \{a + bi \mid a, b \in \mathbb{Z}\}$, les **entiers de Gauss**, et pour $z \in \mathbb{G}$ soit $N(z) = |z|^2$. Vérifiez que $\mathbb{G}$ est un sous-anneau de $\mathbb{C}$ et que la fonction $N : \mathbb{G} \to \mathbb{N}$ a la propriété $N(xy) = N(x)N(y)$. Montrez que pour tous $x, y \in G, y \neq 0$, il existe $q, r \in \mathbb{G}$ tel que $x = qy + r$ et $N(r) < N(y)$. (Notez que lorsqu'on représente $\mathbb{G}$ dans le plan complexe, on a $N(x) < N(y)$ si et seulement si $|x| < |y|$).

Exercice 1.45 (Les quaternions de Hamilton [30]). Soit $\mathbb{R}^4$ muni de l'addition et de la multiplication suivantes :

$$(a_1, b_1, c_1, d_1) + (a_2, b_2, c_2, d_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2, d_1 + d_2)$$

$$\begin{aligned}(a_1, b_1, c_1, d_1) \cdot (a_2, b_2, c_2, d_2) \quad = \quad & (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2, a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2, \\ & a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2, a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\end{aligned}$$

(a) Vérifier que $(1, 0, 0, 0)$ est un élément neutre pour cette multiplication.

(b) Vérifier que $\mathbb{R}^4$ muni de cette addition et de cette multiplication forme un anneau. On appelle cet anneau l'anneau des quaternions et on le désigne par $\mathbb{H}$.

Exercice 1.46. Pour les valeurs $p = 3, 5, 7, 11, 13$, trouvez le plus petit entier qui donne un générateur pour le groupe multiplicatif du corps $\mathbb{F}_p$ des entiers modulo p.

Exercice 1.47. Soit K un corps fini de caractéristique p et ζ un générateur du groupe cyclique K^*. Montrez que ζ^p est aussi un générateur de K^*.

Exercice 1.48. On dit que $A \subseteq \mathbb{R}$ est **dense** dans $\mathbb{R}$ si et seulement si, pour tout $x \in \mathbb{R}$ et tout $\varepsilon > 0$, on a

$$A \cap \{y \in \mathbb{R} \mid |x - y| < \varepsilon\} \neq \varnothing.$$

(a) Montrer que tout sous-groupe de $(\mathbb{R}, +)$ est ou bien dense dans $\mathbb{R}$, ou bien il existe $n \in \mathbb{R}^+$ tel que $H = n\mathbb{Z}$.

(b) Montrer que tout sous-groupe de $(\mathbb{R}, +)$ est soit dense dans $\mathbb{R}$, soit monogène.

(c) Donner des exemples de sous-groupes non triviaux de $\mathbb{R}$, qui sont dense dans $\mathbb{R}$.

(d) Montrer les énoncés analogues pour le groupe des nombres complexes de normes 1, muni de la multiplication.

30. William Rowan Hamilton (1805-1865).

Exercice 1.49 (Groupes topologiques). Rappelons qu'une **topologie** sur un ensemble E est un sous-ensemble $\mathcal{T}$ de $\mathcal{P}(E)$, dont les éléments sont appelés ouverts. On demande que

(1) $\varnothing \in \mathcal{T}$, et $E \in \mathcal{T}$;

(2) toute intersection finie d'éléments de $\mathcal{T}$ est dans $\mathcal{T}$:

$$O_1 \cap \cdots \cap O_n \in \mathcal{T}, \qquad \text{si} \qquad O_i \in \mathcal{T};$$

(3) toute réunion (pas nécessairement finie) d'éléments de $\mathcal{T}$ est dans $\mathcal{T}$:

$$\bigcup_{i \in I} O_i, \qquad \text{si} \qquad \forall (i \in I)\ O_i \in \mathcal{T}.$$

Une fonction **continue** entre deux espaces topologiques $(E_1, \mathcal{T}_1)$ et $(E_2, \mathcal{T}_2)$ est une fonction $f : E_1 \to E_2$ telle que l'image inverse de tout ouvert est un ouvert, c.-à-d. $f^{-1}(O) \in \mathcal{T}_1$ pour tout $O \in \mathcal{T}_2$. Par exemple, la topologie habituelle sur $\mathbb{R}^n$ consiste à dire que $O \subseteq \mathbb{R}^n$ est ouvert si et seulement si pour tout $x \in O$ il existe $\varepsilon > 0$ tel que

$$\{y \in \mathbb{R}^n \mid \operatorname{dist}(x, y) < \varepsilon\} \subseteq O,$$

avec la distance euclidienne habituelle $\operatorname{dist}(x, y)$. On a une topologie sur $\mathcal{M}_n$ qui correspond à considérer que $\mathcal{M}_n = \mathbb{R}^{n \times n}$. Un **homéomorphisme** d'espaces topologiques est une fonction continue bijective, dont l'inverse est continu.

Un groupe **topologique** est un groupe muni d'une topologie, et dont l'opération est continue, ainsi que le passage à l'inverse, c.-à-d. pour tout $g \in G$ on a des fonctions continues $h \mapsto g \cdot h$, $h \mapsto h \cdot g$ et $h \mapsto h^{-1}$. Les groupes de Lie sont des cas particuliers de groupes topologiques. Un isomorphisme de groupes topologiques est un isomorphisme de groupes qui est aussi un homéomorphisme.

(a) Montrer que $\mathbb{R}^n$ avec l'addition vectorielle est un groupe topologique.

(b) Montrer que GL_n, $O(n)$, $SO(n)$, et SL_n sont des groupes topologiques, avec la multiplication de matrices.

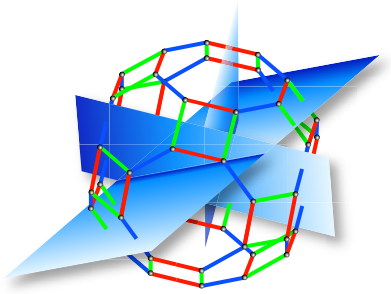
(c) Montrer que si $(E, \mathcal{T})$ est un espace topologique, alors l'ensemble

$$\mathcal{H}(E, E) := \{f \mid f : E \to E,\ f \text{ homéomorphisme}\},$$

avec la composition de fonctions comme opération, est un groupe.

Chapitre 2

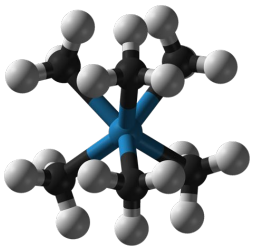
Actions de groupes



Dans ce chapitre nous allons étudier les actions de groupes, c'est-à-dire des fonctions

$$f : G \times E \longrightarrow E,$$

avec de bonnes propriétés qui assurent que f « respecte » l'opération de groupe. Intuitivement, la fonction f exprime en quoi le groupe G permet de « transformer » les éléments de E. Dans un tel contexte, on interprète $f(g, x)$, pour $g \in G$ et $x \in E$, comme une certaine transformation de x selon g.



Hexaméthyltungstène.

C'est souvent la compréhension de ses actions qui permet de bien voir quel est le rôle que joue un groupe donné en mathématiques, ou dans d'autres domaines des sciences. En effet, reformulé pour des physiciens, c'est essentiellement le « principe de relativité » de Galilée[1] qui veut qu'une loi de la physique soit exprimée de façon indépendante de l'observateur. En ce sens, les chimistes utilisent la théorie des groupes pour identifier la forme d'une molécule. Pour exemple, une telle étude permet de déterminer que la molécule d'hexaméthyltungstène $W(CH_3)_6$ à la forme décrite à la figure ci-contre.

Nous allons aussi développer un outil puissant pour l'étude des groupes : le Théorème de Lagrange[2] qui concerne une généralisation du quotient $(\mathbb{Z}, +)$ par son sous-groupe $(n\mathbb{Z}, +)$, donnant le groupe $(\mathbb{Z}_n, +) = (\mathbb{Z}/n\mathbb{Z}, +)$.

1. Galilei Galileo, 1564–1642.
2. Joseph Louis Lagrange (1736–1813).

2.1 Groupes opérants sur des ensembles

On dit qu'un groupe G **opère (à gauche)** sur un ensemble E, si on a une fonction

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

on écrit habituellement $g \cdot x$ pour $f(g, x)$, telle que pour tout $x \in E$, et tout $g_1, g_2 \in G$ on ait

(1) $e \cdot x = x$, où e désigne le neutre de G, et

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

On dit aussi que f est une **action** de G sur E, ou encore que G **agit** sur E par f. Bien entendu, il peut y avoir plusieurs actions différentes d'un groupe sur le même ensemble. Pour G agissant sur E, et x dans E, **l'orbite** de x, notée $\mathrm{Orb}(x)$, est l'ensemble de tous les points de E de la forme $g \cdot x$, pour g parcourant G. En formule,

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

Il y a deux cas extrêmes. Le premier est le cas où il y a une seule orbite, on dit alors que l'action est **transitive**. Le deuxième cas est celui où chaque orbite ne contient qu'un seul élément, on dit alors que l'action est **triviale**. On désigne par E/G **l'ensemble des orbites** de l'action, c.-à-d.

$$E/G = \{\mathrm{Orb}(x) \mid x \in E\};$$

et on constate aisément la proposition suivante.

Proposition 2.1. *Deux orbites distinctes, d'une action de G sur E, sont forcément disjointes.*

Démonstration. Voir exercice 2.1. ■

Une autre façon d'interpréter la démonstration de cette proposition est de dire que l'action induit une relation d'équivalence sur E, définie en posant $x \equiv y$, si et seulement si $\mathrm{Orb}(x) = \mathrm{Orb}(y)$. L'ensemble E/G est alors le quotient de E par la relation d'équivalence, les classes d'équivalences sont les orbites ; et E se décompose de façon unique comme une réunion d'orbites disjointes [3]

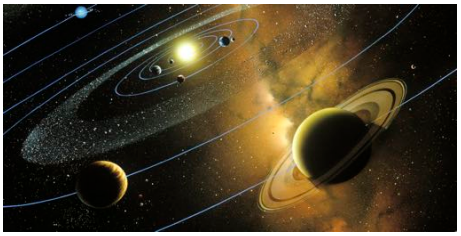
$$E = \sum_{\mathcal{O} \in E/G} \mathcal{O}. \tag{2.1}$$

Autrement dit, si E/G est fini, et si $x_1, x_2 \ldots, x_n$ sont des représentants des diverses classes d'équivalences concernées, alors

$$E = \mathrm{Orb}(x_1) + \mathrm{Orb}(x_2) + \cdots + \mathrm{Orb}(x_n), \tag{2.2}$$

3. On utilise ici la notation $A + B$ pour l'union d'ensembles disjoints A et de B, plutôt que d'autres notations comme $A \uplus B$. Cette notation s'étend aux sommations.

où l'utilisation de la somme entre ensembles souligne qu'on a $\mathrm{Orb}(x_i) \cap \mathrm{Orb}(x_j) = \varnothing$, pour tout $i \neq j$. C'est la **partition en orbites disjointes** de E. Le **stabilisateur** de x, noté $\mathrm{Stab}(x)$, est l'ensemble des éléments de G qui **fixe** x, c.-a-d. que $g \cdot x = x$. En formule, $\mathrm{Stab}(x) := \{g \in G : g \cdot x = x\}$. Il est facile de voir (exercice) que c'est un sous-groupe de G. Parmi les exemples classiques, on a les suivants, plus ou moins classés selon le domaine des mathématiques concerné.



Orbites (selon la NASA).

Un sous-ensemble A de E est dit **stable** ou **invariant** pour l'action de G, si on a $g \cdot x \in A$ pour tout $x \in A$, c.-à-d.

$$g \cdot A \subseteq A, \qquad \text{pour tout} \qquad g \in G.$$

On peut alors restreindre l'action à A, pour obtenir une action $G \times A \to A$. On dit que c'est une **sous-action**. Les orbites d'une action de G sur E correspondent aux plus petits sous-ensembles non vides de E qui sont invariants pour l'action de G. Un sous-ensemble invariant A est forcément une réunion d'orbites, puisque $x \in A$ implique alors $\mathrm{Orb}(x) \subseteq A$.

Ensembles et fonctions. Si G agit sur E, alors on peut se servir de cette action pour construire des actions de G sur les constructions ensemblistes faites à partir de E. Ainsi, on peut faire agir G sur le produit cartésien $E \times E$, en posant

$$G \times (E \times E) \longrightarrow (E \times E), \qquad \text{avec} \qquad g \cdot (x, y) := (g \cdot x, g \cdot y),$$

pour $(x, y) \in E \times E$. Il est facile de vérifier directement que ceci donne bien une action de G. Autre exemple, si $\mathcal{P}(E)$ désigne l'ensemble des parties (sous-ensembles) de E, alors on a l'action

$$G \times \mathcal{P}(E) \longrightarrow \mathcal{P}(E), \qquad \text{avec} \qquad g \cdot A := \{g \cdot x \mid x \in A\}, \tag{2.3}$$

pour A dans $\mathcal{P}(E)$. En particulier, l'ensemble vide est toujours un point fixe pour cette dernière action, c.-à-d. $g \cdot \varnothing = \varnothing$. Il y a un grand nombre d'autres actions qui peuvent ainsi être construites. Ainsi, on a l'action de G sur l'ensemble $\mathrm{Fonct}(F, E)$ des fonctions de F vers E, quelque soit F. En effet, pour $f : F \to E$ et g dans G, il suffit de considérer la fonction $(g \cdot f) : F \to E$, définie en posant $(g \cdot f)(x) := g \cdot (f(x))$, pour tout x dans E. Encore une fois, c'est une action de G :

$$G \times \mathrm{Fonct}(F, E) \longrightarrow \mathrm{Fonct}(F, E), \qquad \text{avec} \qquad (g, f) \mapsto g \circ f.$$

L'étude des actions de groupes sur les ensembles finis correspond à une grande part de la combinatoire moderne. Un des problèmes typiques consiste à décrire explicitement la partition en orbites de telles actions. C'est souvent un problème difficile. On verra plus tard comment le groupe symétrique joue un rôle central dans ce contexte.

Transformations du plan. Pour $G = (\mathbb{R}, +)$, et $E = \mathbb{C}$, on a l'action

$$\mathbb{R} \times \mathbb{C} \to \mathbb{C}, \qquad \text{avec} \qquad (r, z) \mapsto r + z,$$

qui correspond aux **translations horizontales** du plan des complexes. L'orbite $\mathrm{Orb}(z)$ de $z \in \mathbb{C}$ correspond à la droite horizontale qui passe par z, et $\mathrm{Stab}(z) = \{0\}$. On obtient donc $\mathbb{C}$ comme réunion d'orbites correspondant aux droites horizontales. Encore pour $G = (\mathbb{R}, +)$ et $E = \mathbb{C}$, mais maintenant

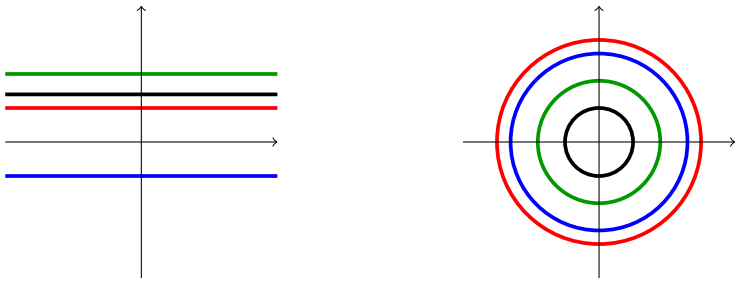
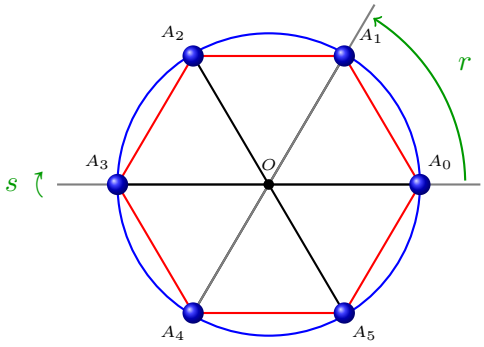


FIGURE 2.1 – Orbites respectives, dans $\mathbb{C}$, pour les actions par translations ou rotations.

avec l'action $\mathbb{R} \times \mathbb{C} \to \mathbb{C}$, avec $(\theta, z) \mapsto e^{i\theta} z$, correspondant aux **rotations centrales** du plan des complexes. Pour $z \in \mathbb{C}$, l'orbite $\mathrm{Orb}(z)$ est donc le cercle de centre 0 passant pas z. Encore une fois, $\mathrm{Stab}(X) = \{e\}$. Enfin, pour $G = (\mathbb{R}^*, \cdot)$ et $E = \mathbb{C}$, on a l'action $\mathbb{R}^* \times \mathbb{C} \to \mathbb{C}$, avec $(r, z) \mapsto rz$, qui multiplie un nombre complexe par un réel non nul. Ce sont les **homothéties** du plan. Pour $z \in \mathbb{C}$, $z \neq 0$, l'orbite $\mathrm{Orb}(z)$ correspond à la droite de direction z, à laquelle on enlève l'origine, et que $\mathrm{Stab}(z) = \{1\}$. D'autre part, pour $z = 0$, l'orbite est $\mathrm{Orb}(0) = \{0\}$, et $\mathrm{Stab}(0) = \mathbb{R}^*$.

Plus généralement, on s'intéresse à des groupes de transformations linéaires d'espaces vectoriels. On peut alors définir des actions de ces groupes sur les constructions faisant intervenir les espaces vectoriels de départ (produis directs, produits tensoriels, etc.). Il y a là de nombreuses connexions avec plusieurs des domaines des mathématiques et de la physique.



Le groupe D_6 agit sur l'hexagone.

Les isométries d'un polygone, groupe diédral. Pour un entier $m \geqslant 3$, on considère le polygone plan régulier convexe P_m à m sommets $A_0 \ldots, A_{m-1}$ inscrits dans le cercle unité de centre O. Le **groupe diédral** D_m est le groupe des isométries du plan qui préserve P_m. On a donc que D_3 est le groupe des isométries du triangle, D_4 celui du carré, D_5 celui du pentagone, D_6 celui de l'hexagone, (voir la figure ci-contre), etc. On observe qu'un élément $f \in D_4$ (par exemple) est déterminé par une permutation des sommets A_0, A_1, A_2, A_3, où il est pratique de poser

$A_k := A_{(k \bmod 4)}$ en général. On a donc $A_4 = A_0$, $A_5 = A_1$ etc. Parmi les éléments de D_4 on retrouve : l'identité e, la rotation r de centre 0 qui envoie A_k sur A_{k+1}, la rotation r^2 de centre 0 qui envoie A_k sur A_{k+2}, la rotation r^3 de centre 0 qui envoie A_k sur A_{k+3}, etc. On remarque que $r^4(A_0) = A_4 = A_0$ donc $r^4 = e$. De plus, on a la symétrie orthogonale s, d'axe OA_0, la symétrie orthogonale t dont l'axe est la médiatrice du segment $[A_0, A_1]$, la symétrie orthogonale s' d'axe OA_1 et la symétrie orthogonale t' dont l'axe est la médiatrice du segment $[A_1, A_2]$. On observe que

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

On vérifie que ce sont les seuls éléments de D_4, et donc

$$D_4 = \{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$$

est d'ordre $2 \cdot 4 = 8$. Plus généralement, pour $m \geqslant 3$, on considère s la **symétrie orthogonale** d'axe OA_0, et r la **rotation** de centre O et d'angle $2\pi/m$. On a alors

$$\begin{aligned} s(O) &= O \quad \text{et} \quad s(A_i) = A_{m-i}, \text{ pour tout } 1 \leqslant i \leqslant m-1, \\ r(A_i) &= A_{i+1}, \text{ pour tout } 1 \leqslant i \leqslant m-1, \text{ et } r(A_{m-1}) = A_0. \end{aligned}$$

Les transformations s et r préservent P_m, d'où on a la proposition suivante.

Proposition 2.2. *Soit $m \in \mathbb{N}$, $m \geqslant 3$, alors*

(1) *$s, r \in D_m$. De plus, $\mathrm{ord}(s) = 2$, $\mathrm{ord}(r) = m$, et $srs = r^{-1}$.*

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

Démonstration.

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

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

Ainsi $rsrs$ fixe plus de trois points du plan, donc $rsrs = e$. D'où la relation $srsr = e$.

(2) Les seules isométries qui préservent P_m sont :

(i) Les rotations d'angles $2k\pi/m$, c'est-à-dire, les r^k $(e = r^0)$.

(ii) Les symétries d'axe OA_k et celles passant par les médiatrices des segments $[A_i, A_{i+1}]$ (qui peuvent être les mêmes, selon que si m est pair ou impair) : c'est à dire les sr^{m-k}.

D'où le résultat. ∎

La relation $rsrs = e$ suffit à construire D_m, pour peu que l'on sache que $s^2 = e$ et $r^m = e$, on dit que D_m est **présenté** par les **générateurs** s, r et les **relations** $s^2 = r^m = srsr = e$. On note ce fait comme suit

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

L'action par conjugaison de G sur G. Une autre action intéressante, de G sur lui-même, est celle obtenue en posant

$$G \times G \to G, \qquad \text{avec} \qquad (g, h) \mapsto g \cdot h := ghg^{-1}.$$

C'est l'action par **conjugaison**. On a bien $e \cdot h = ehe^{-1} = ehe = h$ et

$$(g_1 g_2) \cdot h = (g_1 g_2)h(g_1 g_2)^{-1} = g_1 g_2 h g_2^{-1} g_1^{-1} = g_1(g_2 \cdot h)g^{-1} = g_1 \cdot (g_2 \cdot h).$$

On dit de $\mathrm{Orb}(h)$ que c'est la **classe de conjugaison** de h, et de ses éléments que ce sont les **conjugués** de h. On dit du stabilisateur

$$\mathrm{Stab}(h) = \{g \in G \mid ghg^{-1} = h\} = \{g \in G : gh = hg\},$$

que c'est le **centralisateur** de h, et on le dénote alors $C(h)$. Plus généralement, on considère sur $E = \mathcal{P}(G)$, l'action de

$$G \times \mathcal{P}(G) \to \mathcal{P}(G), \qquad \text{avec} \qquad g \cdot X = gXg^{-1} := \{gxg^{-1} : x \in X\}.$$

Si $X = H$ est un sous-groupe de G, alors $\mathrm{Orb}(H)$ consiste en les conjugués de H, et

$$\mathrm{Stab}(H) = \{g \in G : gHg^{-1} = H\}$$

est appelé **normalisateur** de H. On le dénote alors par $N(H)$. Si $N(H) = G$, on dit de H que c'est un sous-groupe **normal**. Autrement dit, H est normal si et seulement si on a

$$H = gHg^{-1}, \qquad \text{pour tout} \qquad g \in G.$$

On écrit alors, $H \lhd G$. Il est clair que H est toujours un sous-groupe normal de $\mathrm{Stab}(H)$, c.-à-d. $H \lhd \mathrm{Stab}(H)$. Nous allons voir plus loin que la notion de sous-groupe normal joue un rôle très important.

2.2 Actions de S_E

Pour un ensemble (fini) E, on a plusieurs actions intéressantes du groupe $G = S_E$. La plus simple est **l'action naturelle**

$$S_E \times E \to E, \qquad \text{avec} \qquad g \cdot x = g(x).$$

Plusieurs exemples s'obtiennent par des constructions ensemblistes classiques. Ainsi, on a l'action de S_E sur les produits cartésiens

$$E^n := \begin{cases} E \times E^{n-1} & \text{si } n > 1, \\ E & \text{si } n = 1. \end{cases}$$

obtenue en posant

$$\sigma \cdot (x_1, x_2, \ldots, x_n) = (\sigma(x_1), \sigma(x_2), \ldots \sigma(x_n)),$$

pour les $x_i \in E$. On a aussi l'action de E sur l'ensemble $\mathcal{P}(E)$ des parties de E (voir (2.3)), obtenue en posant

$$\sigma \cdot A := \{\sigma(x) \mid x \in A\}.$$

Combinant ces deux constructions, on a l'action de S_E sur l'ensemble des **relations** sur E, c.-à-d. sur l'ensemble $\mathcal{P}(E \times E)$:

$$\sigma \cdot \mathcal{R} := \{(\sigma(x), \sigma(y)) \mid (x, y) \in \mathcal{R}\}.$$

D'autres exemples classiques correspondent à des actions de S_E sur l'ensemble $\mathcal{F}(E)$ des fonctions de E vers E. Ainsi, on a l'action par **conjugaison**

$$\sigma \cdot f := \sigma \circ f \circ \sigma^{-1},$$

pour $f : E \to E$; l'action par **composition à gauche**

$$\sigma \cdot f := \sigma \circ f;$$

ou l'action par **composition à droite**

$$\sigma \cdot f := f \circ \sigma^{-1}.$$

Observons, dans ce dernier cas, que le fait d'utiliser l'inverse assure qu'on a bien une action, puisque

$$\begin{aligned} (\sigma \circ \tau) \cdot f &= f \circ (\sigma \circ \tau)^{-1} \\ &= f \circ (\tau^{-1} \circ \sigma^{-1}) \\ &= (f \circ \tau^{-1}) \circ \sigma^{-1} \\ &= (\tau \cdot f) \circ \sigma^{-1} \\ &= \sigma \cdot (\tau \cdot f). \end{aligned}$$

On peut poursuivre ce genre de constructions dans toutes sortes de directions. C'est en fait le coeur d'une grande partie de la combinatoire, qui donne lieu entre autres à la Théorie des espèces de structures [4]. Les notions de stabilisateurs, d'orbites, et plusieurs autres concepts de la théorie des groupes y jouent un rôle

4. Développée par les mathématiciens de l'UQAM dans les années 1980. Voir un texte d'introduction disponible sur le web à l'adresse : http://bergeron.math.uqam.ca/files/2013/11/book.pdf.

fondamental. Exploitant des idées de la théorie des groupes (et de la théorie des catégories), la théorie des espèces (combinatoire) permet de résoudre de manière élégante (algébrique) un grand nombre de problèmes concernant des objets comme les fonctions, les graphes, les arbres, les permutations, les dérangements, les partitions, les ordres, etc. En plus de donner des fondements rigoureux à un large pan de la combinatoire énumérative, la théorie des espèces donne un riche contexte algébrique pour la construction de nouvelles espèces de structures. En plus de riches liens avec de nombreux domaines des mathématiques, elle a des applications en Physique théorique (diagrammes de Feynman, Théorie quantique des champs, etc.), Informatique théorique (Structures de données, Analyse de la complexité d'algothimes, Programmation fonctionnelle, Sémantique des langages de programmation, etc.), et dans l'étude de certains processus stochastiques.

2.3 Classes modulo un sous-groupe

S'inspirant de la relation de congruence modulo n dans $\mathbb{Z}$:

$$a \equiv b \pmod{n} \qquad \text{ssi} \qquad (-a) + b \in n\mathbb{Z},$$

on considère la définition suivante. Pour H sous-groupe d'un groupe G, on considère la **congruence à gauche** modulo H sur G, définie en posant

$$g_1 \equiv g_2 \pmod{H} \iff g_1^{-1} q_2 \in H. \tag{2.4}$$

C'est une relation d'équivalence (voir la preuve ci-dessous), et on dit de la classe d'équivalence

$$x\,H = \{g\,h \,|\, h \in H\}, \qquad \text{pour} \qquad g \in G,$$

que c'est une **classe à gauche** modulo H. On note G/H l'ensemble quotient résultant, c.-à-d.

$$G/H := \{g\,H \mid g \in G\} \tag{2.5}$$

Pour G noté additivement, on écrit $x + H$ pour la classe d'équivalence de x modulo H. On retrouve alors la notation « usuelle » pour le cas $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, à savoir $k + n\mathbb{Z}$, pour $k \in \mathbb{Z}$; et l'ensemble quotient est bien $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Observons que $xH = H$ si et seulement si $h \in H$. Observons aussi que, pour $x \neq y$, il est fort possible que $xH = yH$. On vérifie (exercice) que cela ne se produit que dans la cas où

$$xH = yH \iff x^{-1}yH = H \iff y^{-1}xH = H \iff x^{-1}y \in H. \tag{2.6}$$

C'est le **critère d'égalité** de classes à gauche.

De façon toute similaire, on a une notion de **congruence à droite** modulo H, définie en posant

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

On pose aussi que $Hx = \{hx \,|\, h \in H\}$. C'est la **classe à droite** modulo H. L'ensemble quotient résultant est noté $H\backslash G$. Comme pour les classes à gauche, on a la caractérisation suivante des classes à droite

$$y \in xH \qquad \text{ssi} \qquad y^{-1} \in Hx^{-1}.$$

Pour G est abélien, les deux notions de classes à gauche et à droite coïncident, c.-à-d. que $xH = Hx$ pour tout $x \in G$. On dit d'un sous-groupe tel que $xH = Hx$, pour tout $x \in H$, qu'il est **normal**. Nous approfondirons ces notions au Chapitre 4. Il est évident que tout groupe G contient au moins deux sous groupes normaux, dit **triviaux**. Il s'agit simplement du sous-groupe $\{e\}$, et de G lui-même. Un groupe est dit **simple** si et seulement si ces seuls sous-groupes normaux sont ces deux sous-groupes triviaux. Un de aspect fondamental de cette notion est que : tout groupe fini peut se « construire » à partir des groupes finis simples (voir Section 3.7).

Le fait que H soit un sous-groupe assure que la relation $\equiv$, définie en (2.4), est bien une « relation d'équivalence ». En effet la réflexivité découle de ce que $e \in H$, puisqu'alors $x^{-1}x = e \in H$, et donc $x \equiv x$; la symétrie découle du fait que tout élément est inversible dans H, ce qui fait que $y^{-1}x = (x^{-1}y)^{-1} \in H$, et donc $x \equiv y$ si et seulement si $y \equiv x$; et la transitivité du fait que H est stable. En effet, si $x \equiv y$ et $y \equiv z$ alors $x^{-1}y \in H$ et $y^{-1}z \in H$, et alors on a

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

Reste à montrer que la classe d'équivalence de x est bien $xH = \{xh \,|\, h \in H\}$. On raisonne comme suit. Par définition, pour $y \in xH$, on a $h \in H$ tel que $y = xh$. Donc $x^{-1}y = h \in H$ et il s'ensuit que $x \equiv y$. Réciproquement, soit $y \equiv x$, alors $h = x^{-1}y \in H$. Il existe donc $h \in H$ tel que $y = xh$, ce qui prouve l'affirmation.

Une propriété importante des classes à gauche (ou à droite) est soulignée par la proposition suivante.

Proposition 2.3. *Soit G un groupe et $H \leqslant G$, alors*

(1) *Pour tout $x \in G$, xH, Hx et H ont même cardinal.*

(2) *Les ensembles quotients G/H et $H\backslash G$ sont en bijection.*

Démonstration. On montre d'abord que la fonction $h \mapsto xh$ est une bijection de H sur xH (exercice). Posons $f(xH) = Hx^{-1}$, pour tout $x \in G$. La fonction $f : G/H \to H\backslash G$ est **bien définie**, à savoir que

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

Montrons que f est une bijection. Elle est injective, puisqu'on a

$$f(xH) = f(yH) \iff Hy^{-1} = Hx^{-1} \iff xH = yH.$$

De plus, f est surjective, puisque $Hx \in H\backslash G$ entraîne$f(x^{-1}H) = H(x^{-1})^{-1} = Hx$. ∎

Cette proposition rend possible la définition suivante, pour tout H sous-groupe d'un groupe G. On dit du cardinal de l'ensemble quotient G/H (qui est égal au cardinal de $H\backslash G$) que c'est **l'indice** de H dans G. On le note

$$[G : H] := |G/H| \tag{2.7}$$

Lorsque G/H est un ensemble fini, on dit que H est **d'indice fini** dans G. Par exemple, on a $[\mathbb{Z} : n\mathbb{Z}] = n$. L'indice peut donc être fini même si G et H sont infinis. Le théorème suivant permet de calculer l'indice.

Théorème 2.4 (Théorème de Lagrange)**.** *Soit G un groupe fini et $H \leqslant G$ alors*

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

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

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

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

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

Corollaire 2.5. *Pour G un groupe fini d'ordre n, alors $x^n = e$ pour tout $x \in G$. De plus, si p est premier, alors G est un groupe cyclique.*

Démonstration. Soit $x \in G$, d'ordre d. Le théorème de Lagrange assure que d divise $|G| = n$. On a donc $k \in \mathbb{N}$ tel que $n = d\,k$, et on a donc

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

La seconde partie est laissée en exercice. ∎

La prochaine étape de notre cheminement consiste à faire agir G sur G/H. Pour ce faire, on exploite l'action de G sur lui-même par **multiplication à gauche** :

$$G \times G \to G, \qquad \text{avec} \qquad g \cdot h := gh.$$

On a bien $e \cdot h = eh = h$ et $(g_1 g_2) \cdot h = (g_1 g_2)h = g_1(g_2 h) = g_1 \cdot (g_2 \cdot h)$, puisque c'est l'associativité de l'opération de G. Plus généralement, on considère $E = \mathcal{P}(G)$ c'est-à-dire l'ensemble des parties de G. On a alors l'action de

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

Si $X = H$ est un sous-groupe de G, on a vu plus haut que les orbites $\mathrm{Orb}(H)$ sont les classes à gauche de H, et $\mathrm{Stab}(H) = \{g \in G : gH = H\} = H$. Pour tout sous-groupe H, le groupe G agit sur le quotient G/H en posant

$$G \times G/H \to G/H, \qquad \text{avec} \qquad h \cdot (gH) := (hg)H. \tag{2.8}$$

Il faut alors vérifier que cela est une « bonne définition ». En effet, rien n'assure (a priori) que l'effet de h sur g_1H sera le même que sur g_2H, pour $g_1 \neq g_2$ avec $g_1H = g_2H$. Le calcul suivant montre que cela est toujours le cas.

Nous sommes maintenant presque prêts à aborder la classification des actions de groupes.

2.4 Orbites vs stabilisateurs

Comme on va le voir à la section 2.6, la proposition suivante ouvre la porte à la description de « toutes » les actions de groupes. Elle suggère aussi que la compréhension des orbites est importante.

Proposition 2.6. *Soit G un groupe agissant sur un ensemble E, et $x \in E$, alors la relation « l'élément x est dans l'orbite de l'élément y » est une relation d'équivalence sur E. En conséquence, E est la réunion disjointe des orbites.*

Démonstration. Par définition, $x \in \mathrm{Orb}(y)$ si et seulement si il existe $g \in G$ tel que $y = g \cdot x$. La relation considérée est donc $x \sim y$, si et seulement si il existe $g \in G$ tel que $y = g \cdot x$. En prenant $g = e$ on voit que « $\sim$ » est réflexive. Comme $y = g \cdot x$ si et seulement si $x = g^{-1} \cdot y$, la relation est symétrique. Enfin, vérifier la transitivité correspond à constater que $z = h \cdot y$ et $y = g \cdot x$ entraîne que $z = (hg) \cdot x$. Autrement dit, le fait qu'on ait une relation d'équivalence correspond exactement aux propriétés qui caractérisent une action. ∎

On relie l'étude des orbites à l'étude des stabilisateurs via la proposition suivante. De plus la proposition révèle un lien important entre stabilisateurs d'éléments qui se trouvent dans une même orbite. Cela nous sera fort utile pour comprendre les actions transitives.

Proposition 2.7. *Pour tout groupe G opérant sur un ensemble E, et $x \in E$, on a les propriétés suivantes.*

(1) *Il y a une bijection entre* $\mathrm{Orb}(x)$ *et les classes à gauche de* $\mathrm{Stab}(x)$. *En particulier, si* $\mathrm{Orb}(x)$ *est fini, alors* $\mathrm{Stab}(x)$ *est d'indice fini et* $|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)]$.

(2) *Si* $\mathrm{Orb}(x) = \mathrm{Orb}(y)$, *alors* $\mathrm{Stab}(x)$ *et* $\mathrm{Stab}(y)$ *sont conjugués.*

Démonstration.

(1) Considérons les ensembles $\mathrm{Orb}(x)$ et $\{g\,\mathrm{Stab}(x) : g \in G\}$ (ce sont les éléments $G/\mathrm{Stab}(x)$). Notons que

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

On peut donc définir la fonction

$$\mathrm{Orb}(x) \to \{g\,\mathrm{Stab}(x) : g \in G\}, \qquad \text{avec} \qquad g \cdot x \mapsto g\,\mathrm{Stab}(x),$$

qui donne une bijection.

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

$$\begin{aligned} h \cdot (g \cdot x) = g \cdot x \quad &\iff \quad (hg) \cdot x = g \cdot x \\ &\iff \quad g^{-1}hg \cdot x = x \\ &\iff \quad g^{-1}hg \in \mathrm{Stab}(x), \end{aligned}$$

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

Corollaire 2.8. *Soit G opérant sur E, où G et E sont finis. Soit $E = \mathrm{Orb}(x_1) + \ldots + \mathrm{Orb}(x_n)$, la partition de E en orbites pour cette action (voir (2.2)). Alors*

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

Ce corollaire est à la base de beaucoup d'applications des groupes finis. En particulier, on a la suivante. Pour l'action de G sur lui-même par conjugaison, on a la partition en orbites

$$G = \mathrm{Orb}(h_1) + \ldots + \mathrm{Orb}(h_r),$$

pour un bon choix de éléments $h_1, \ldots, h_r$. Notons que

$$h \in Z(G) \quad \iff \quad \mathrm{Orb}(h) = \{h\},$$

où on rappelle que $Z(G)$ désigne le centre de G. On conclut donc qu'on a la formule

$$|\,G\,| = |\,Z(G)\,| + \sum_{h_i \notin Z(G)} [G : C(h_i)] \tag{2.9}$$

2.5 Lemme de Burnside

Quand E et G sont finis, avec G agissant sur E, on s'intéresse souvent à calculer le nombre d'orbites de E pour cette action. Le lemme[5] de Burnside permet de transformer ce « difficile » calcul en un calcul plus facile du nombre moyen d'éléments de E qui sont fixés par les éléments de G. On désigne $\mathrm{fix}_g(E)$, l'ensemble des **points fixés** par g dans E, c.-à-d.

$$\mathrm{fix}_g(E) := \{x \in E \mid g \cdot x = x\}.$$

On a alors l'énoncé suivant.

Théorème 2.9 (Lemme de Burnside-Cauchy-Frobenius)**.** *Pour toute action d'un groupe fini G, sur un ensemble fini E, on a*

$$|E/G| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{fix}_g(E)\,|.$$

Démonstration. La preuve consiste simplement à calculer le cardinal de l'ensemble

$$|\,\{(g,x) \in G \times E \mid g \cdot x = x\}\,|,$$

de deux manières. D'abord,

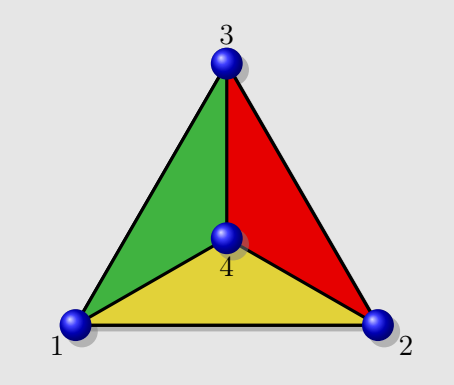
$$|\,\{(g,x) \in G \times E \mid g \cdot x = x\}\,| = \sum_{g \in G} |\,\mathrm{fix}_g(E)\,|.$$

Utilisant la première partie de la proposition 2.7, c.-à-d. $|G| = |\mathrm{Stab}(x)| \cdot |\mathrm{Orb}(x)|$, on trouve d'autre part

$$\begin{aligned}
|\,\{(g,x) \in G \times E \mid g \cdot x = x\}\,| &= \sum_{x \in E} |\mathrm{Stab}(x)| \\
&= \sum_{x \in E} \frac{|G|}{|\mathrm{Orb}(x)|} \\
&= |G| \sum_{\mathcal{O} \in E/G} \left(\sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} \right) \\
&= |G| \sum_{\mathcal{O} \in E/G} 1, \\
&= |G| \cdot |E/G|.
\end{aligned}$$

Comparant les deux calculs, on trouve l'énoncé de la proposition. ∎

5. Il n'est pas dû à William Burnside (1852–1927), qui l'a énoncé comme un lemme dans son livre : *The Theory of Groups of Finite Order*. Il semble plutôt dû à Ferdinand Georg Frobenius (1849-1917), ou même à Augustin Louis Cauchy (1789 -1857) avant lui. Depuis lors, c'est le surnom qu'on donne couramment à cet énoncé.



Coloration du tétraèdre.
(La face cachée est bleue)

Un exemple typique est le suivant. On considère l'ensemble des colorations des faces d'un tétraèdre avec k couleurs, à symétries près du tétraèdre. Autrement dit, deux colorations sont considérées comme équivalentes si on peut passer de l'une à l'autre via une des symétries du tétraèdre. Si les sommets du tétraèdre sont étiquetés $\{1,2,3,4\}$, les faces s'identifient aux 4 sous-ensembles à trois éléments $A := \{1,2,3\}$, $B := \{1,2,4\}$, $C := \{1,3,4\}$, et $D := \{2,3,4\}$. Une coloration est une simplement une fonction $\{A,B,C,D\} \longrightarrow \{1,2\ldots,k\}$. Les symétries du tétraèdre correspondent exactement aux permutations de $\{A,B,C,D\}$, et l'action de σ sur une coloration f est de produire la nouvelle coloration

$$\sigma \cdot f : \{A,B,C,D\} \longrightarrow \{1,2\ldots,k\},$$

où $(\sigma \cdot f)(x) := f(\sigma^{-1}(x))$. La présence de l'inverse assure qu'on a bien une action, puisqu'on calcule que

$$\begin{aligned}(\tau \cdot (\sigma \cdot f))(x) &= (\sigma \cdot f))(\tau^{-1}(x)) \\ &= f(\sigma^{-1}(\tau^{-1}(x)) \\ &= f((\tau \circ \sigma)^{-1}(x) \\ &= (\tau \circ \sigma) \cdot f(x).\end{aligned}$$

Pour comprendre quand une coloration est fixée par une permutation, il suffit de considérer sa

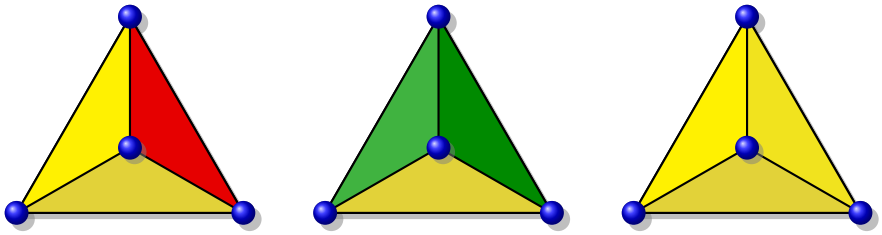


FIGURE 2.2 – Autres colorations possibles du tétraèdre (la face cachée aussi est colorée).

décomposition en cycles disjoints. En effet, toutes les faces qui sont dans le même cycle doivent être colorées de la même façon, et c'est la seule condition qui doit être satisfaite. Le nombre de colorations laissées fixes par une permutation est donc $k^{\gamma(\sigma)}$, où $\gamma(\sigma)$ est le nombre de cycles de γ (incluant les cycles de longueur 1). Rappelons que le type cyclique des permutations considérées est l'un des 5 partages de 4, et que le nombre de permutations ayant ces types respectifs sont : une permutation de type 1111 (qui fixe k^4 colorations), six permutations de type 211 (qui fixent k^3 colorations), trois permutations de type 22 (qui fixent k^2 colorations), huit permutations de type 31 (qui fixent k^2 colorations), et six de

type 4 (qui fixent k colorations). En sommant pour les 5 termes, et divisant par 24, on trouve par le lemme de Burnside que le nombre de k-colorations à symétries près du tétraèdre est :

$$\frac{1}{24}(k^4 + 6\,k^3 + 3\,k^2 + 8\,k^2 + 6\,k) = \frac{k(k+1)(k+2)(k+3)}{24} = \binom{k+3}{4}.$$

Les applications de ce genre mènent à la Théorie de Pólya[6], qui considère en général l'énumération des structures discrètes modulo l'action d'un groupe.

2.6 Morphismes d'actions, sommes d'actions, et actions transitives.

Pour comparer deux actions

$$G \times E \to E, \qquad \text{et} \qquad G \times F \to F,$$

de G, on considère les fonctions $\theta : E \to F$ qui « préservent » l'action. Plus précisément, on dit que θ est un **morphisme** d'action, si et seulement si on a

$$\theta(g \cdot x) = g \cdot \theta(x), \tag{2.10}$$

pour tout g dans G, et tout x dans E. Soulignons que le sens de $g \cdot (-)$ est différent à gauche de l'égalité ci-dessus. À gauche, c'est la première action qui est en cause, et à droite la seconde. Si θ est une fonction bijective, alors on dit que c'est un **isomorphisme** d'action. Informellement, deux actions isomorphes sont les « mêmes ». Un des problèmes centraux de la théorie des groupes est de « classifier » toutes les actions d'un groupe, à isomorphisme près. Se restreignant au cas fini pour simplifier l'histoire, une partie de la réponse débute par l'observation suivante. On peut introduire la notion suivante de « somme » d'actions de G. Si G agit sur deux ensembles (disjoints) E et F, on a une action de G sur $E + F$, l'union disjointe des ensembles E et de F. En effet, on défini $G \times (E + F) \to (E + F)$ en posant, pour $z \in (E + F)$, que $g \cdot z$ se calcule avec l'action de G sur E si $z \in E$, et avec l'action de G sur F si $z \in F$. La proposition suivante est alors une traduction directe de la proposition 2.6, où chaque orbite correspond à une composante transitive.

Proposition 2.10. *Pour G et E fini, toute action de G sur E se décompose de façon unique en une somme finie d'actions transitives, c.-à-d. qu'on a un isomorphisme*

$$\varphi : E \longrightarrow E_1 + E_2 + \ldots + E_k,$$

avec k fixé, et les E_i uniques à isomorphisme près et à l'ordre des termes près.

6. Le théorème de Pólya originellement dû à John Howard Redfield, a été redécouvert par George Polya (1887-1985) qui en a souligné les applications à la classification des isomères.

Cette proposition montre que la classification des actions d'un groupe (fini) se ramène à la classification de ses actions transitives (à isomorphisme près). Nous allons voir qu'il y en a un nombre fini. On amorce cette partie de notre histoire avec la proposition suivante, qui ne suppose pas que G ou E soit fini.

Proposition 2.11. *Pour tout sous-groupe H de G, l'action de G sur G/H définie en (2.8) est transitive.*

Démonstration. Il suffit d'observer que toute classe à gauche xH s'obtient évidement de la classe H par l'action de x sur H, c.-à-d. $x \cdot H = x\,H$. ∎

La prochaine étape consiste à montrer que toute autre action transitive $G \times E \to E$, est isomorphe à l'une des actions G/H, pour un bon choix de H. Autrement dit, on cherche une bijection $\theta : E \to G/H$, avec un candidat judicieux du sous-groupe H. La clé est la proposition 2.7. En effet, on a déjà observé que le stabilisateur de l'élément H de G/H est le sous-groupe H (donc H joue deux rôles distincts ici). Cela suggère d'utiliser la stratégie suivante. On choisit $x \in E$ (le choix n'a pas d'importance), et on pose $H := \mathrm{Stab}(x)$. La bijection θ est alors définie en posant

$$\theta(y) := g\,H \qquad \text{ssi} \qquad y = g \cdot x,$$

et nous avons déjà vérifié que cela est une bonne définition. Bien entendu, l'inverse de θ est $\theta^{-1}(g\,H) := g \cdot x$.

Pour achever notre entreprise de classification des actions transitives de G, on doit déterminer quand deux sous-groupes H et K donnent des actions G/H et G/K qui sont isomorphes. On aura alors une « classification » complète (et sans redondance) des actions transitives de G, à isomorphisme d'actions près. La réponse à cette dernière question correspond aussi au cas particulier d'une seule orbite de la Proposition 2.7, et se reformule comme suit.

Théorème 2.12. *Toute action transitive d'un groupe G est isomorphe à une action de la forme G/H, pour H un sous-groupe de G. Deux telles actions G/H et G/K sont isomorphes, si et seulement si H et K sont conjugués. C'est donc dire qu'il existe $g \in G$, tel que $K = g^{-1}\,H\,g$.*

Corollaire 2.13. *Pour G fini, le nombre d'actions transitives distinctes de G est égal au nombre de classes de conjugaison de sous-groupes de G.*

Avec un système de calcul formel, on peut calculer explicitement tous les sous-groupes d'un groupe fini. Dans le cas particulier du groupe symétrique S_4, on obtient qu'il y a 30 tels sous-groupes, qui sont inclus[7] les uns dans les autres de la manière illustrée à la Figure 2.3. Le sous-groupe K_4 (le groupe de Klein) est un sous-groupe normal de A_4, d'ordre 4. On constate qu'il y a 11 classes de conjugaison de sous-groupes de S_4, avec les sous-groupes d'une même classe de même couleur (non étiquetté). Les seuls

7. Un treillis est un ensemble ordonné avec certaines bonnes propriétés. Pour plus de détails, voir ici.

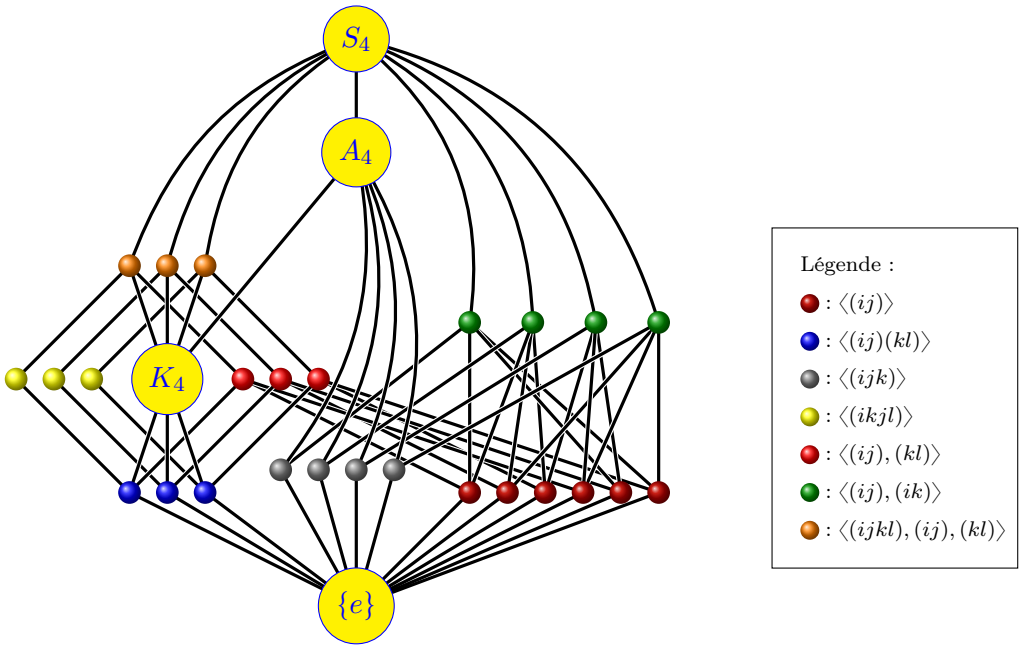


FIGURE 2.3 – Le treillis des 30 sous-groupes de S_4.

sous-groupes normaux sont ceux qui sont étiquettés, c.-à-d. $\{e\}$, K_4, A_4 et S_4. Les premiers termes de la suite donnant le **nombre de sous-groupes** de S_n sont

$$1, 1, 2, 6, \mathbf{30}, 156, 1455, 11300, 151221, 1694723, 29594446, 404126228, 10594925360, 175238308453, \ldots$$

D'autres termes sont connus, le plus grand étant le 18-ième qui égal à

$$7598016157515302757.$$

Pour l'instant, il semble difficile d'aller beaucoup plus loin dans le calcul de ces nombres. Les premiers termes de la suite donnant le **nombre de classes de conjugaisons** de sous-groupes de S_n sont :

$$1, 1, 2, 4, \mathbf{11}, 19, 56, 96, 296, 554, 1593, 3094, 10723, 20832, 75154, 159129, 686165, 1466358, 7274651, \ldots$$

Il ne semble pas qu'on en connaisse d'autres termes, et aucune formule n'est connue pour cette suite. Seul un calcul « brutal » permet de l'obtenir. La proposition suivante donne une autre indication de l'importance du groupe des permutations, sur laquelle nous reviendrons à la Section 3.5

Proposition 2.14. *Soit G qui opère sur E. Pour $g \in G$, posons*

$$\gamma_g : E \to E, \qquad \text{avec} \qquad \gamma_g(x) := g \cdot x.$$

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

Démonstration. Montrons que γ_g est surjectif et injectif. Pou montrer la surjectivité, on considère $x \in E$ quelconque. On a

$$x = e \cdot x = (gg^{-1}) \cdot x = g \cdot (g^{-1} \cdot x) = \gamma_g(g^{-1} \cdot x).$$

Il s'ensuit que chaque $x \in E$ possède au moins un antécédent par γ_g. Pour l'injectivité, supposons $\gamma_g(x) = \gamma_g(y)$, on a alors

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

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

Cette proposition donne une fonction $\gamma : G \to S_E$, définie par $\gamma(g) := \gamma_g$. C'est un exemple de ce qu'on appelle un « morphisme » de groupes au Chapitre 3. On verra alors que tout morphisme de groupe $G \to S_E$ correspond à une action de G sur E.

2.7 Le système de cryptographie RSA

La généralisation suivante du petit théorème de Fermat [8] (due à Gauss [9]), se comprend bien du point de vue de la théorie des groupes. Ce n'est qu'un cas particulier du théorème de Lagrange. Comme on va le voir, le théorème rend possible [10] le système de cryptographie à clé publique « RSA ».

Théorème 2.15 (Fermat-Euler). *Soit $n \in \mathbb{N}^*$ et a un entier premier avec n alors*

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

où φ est l'indicatrice d'Euler [11].

En effet, comme a est premier avec n, le sous-groupe $\langle a \rangle$ qu'il engendre dans $\mathbb{Z}_n^\times$ est un groupe multiplicatif d'ordre $\varphi(n)$. La conclusion est alors assurée par Lagrange.

8. Pierre Fermat, 1601-1665.
9. Carl Friedrich Gauss (1777-1855).
10. Cela n'est qu'une de ses nombreuses applications.
11. Leonhard Euler, 1707-1783.

Les systèmes de cryptographie à clé publique sont de grand intérêt dans le contexte des transactions informatiques. L'algorithme RSA [12] est le plus connu, et il très simple à décrire avec les outils dont nous disposons maintenant. La sécurité du système RSA est basée sur le fait que la puissance modulaire est très facile à calculer, mais très difficile à inverser. Cette dernière difficulté repose sur la difficulté (même avec des ordinateurs très puissants) de factoriser de très grands nombres en nombres premiers. Nous n'avons besoin que du lemme suivant.

Lemme 2.16. *Si $n = pq$ avec $p \neq q$ nombres premiers, alors $\varphi(n) = (p-1)(q-1)$.*

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

Le système RSA. Chaque intervenant, on l'appelle souvent Bob, se construit une **clef publique**, c.-à-d. un couple d'entiers (n, e), de la manière suivante.

(a) En premier lieu, Bob se génère [13] un couple de très grands nombres premiers p et q, qu'il gardera secret. Bob restera donc le seul à connaître p et q. Et il calcule $n := pq$.

(b) Bob génère ensuite un troisième grand entier e quelconque, mais relativement premier à $\varphi(n) = (p-1)(q-1)$. L'entier e est donc inversible dans $\mathbb{Z}_{\varphi(n)}$.

La clef publique (n, e) est alors partagée avec tous les autres intervenants (toujours en gardant p et q secret). Parmi ces autres intervenants se trouve Alice, qui cherchera à communiquer secrètement avec Bob. Pratiquement, il est impossible [14] de retrouver p et q à partir de n. Grâce à sa connaissance de p et q, Bob est en mesure de calculer facilement (avec l'algorithme d'Euclide) sa **clef privée**, c.-à-d. l'entier d tel que $\overline{d}$ est l'inverse de e dans $\mathbb{Z}_{\varphi(n)}$. Sans connaître p et q, la valeur de $\varphi(n)$ est « très » difficile à calculer (encore une fois dans un temps raisonnable), et c'est donc le cas aussi pour d. Voilà, tout est en place.

Chiffrement d'un message. Pour envoyer son message M (c'est un nombre plus petit que n) à Bob, Alice procède comme suit. Au moyen de la clef publique (n, e) de Bob, Alice calcule $C \equiv M^e \pmod{n}$. Cela peut se faire très efficacement et rapidement. Alice publie le message C à l'intention de Bob. Tous les intervenants connaissent la clé publique de Bob, et le message codé d'Alice.

12. Rivest, Shamir et Adleman (1977).
13. Il existe des algorithmes "simples" et efficaces pour ce faire.
14. Ce n'est pas un théorème, mais on ne sait pas le faire dans un temps raisonnable (au moins quelques années), même avec les ordinateurs les plus puissants.

Déchiffrement du message. Seul Bob peut déchiffrer le message C d'Alice. Il lui suffit de calculer C^d modulo n. Le Théorème d'Euler-Fermat assure que le résultat est bien M, le message original d'Alice.

Démonstration. En effet,

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

car $ed \equiv 1 \pmod{\varphi(n)}$ ($\overline{e} = \overline{d}^{\,-1}$). Donc si M est premier avec n, en vertu du théorème

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

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

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

Si p ne divise pas M, alors le petit théorème de Fermat assure que

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

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

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

Puisque $M < n$, le résultat de ce calcul est M. ■

Exemple. En pratique, on s'attend à travailler avec de grands nombres premiers p et q comme les suivants :

$$\begin{aligned} p &= 6323829139021280799955082643342097928393309970508654992131084968361905198610474978033098 01 \\ q &= 5582183332721710984303341149394307079249672541973129902496045727580819388677553000169641 27. \end{aligned}$$

L'exposant e est lui aussi un grand nombre, comme

$$\begin{aligned} e &= 1506509050075534087481820828159849293596322698526815858095047097397384852311042480456938047100981883026555380108188664760543107881755421364073741062056055236872239468000258122420 19. \end{aligned}$$

Illustrons plutôt le processus avec de petits nombres comme $p = 7$ et $q = 13$. On a $n = 7 \cdot 13 = 91$, $\varphi(n) = (7-1)(13-1) = 72$;, et on peut choisir $e = 23$. Alors,

(a) La clef publique est $(91, 23)$.

(b) Après calcul, on trouve la clef privée est $d = 47$. En effet $23 \cdot 47 = 1 + 15 \cdot 72 \equiv 1 \pmod{\varphi(n)}$.

Supposons que le message est $M = 8$, alors le message crypté est $C = (M^e \bmod n) = (8^{23} \bmod 91) = 57$. Pour décoder le message, on trouve bien

$$(C^d \bmod n) = (57^{47} \bmod 91) = 8.$$

2.8 Le groupe des isométries du cube

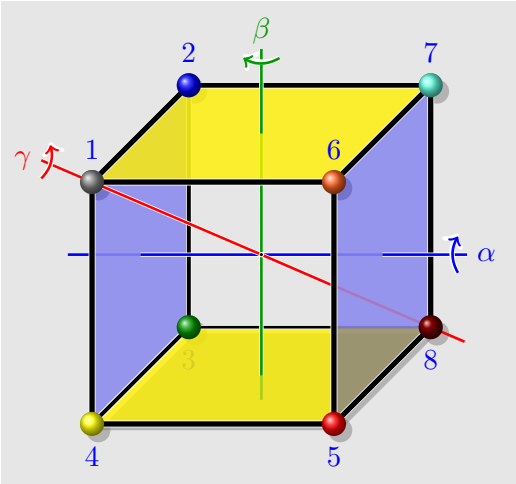


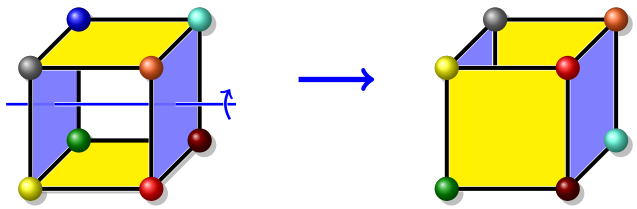
FIGURE 2.4 – Rotations du cube.

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

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

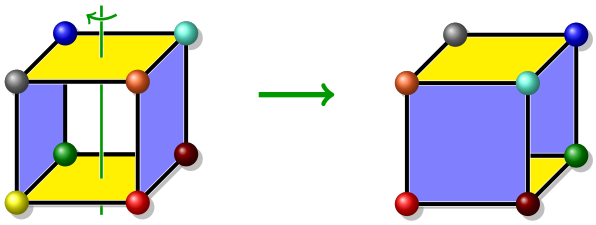
pour laquelle on ne conserve que les isométries qui préservent le cube, c'est-à-dire le stabilisateur de $\mathcal{C}$ pour cette action. Nous allons déterminer ce groupe à isomorphisme près. Puisque les distances et les angles sont conservés par le groupe, on peut considérer que G permute les sommets entre eux. Ceci permet de considérer G comme un groupe de permutation des sommets, via le morphisme de restriction $\rho : G \to S_8$, où $\rho(g) := g\,|_{\{\text{sommets}\}}$. Un premier élément de G est α, la rotation d'angle $\pi/2$ autour de l'axe vertical passant par le centre des faces 1234 et 5678. Comme permutation, décomposée en cycles, α s'exprime comme

$$\alpha = (1234)(5678).$$



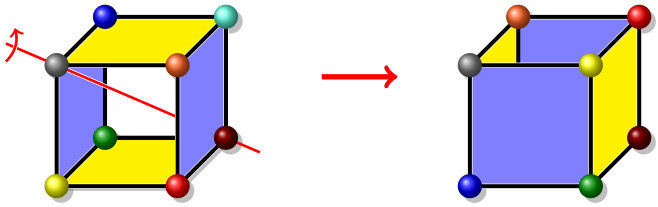
C'est donc un élément d'ordre 4. De même, on a la rotation β, d'angle $\pi/2$ autour de l'axe vertical passant par le centre des faces 1276 et 4385, qui s'exprime comme la permutation d'ordre 4

$$\beta = (1276)(4385).$$



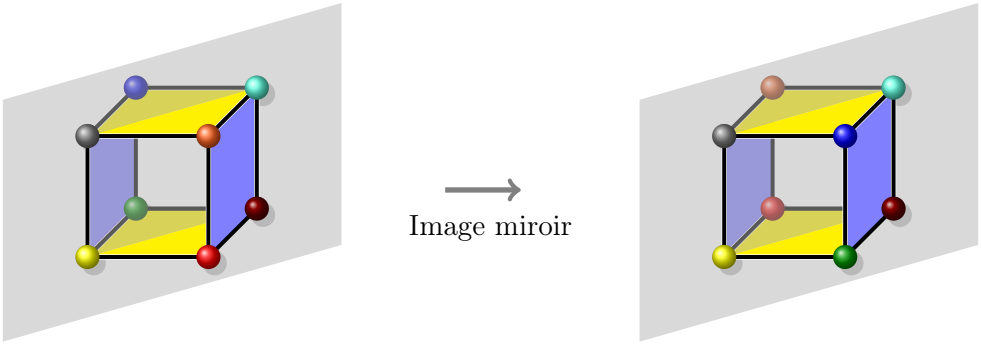
De plus, on considère γ, la rotation d'angle $2\,\pi/3$ autour de l'axe qui passe par les points 1 et 8, telle que

$$\gamma = (246)(357).$$



C'est donc un élément d'ordre 3, avec 1 et 8 comme points fixes ; et on calcule que $\gamma^2 = (264)(375)$. Le groupe engendré par α, β et γ donne toutes les isométries du cube qui en respecte l'orientation [15]. Restent les « réflexions » du cube, c.-à-d. les isométries d'ordre 2 qui renverse l'orientation. Pour les obtenir, il suffit d'ajouter la réflexion par rapport au plan 1487, dont la décomposition cyclique est

$$\delta := (26)(35),$$



et dont les points fixes sont 1, 4, 7 et 8. On veut vérifier que le groupe G est engendré par α, β, γ, et δ. Pour le voir, considérons l'orbite du sommet 1 ; on a clairement

$$\begin{aligned} \alpha(1) = 2, \quad \alpha^2(1) = 3, \quad \alpha^3(1) = 4, \\ \beta(1) = 2, \quad \beta^2(1) = 7, \quad \beta^3(1) = 6, \end{aligned}$$

15. Quand on situe sa main droite en 1, avec l'index et le pouce pointant respectivement vers 2 et 4, alors le majeur pointe vers 6. Pour l'orientation inverse, on utilise la même règle avec la main gauche.

et on calcule directement que

$$\alpha\beta^2 = (18)(27)(36)(45), \qquad \text{et} \qquad \alpha^2\beta^2 = (15)(28)(37)(46),$$

d'où $\alpha\beta^2(1) = 8$, et $\alpha^2\beta^2(1) = 5$. On s'ensuit que l'orbite de 1 est

$$\mathrm{Orb}(1) = \{1, 2, 3, 4, 5, 6, 7, 8\}.$$

Autrement dit, il a une seule orbite pour l'action de G. C'est donc une action transitive. En vertu du théorème sur les actions transitives, on a que

$$8 = |\mathrm{Orb}(1)| = [G : \mathrm{Stab}(1)] = |G|/|\mathrm{Stab}(1)|,$$

il suffit donc de calculer $|\mathrm{Stab}(1)|$ pour connaître l'ordre de G. On sait que γ et δ fixent 1, et donc $\mathrm{Stab}(1)$ contient le sous-groupe qu'ils engendrent. Comme $\gamma^3 = e$ et $\delta^2 = e$, il suffit de vérifier par calcul direct qu'on a

$$\gamma\delta = (37)(46) = \delta\gamma^2, \qquad \gamma^2\delta = (24)(57) = \delta\gamma,$$

pour conclure qu'on a (au moins [16]) les 6 éléments distincts suivants dans $\mathrm{Stab}(1)$:

$$e, \quad \gamma, \quad \gamma^2, \quad \delta, \quad \gamma\delta, \quad \text{et} \quad \delta\gamma.$$

On constante donc que $|\mathrm{Stab}(1)| \geqslant 6$, ce qui entraîne que $|G| \geqslant 48$.

Nous allons obtenir une borne supérieure pour l'ordre de G, grâce à un théorème d'un chapitre ultérieur. On remarque que les isométries du cube échangent entre elles les diagonales de ce cube. En effet, une isométrie envoie les paires de points les plus éloignés du cube dans des paires de points de la même nature. Les diagonales sont précisément les segments dont les extrémités sont de telles paires. On peut donc considérer la restriction de G au groupe des permutations de ces quatre diagonales. Celles-ci correspondent aux quatre sous-ensembles de paires de sommets $\{1, 8\}$, $\{2, 5\}$, $\{3, 6\}$ et $\{4, 7\}$. On a donc un morphisme

$$\theta : G \to S_\Gamma, \qquad \text{pour} \qquad \Gamma := \{\{1, 8\}, \{2, 5\}, \{3, 6\}, \{4, 7\}\},$$

obtenu en posant

$$\theta(g)(\{i, j\}) := \{g(i), g(j)\}.$$

Soit

$$\sigma := (18)(25)(36)(47),$$

l'application **antipode** par rapport au centre du cube. C'est un élément de G, qui laisse globalement fixe chaque diagonale de sorte que sa restriction à l'ensemble des quatre diagonales est l'application identité. D'autre part, soit g est un élément de G tel que $\theta(g) = e$ autre que l'identité. Comme $g \neq e$, on peut choisir i tel que $g(i) \neq i$. Pour fixer les idées, disons que $i = 2$. On a $\theta(g)(\{i, j\}) = \{i, j\}$, pour

16. En fait il n'y en a pas d'autres, mais nous n'avons pas besoin de le savoir aux fins de l'argument.

toutes les diagonales. En particulier, $\theta(g)(\{2,5\}) = \{g(2), g(5)\} = \{2,5\}$, et donc $g(2) = 5$ (puisqu'on a supposé $g(2) \neq 2$). Comme on doit aussi conserver les autres distances, par exemple celle entre 1 et 2, on doit avoir que $g(1)$ est voisin de $g(2)$. Cela force $g(1) = 8$. De même on trouve $g(3) = 6$ et $g(4) = 7$. On trouve donc que g est forcément égal à σ. On a donc $\ker(\theta) := \{e, \sigma\} = \{g \in G \mid \theta(g) = e\}$ (nous allons revenir plus tard sur cette notation).

Par le théorème des isomorphismes (voir 4.4), on obtient

$$|G|/|\ker(\theta)| = |G/\ker(\theta)| \leqslant |S_\Gamma|$$

Dans notre cas, cela correspond à $|G|/2 \leqslant 24$. En conclusion globale, on trouve qu'il y a $|G| = 48$ isométries du cube.

2.9 Espaces homogènes

Dans son « programme d'Erlangen » de 1878, Felix Klein propose d'approcher systématiquement la géométrie via la théorie des groupes. Cela correspond à des actions transitives de groupes. Plus précisément, on suppose que E est un **espace topologique** sur lequel un groupe G agit transitivement. Intuitivement, le groupe détermine la géométrie de E. Comme, par transitivité de l'action, on peut passer de n'importe quel point $x \in E$ à n'importe quel autre point $y = g \cdot x$, on dit que l'espace E est **homogène** parce que tous les points se « comporte » de la même façon. Utilisant le Théorème 2.12, la construction d'espaces homogènes se ramène à choisir un groupe G, et un sous-groupe H de G. Parmi les groupes qui jouent un rôle particulièrement intéressant dans ce contexte, on retrouve les groupes de Lie GL_n, $O(n)$, ou encore GA_n (le groupe général affine). Ainsi, la géométrie de la sphère correspond à $O(n)/O(n-1)$, et la géométrie affine à GA_n/GL_n.

Au 7e congrès international de mathématiques, qui a eu lieu en 1924 à Toronto, le mathématicien français Elie Cartan à fait une présentation invitée intitulée *La théorie des groupes et les recherches récentes en géométrie différentielles*. On a accès sur le web à cette référence historique, expliquant pour un public général cette approche et ses liens avec la théorie de la relativité. La section suivante approfondie, dans un cas particulier, certaines questions reliées à ce sujet.

2.10 Le groupe $\mathrm{SL}_2(\mathbb{Z})$

Le groupe des matrices $n \times n$, à coefficients entiers et de déterminant 1, est dénoté $\mathrm{SL}_n(\mathbb{Z})$. Le cas particulier $n = 2$ est déjà très intéressant. On peut montrer qu'il est engendré par les matrices

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \text{et} \qquad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

avec les relations $S^4 = \mathrm{Id}$, et $(ST)^6 = \mathrm{Id}$. La matrice T est d'ordre infini, puisque

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \qquad \text{pour tout} \qquad n \in \mathbb{Z}.$$

Comme $T = S^3\,(ST)$, le groupe $\mathrm{SL}_2(\mathbb{Z})$ est aussi engendré par les deux matrices S et ST.

On observe que

$$S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}, \qquad \text{et} \qquad T^n\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}.$$

On peut exploiter ceci, et la division euclidienne dans $\mathbb{Z}$, pour déterminer comment écrire toute matrice de $\mathrm{SL}_2(\mathbb{Z})$ comme produit de la forme

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & n_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & n_2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & n_k \\ 0 & 1 \end{pmatrix},$$

avec $n_i \in \mathbb{Z}$. Pour trouver une telle expression, on procède avec l'algorithme suivant [17], en faisant agir le groupe sur lui-même par multiplication à gauche. Si $c \neq 0$ et $|a| \geqslant |c|$, applicant la division euclidienne de a par c, on trouve q et r tels que $a = qc + r$, avec $|c| > r \geqslant 0$. Alors, on observe que

$$T^{-q}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r & b-qd \\ c & d \end{pmatrix}, \qquad \text{et donc} \qquad ST^{-q}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ r & b-qd \end{pmatrix}.$$

On réapplique l'étape précédente, jusqu'à ce qu'on se retrouve dans le cas $c = 0$. Or, les seules matrices dans $\mathrm{SL}_2(\mathbb{Z})$ de la forme $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ sont les matrices

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix} = S^2T^n,$$

puisque leur déterminant est $ad = 1$, ce qui force $a = d = 1$ ou $a = d = -1$. Par exemple, on trouve ainsi que

$$\begin{pmatrix} 17 & 46 \\ 7 & 19 \end{pmatrix} = T^2ST^{-3}ST^{-2}ST^{-2}ST^2S^2.$$

Action de $\mathrm{SL}_2(\mathbb{Z})$ sur le plan hyperbolique. Sans tenir compte de l'aspect géométrique, une réalisation du plan hyperbolique $\mathbf{H}$ est simplement l'ensemble des nombres complexes dons la partie imaginaire est positive :

$$\mathbf{H} := \{z = x + iy \mid x, y \in \mathbb{R}, \quad y \geqslant 0\}.$$

17. C'est essentiellement l'algorithme d'Euclide.

Pour chaque matrice dans $\mathrm{SL}_2(\mathbb{Z})$, on a une transformation, dite de **Möbius**[18], du plan hyperbolique, qui correspond à

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az+b}{cz+d}. \tag{2.11}$$

Comme on calcule que

$$\begin{aligned}
\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \left(\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \cdot z \right) &= \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \left(\frac{a_2 z + b_2}{c_2 z + d_2} \right) \\
&= \frac{a_1(a_2 z + b_2)/(c_2 z + d_2) + b_1}{c_1(a_2 z + b_2)/(c_2 z + d_2) + d_1} \\
&= \frac{a_1(a_2 z + b_2) + b_1(c_2 z + d_2)}{c_1(a_2 z + b_2) + d_1(c_2 z + d_2)} \\
&= \frac{(a_1 a_2 + b_1 c_2) z + (a_1 b_2 + b_1 d_2)}{(c_1 a_2 + d_1 c_2) z + (c_1 b_2 + d_1 d_2)} \\
&= \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix} \cdot z
\end{aligned}$$

C'est bien une action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbf{H}$, puisqu'on vérifie aussi par calcul direct que $A \cdot z$ est dans $\mathbf{H}$, pour

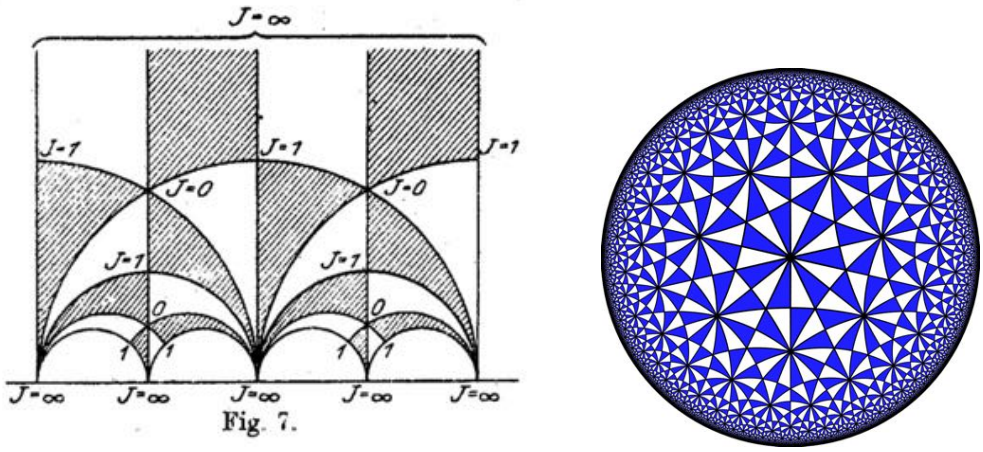


FIGURE 2.5 – SL_2-pavage de Klein du plan hyperbolique, et sa version circulaire.

tout $A \in \mathrm{SL}_2(\mathbb{Z})$. On remarque, pour A dans $\mathrm{SL}_2(\mathbb{Z})$, la matrice $(-A)$ donne la même transformation que A, c.-à-d. $A \cdot z = (-A) \cdot z$. Travailler modulo l'identification de ces deux matrices donne lieu au

18. August Ferdinand Mobius (1790-1868). Voir le vidéo expliquant les transformations de Möbius.

groupe modulaire. Les transformations qui correspondent aux générateurs S et T sont respectivement

$$S : z \mapsto -1/z, \qquad \text{et} \qquad T : z :\mapsto z + 1,$$

et ces transformations engendrent toutes celles qui correspondent à (2.11). Chaque orbite de cette action contient un et un seul élément dans la région

$$\{z \in \mathbb{C} \mid |\Re(z)| < 1/2,\ |z| > 1\},$$

et le plan $\mathbf{H}$ se pave avec des copies de cette région selon l'action de $\mathrm{SL}_2(\mathbb{Z})$, comme l'illustre la Figure 2.5 dûe à Klein [19], dont il attribue l'idée à Dedekind [20].

2.11 Actions linéaires

Pour une action $G \times V \to V$, où V est un espace vectoriel (sur $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, etc.), on dit que l'action est **linéaire** si (en plus des axiomes d'actions) on a

(a) $g \cdot (x + y) = g \cdot x + g \cdot y$, pour tout $x, y \in V$ et $g \in G$, et

(b) $g \cdot (\alpha\, x) = \alpha\, (g \cdot x)$, pour tout x, g, et α un scalaire.

On dit aussi d'une telle action que c'est une **représentation linéaire** du groupe G, et on parle de la représentation [21] V. Si G agit sur deux espaces vectoriels V et W, alors on a une action linéaire de G sur l'espace vectoriel $V \oplus W$, définie en posant $g \cdot (v + w) := g \cdot v + g \cdot w$. Dans ce cas, on dit qu'on a une **somme** d'actions. Bien entendu, on a la somme de plusieurs actions. Tout comme dans le cas des actions, un **isomorphisme** allant d'une action linéaire $G \times V \to V$ à une action linéaire $G \times W \to W$ est une transformation linéaire inversible $\theta : V \to W$, telle qu'on ai le diagramme **commutatif**

$$\begin{array}{ccc} G \times V & \longrightarrow & V \\ {\scriptstyle \mathrm{Id}\times\theta}\downarrow & & \downarrow{\scriptstyle \theta} \\ G \times W & \longrightarrow & W, \end{array}$$

ce qui signifie que $g \cdot \theta(v) = \theta(g \cdot v)$, pour tout $v \in V$ et tout $g \in G$. L'étude et la classification des actions linéaires (à isomorphisme près) font l'objet de la théorie de la représentation des groupes, qui est un domaine de recherche particulièrement actif. Pour un groupe fini, les deux théorèmes de base

19. *Uber die Transformation der elliptischen Funktionen und die Auflosung der Gleichungen funften Grades*, Mathematische Annalen, 1878.

20. Julius Wilhelm Richard Dedekind (1831-1916).

21. Malgré le fait qu'on puisse avoir deux actions différentes sur le même espace V, c'est l'habitude dans le domaine de s'exprimer ainsi. Dans la plupart des cas, cela ne porte pas à confusion.

de la théorie[22] affirment d'abord que toute action se décompose de manière unique (à isomorphisme près) en une somme d'actions dites « irréductibles » ; puis qu'il y a un nombre fini (à isomorphisme près) d'actions irréductibles, pour chaque groupe G. Le nombre de ces actions irréductibles est égal au nombre de classes de conjugaison d'éléments du groupe. En un certain sens, c'est une version plus riche du fait qu'on a une partition en orbites pour un ensemble muni d'une action. Par exemple, une action du groupe des permutations S_3 agit sur $\mathbb{R}^3$ correspond à poser

$$\sigma \cdot (x_1, x_2, x_3) := (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}((2)}, x_{\sigma^{-1}(3)}).$$

La présence de l'inverse assure qu'on a bien une action. En effet, on calcule qu'on a bien

$$\begin{array}{rcll} \tau \cdot (\sigma \cdot (x_1, x_2, x_3)) & = & \tau \cdot (y_1, y_2, y_3), & \text{où} \qquad y_i = x_{\sigma^{-1}(i)} \\ & = & (y_{\tau^{-1}(1)}, y_{\tau^{-1}(2)}, y_{\tau^{-1}(3)}), & \\ & = & (x_{\sigma^{-1}(\tau^{-1}(1))}, x_{\sigma^{-1}(\tau^{-1}(2))}, x_{\sigma^{-1}(\tau^{-1}(3))}, & \\ & = & (x_{(\tau\sigma)^{-1}(1)}, x_{(\tau\sigma)^{-1}(2)}, x_{(\tau\sigma)^{-1}(3)}, & \\ & = & (\tau\sigma) \cdot (x_1, x_2, x_3). & \end{array}$$

La linéarité est évidente. La décomposition de cette action en action irréductible correspond à décomposer l'espace vectoriel $\mathbb{R}^3$ en somme directe de deux sous-espaces V et W, où

(a) $V = \{(x, x, x) \mid x \in \mathbb{R}\}$, autrement dit une droite de $\mathbb{R}^3$;

(b) $W = \{(x, y, z) \mid x + y + z = 0\}$, autrement dit un plan orthogonal à la droite V.

L'invariance de ces sous-espaces se déduit facilement de la définition. Comme V est de dimension 1, il est forcément irréductible. On montre aussi que W est irréductible. Une autre façon d'envisager tout ceci est de constater que tout vecteur s'écrit de manière unique comme combinaison linéaire de la forme

$$(x, y, z) = a\,(1, 1, 1) + b\,(1, -1, 0) + c\,(1, 0, -1),$$

où il suffit de poser

$$a = (x + y + z)/3, \qquad b = (x - 2\,y + z)/3, \qquad \text{et} \qquad c = (x + y - 2\,z)/3.$$

L'effet de toute permutation sur (x, y, z) est de la forme

$$\sigma \cdot (x, y, z) = a\,(1, 1, 1) + b_\sigma\,(1, -1, 0) + c_\sigma\,(1, 0, -1),$$

pour certaines (jolies) expressions b_σ et c_σ. Le calcul des expressions en question est un exercice intéressant et important à savoir-faire pour d'autres contextes du genre. C'est un des défis de la théorie de la représentation des groupes. Par exemple, la théorie de la représentation des groupes cycliques mène à la notion de transformée de Fourier discrète pour effectuer ces calculs.

22. Pour des espaces vectoriels sur des corps de caractéristique 0. Le cas de caractéristique fini est aussi connu, mais la théorie est plus complexe.

Invariants polynomiaux. Une famille d'exemples particulièrement importante consiste à considérer les groupes finis de matrices $n \times n$ agissant sur les polynômes à n variables. On a donc $G \leqslant \mathrm{GL}_n(\mathbb{C})$ un tel groupe, avec

$$g = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

qui agit sur un polynôme $f(z_1, z_2, \dots, z_n)$, en remplaçant dans f les variables z_i par

$$z_i \mapsto a_{1i}z_1 + a_{2i}z_2 + \ldots + a_{ni}z_n.$$

On dit alors qu'un polynôme f est **G-invariant** si et seulement si on a $g \cdot f = f$, pour tout élément g du groupe G. Cette notion joue un rôle fondamental en théorie de Galois et dans une foule d'autres domaines (comme en physique). En particulier, si G est le groupe des matrices de permutations (c.-à-d. dont les coefficients a_{ij} sont tous 0, sauf un 1 par ligne et un 1 par colonne), on dit des polynômes G-invariants qu'ils sont symétriques, et l'action du groupe correspond à permuter les variables. Plus explicitement, pour $n = 3$, un polynôme $f(x, y, z)$ est symétrique, si et seulement si

$$f(x, y, z) = f(x, y, z) = f(y, x, z) = f(y, z, x) = f(z, x, y) = f(z, y, x),$$

et on a les exemples suivants de tels polynômes

$$\begin{array}{rcl} e_1(x, y, z) & = & x + y + z, \\ e_2(x, y, z) & = & x\,y + x\,z + y\,z \\ e_3(x, y, z) & = & x\,y\,z. \end{array} \tag{2.12}$$

Le cas $n = 3$ du théorème fondamental des polynômes symétriques, dû à Newton [23], affirme que tout polynôme symétrique $f(x, y, z)$ s'exprime comme somme de produit des trois polynômes e_1, e_2, et e_3 ci-dessus. Par exemple, on voit facilement que

$$D(x, y, z) = (x - y)^2(x - z)^2(y - z)^2 \tag{2.13}$$

est un polynôme symétrique. Le théorème de Newton assure qu'on peut trouver une expression pour $D = D(x, y, z)$ en terme de e_1, e_2, et e_3. On trouve en effet que

$$D = e_1^2e_2^2 + 18\,e_1e_2e_3 - 4\,e_2^3 - 4\,e_1^3e_3 - 27\,e_3^2. \tag{2.14}$$

C'est le **discriminant** (l'analogue de $b^2 - 4a\,c$) pour les polynômes de degré 3. Plus explicitement, le polynôme en la variable t

$$(t - x)(t - y)(t - z) = t^3 - e_1\,t^2 + e_2\,t - e_3,$$

23. Sir Issac Newton (1643-1727).

a (au moins) deux racines[24] égales si et seulement si son discriminant est nu, $D = 0$. On observe que l'expression des coefficients e_1, e_2, et e_3 du polynôme (attention aux signes), en terme de ses racines, donne précisément les expressions (2.12). Par exemple, pour le polynôme $t^3+3\,t^2-9\,t+5$, on a $e_1 = -3$, $e_2 = -9$, et $e_3 = -5$. A priori, on ne connaît pas ses racines, et on ne peut utiliser la formule (2.13) pour calculer le discriminant. Par contre, la formule (2.14) est facilement calculable, et on trouve

$$D = (-3)^2(-9)^2 + 18\,(-3)(-9)(-5) - 4\,(-9)^3 - 4\,(-3)^3(-5) - 27\,(-5)^2 = 0.$$

On conclut donc que le polynôme a deux racines égales que l'on ne connaît toujours pas. Autrement dit, le polynôme est de la forme $(t-a)^2(t-b)$, pour certaines valeurs de a et de b qu'on pourrait chercher à trouver, si on le désire.

2.12 Exercices

Exercice 2.1 (Voir solution 2). Pour une action de G sur E. Montrer que tout sous-ensemble invariant de E est une réunion d'orbites, et que l'orbite de tout élément $x \in E$ est le plus petit sous-ensemble invariant contenant x.

Exercice 2.2 (Voir solution 3). Montrer que le groupe A_4 ne possède pas de sous-groupe d'ordre 6 (même si 6 est un diviseur de 12 qui est l'ordre de A_4).

Exercice 2.3 (Voir solution 4). Dans cet exercice nous allons établir des propriétés de base du groupe symétrique S_n.

(a) Considérons l'action naturelle du groupe symétrique S_n sur l'ensemble $\{1, 2, \ldots, n\}$ et soit $\sigma \in S_n$. En considérant l'action induite du sous-groupe $H = \langle\sigma\rangle$ engendré par σ et les orbites de cette action, donner une autre démonstration du fait que σ se décompose en un produit de permutations cycliques disjointes ou cycles disjoints, c.-à-d.

$$\sigma = \underbrace{(i_1, \ldots, i_s)}_{\gamma_1} \ldots \underbrace{(j_1, \ldots, j_t)}_{\gamma_k},$$

avec $\{i_1, \ldots, i_s\} \cap \{j_1, \ldots, j_t\} = \varnothing$. Vérifier que des cycles disjoints commutent entre eux et que la décomposition ci-dessus est unique à l'ordre des facteurs près.

(b) Pour une décomposition d'un entier n sous la forme d'une somme

$$n = \mu_1 + \mu_2 + \ldots + \mu_k, \qquad \text{avec} \qquad \mu_1 \geqslant \mu_2 \geqslant \ldots \geqslant \mu_k \geqslant 1,$$

on dit que $\mu = (\mu_1, \mu_2, \ldots, \mu_k)$ est un **partage** de longueur k de n, et on écrit $\mu \vdash n$. Les μ_i sont les **parts** du partage μ. On désigne $p(n)$ le nombre de partages de n. Par exemple $p(4) = 5$, puisqu'on a les 5 décompositions de 4 suivante

$$4, \quad 3+1, \quad 2+2, \quad 2+1+1, \quad 1+1+1+1.$$

24. Ce sont ici x, y et z.

L'unique décomposition $\sigma = \gamma_1 \dots \gamma_k$ d'une permutation $\sigma \in S_n$, en un produit de cycles disjoints γ_i, détermine un partage du nombre n, pour laquelle μ_i égal à la longueur de γ_i. Montrer que les classes de conjugaison du groupe S_n sont en correspondance bijective avec les partages de n.

(c) Montrer que le nombre de permutations, dans la classe de conjugaison qui correspond à un partage μ, est donné par la formule

$$\frac{n!}{1_1^d d_1! 2_2^d d_2! \cdots n_n^d d_n!} \tag{2.15}$$

où chaque $d_\ell = d_\ell(\mu)$ est le nombre de parts égale à ℓ dans μ.

Exercice 2.4.

(a) Soit $g : \mathbb{C} \to \mathbb{C}$ un automorphisme d'anneaux de $\mathbb{C}$, c.-à-d. un automorphisme du groupe additif $(\mathbb{C}, +)$ mais qui a aussi la propriété que $g(xy) = g(x)g(y)$ pour tous $x, y \in \mathbb{C}$. Vérifier que pour tout $x \in \mathbb{Q}$, on a $g(x) = x$. (Aide : vérifier d'abord que $g(1) = 1$.)

(b) Soit $f \in \mathbb{Q}[X]$ un polynôme à coefficients dans $\mathbb{Q}$, et soit

$$E = \{z \in \mathbb{C} : f(z) = 0\}$$

l'ensemble des racines de f. Soit G le groupe des automorphismes d'anneaux de $\mathbb{C}$. Vérifier que pour tout $z \in E$ et tout $g \in G$ on a $g(z) \in E$, et que l'opération de $G \times E$ dans E définie par $g \cdot z = g(z)$ donne une action de G sur E. (Rappel : l'opération dans le groupe G est la composition des fonctions.)

Exercice 2.5. Soit $f \in \mathbb{Q}[X]$ et G le groupe des automorphismes d'anneau de $\mathbb{C}$. On sait que G agit de façon naturelle sur l'ensemble $L = \{z \in C : f(z) = 0\}$ des racines de f.

(a) Montrer que deux racines de f qui appartiennent à la même orbite doivent être racines d'un même facteur irréductible de f dans $\mathbb{Q}[X]$.

(b) Déduire de (a) que si f n'a pas de racine multiple et que l'action de G sur L n'a qu'une seule orbite, alors f est irréductible dans $\mathbb{Q}[X]$.

Exercice 2.6. Soit un groupe G opérant sur un ensemble E et soit $Y \subseteq E$. Montrer que $\{g \in G : g \cdot y = y, \text{ pour tout } y \in Y\}$ est un sous-groupe de G.

Exercice 2.7. Soit G un groupe et $H \leqslant G$, montrer que

(a) si $x \in G$ alors $xH = H$ si et seulement si $x \in H$;

(b) si $x, y \in G$ alors $xH = yH \iff x^{-1}yH = H \iff y^{-1}xH = H \iff x^{-1}y \in H$;

(c) si G est abélien, alors $xH = Hx$ pour tout $x \in G$;

(d) si $x, y \in G$, alors $y \in xH \iff y^{-1} \in Hx^{-1}$;

(e) si $x \in H$, alors la fonction $h \mapsto xh$ est une bijection de H sur xH.

(f) En déduire que xH, H et Hx ont même cardinal.

Exercice 2.8. On considère $G = S_3$.

(a) Trouver tous les sous-groupes de S_3 ;

(b) Pour tous les sous-groupes H de S_3, calculer G/H.

Exercice 2.9. Soit G un groupe d'ordre p premier, montrer que G est cyclique.

Exercice 2.10. Soit G un groupe et H, K deux sous-groupes finis de G.

(a) Montrer que si $|H|$ et $|K|$ sont premiers entre eux, alors $H \cap K = \{e\}$.

(b) On pose $n = [H : H \cap K]$. Soit $\{x_i \,|\, 1 \leqslant i \leqslant n\}$ un système de représentants des classes de $H/H \cap K$.

(i) Montrer que $\{x_i K \,|\, 1 \leqslant i \leqslant n\}$ est une partition de HK.

(ii) Montrer que

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

Exercice 2.11. Soit G un groupe abélien d'ordre $|G| = nm$ où n et m sont premiers entre eux. Soit H et K deux sous-groupes de G tel que $|H| = n$ et $|K| = m$. Montrer que $G \simeq H \times K$.

Exercice 2.12. Soit G un groupe et $H_1, \ldots, H_n$ des sous-groupes de G **d'indice fini**. Montrer par récurrence sur $n \in \mathbb{N}^*$ que l'indice du sous-groupe $\bigcap_{i=1}^n H_i$ est fini.

Exercice 2.13. Soit G un groupe et $x, y \in G$ d'ordre fini tel que $xy = yx$. Montrer que :

(a) xy est d'ordre fini ;

(b) si $\mathrm{ord}(x) = n$ et $\mathrm{ord}(y) = m$ sont premiers entre eux, alors $\mathrm{ord}(xy) = nm$.

Exercice 2.14. (Formule de l'indice) Soit H un sous-groupe d'indice fini d'un groupe G et $K \leqslant H$. Le but de ce problème est de montrer que K est d'indice fini dans G si et seulement si il est d'indice fini dans H, ainsi que la formule suivante :

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

(a) Si $K \subseteq H$, notons $I \subseteq G$ un système de représentant des classes à gauche modulo H et $J \subseteq H$ un système de représentant des classes à gauche H/K modulo K. Montrer que

(i) $\Lambda = IJ$ est un système de représentant des classes G/K ;

(ii) Λ est en bijection avec $I \times J$.

(b) Montrer que $[G : K] = [G : H][H : K]$.

(c) En déduire que K est d'indice fini dans G si et seulement si il est d'indice fini dans H.

Exercice 2.15. Soit

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} ; a, b, c \in \mathbb{R} \text{ et } ac \neq 0 \right\}$$

(a) Vérifier que G est un sous-groupe de $GL_2(\mathbb{R})$ et que G agit sur $\mathbb{R}$ par l'opération

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot x = \frac{ax+b}{c}$$

(b) Déterminer l'orbite de 0 et le stabilisateur de 0 pour cette action.

Exercice 2.16. On dit d'une bijection $f : \mathbb{R}^3 \to \mathbb{R}^3$ que c'est une **isométrie** si elle conserve la distance entre les points, c'est-à-dire que pour tous points $P, Q \in \mathbb{R}^3$ on a

$$\mathbf{d}(f(P), f(Q)) = \mathbf{d}(P, Q).$$

Par exemple, une rotation est une isométrie, une symétrie par rapport à un plan fixé (*image miroir*) est aussi une isométrie (N.B. Il y en a d'autres).

(a) Montrer que les isométries forment un sous-groupe du groupe $S_{\mathbb{R}^3}$ de toutes les permutations de $\mathbb{R}^3$. Soit $\mathrm{ISO}_{\mathbb{R}^3}$ le groupe des isométries de $\mathbb{R}^3$, vérifier que $\mathrm{ISO}_{\mathbb{R}^3}$ agit sur $\mathbb{R}^3$ par l'action naturelle $\mathrm{ISO}_{\mathbb{R}^3} \times \mathbb{R}^3 \to \mathbb{R}^3$, définie par $f \cdot P = f(P)$.

(b) Montrer qu'on peut considérer une action de $\mathrm{ISO}_{\mathbb{R}^3}$ sur les ensembles de n points, en posant

$$f \cdot A := \{f(P) \mid P \in A\},$$

pour tout $A = \{P_1, P_2, \ldots, P_n\}$, avec les P_i des points distincts deux à deux.

Exercices exploratoires

Exercice 2.17 (Autre preuve du théorème de Wilson[25]). Cet exercice a pour but de proposer une preuve du théorème de Wilson qui exploite les notions de ce chapitre.

Théorème 2.17 (Wilson). *Soit $n \in \mathbb{N}$, $n \geqslant 2$, alors n est premier si et seulement si*

$$(n-1)! \equiv -1 \pmod{n}.$$

(a) Pour p premier, montrer dans $\mathbb{Z}_p$ que $x = (p-1)!$ est le produit de tous les éléments du groupe abélien $\mathbb{Z}_p^\times$.

(b) Soit G un groupe abélien fini et x le produit des éléments de G.

(i) Si $|G|$ est impair, montrer que $x = e$;

(ii) si $|G|$ est pair et G ne contient qu'une involution alors montrer que x est cette unique involution ;

25. John Wilson (1741-1793).

(iii) si $|G|$ est pair et G contient plus d'une involution, montrer que $x = e$ (difficile).

(c) En déduire la preuve du théorème de Wilson.

Exercice 2.18. Si X est un espace topologique (voir Exercice 1.49), et G est un groupe topologique, on dit qu'on a une **action continue de groupes**

$$X \times G \to X,$$

si les fonctions $x \mapsto g \cdot x$ et $g \mapsto g \cdot x$ sont continues quelques soient $x \in X$ et $g \in G$.

(a) Montrer que l'action usuelle de GL_n sur $\mathbb{R}_n$ est une action continue.

(b) Montrer que l'action par multiplication à gauche et l'action par conjugaison sont des actions continues d'un groupe topologique G sur lui-même.

(c) Décrire la notion d'isomorphisme pour les actions continues de groupes.

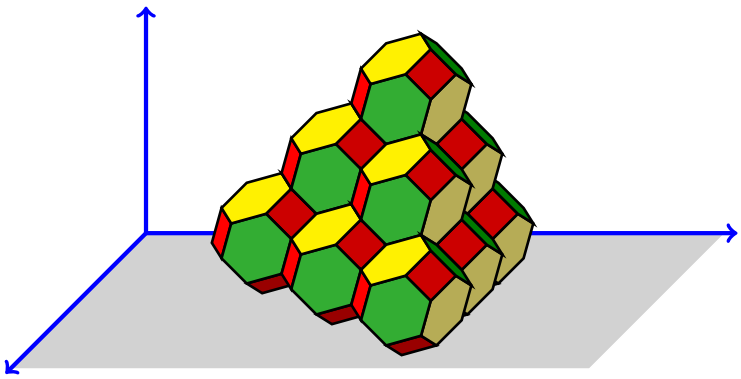


FIGURE 2.6 – Portion de pavage de $\mathbb{R}^3$ par le permutoèdre.

Exercice 2.19 (Construction du permutoèdre).

(a) Montrer qu'on peut réaliser géométriquement le permutoèdre dans $\mathbb{R}^3$, en considérant que ses sommets sont les permutations des 4 points $(0, \pm 1, \pm 2)$.

(b) En déduire qu'on peut paver l'espaces avec des copies du permutoèdre. Une partie de ce pavage est illustré à la figure 2.6.

(c) On peut obtenir tous les permutoèdre de ce pavage par des translations du permutoèdre « de base ». Identifier le group de ces translations.

Chapitre 3

Morphismes de groupes

Dans tout contexte mathématique, il importe de bien comprendre comment comparer les objets qui sont considérés, cela permet de mieux comprendre leur rôle. Lorsque ce contexte est algébrique, on parle de morphisme. Ce sont les fonctions entre structures algébriques de même nature qui « respectent » les opérations considérées. Dans notre cas, ce sont les fonctions qui respectent les lois de composition de groupes. Les morphismes de groupes sont de première importance pour la théorie des groupes.

3.1 Définition

Pour deux groupes $(G, \cdot)$ et $(G', *)$, un **morphisme** (ou **homomorphisme**, comme les anglophones) de groupes, de G vers G', est une fonction $\theta : G \to G'$ telle que

$$\theta(x \cdot y) = \theta(x) * \theta(y), \quad \text{pour tout} \quad x, y \in G. \tag{3.1}$$

De façon rigoureuse, il faudrait toujours distinguer les lois de décompositions de G et de G'. Cependant, le contexte permet généralement de bien faire la nuance, sans avoir à explicitement adopter des notations différentes. Ainsi, ci-dessus il n'y aurait pas eu d'ambiguïté à écrire $\theta(xy) = \theta(x)\theta(y)$. En effet, comme $\theta(x)$ et $\theta(y)$ sont dans G', l'opération à considérer dans le membre de droite est forcément celle de G'. Pour la même raison, on écrira souvent simplement e pour l'élément neutre de chacun des deux groupes.

On dit d'un morphisme de G vers lui-même que c'est un **endomorphisme** de G. On note $\mathrm{Hom}(G, G')$ l'ensemble des morphismes de G vers G', et $\mathrm{End}(G)$ l'ensemble des endomorphisme de G. Il est clair que ces deux ensembles sont non-vides, puisqu'on a toujours au moins le morphisme **trivial** $\theta : G \to G'$, qui envoie tous les éléments de G sur l'élément neutre de G'. Le signe $\varepsilon : S_n \to \{+1, -1\}$ est un

morphisme de groupes [1] surjectif, de même que le déterminant dét : $\mathrm{GL}_n \to \mathbb{R}^*$ (où $\mathbb{R}^*$ est muni de la multiplication). On dit d'un morphisme surjectif que c'est un **épimorphisme**, et on utilise la notation [2]

$$\theta : G \twoheadrightarrow G' .$$

Pour tout $n \in \mathbb{N}^*$, la fonction $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}_n$ définie par $\pi(k) = (k \bmod n)$ est un épimorphisme. Comme un le verra plus tard, c'est un cas spécial de « surjection canonique ». Si H est un sous-groupe de G, alors l'inclusion $\iota : H \to G$, telle que $\iota(g) = g$, est un morphisme de groupes injectif. On dit d'un morphisme injectif, que c'est un **monomorphisme**, et on écrit

$$\theta : G \hookrightarrow G' .$$

On dit d'un morphisme bijectif que c'est un **isomorphisme**. S'il existe un isomorphisme entre deux groupes, on dit qu'ils sont **isomorphes** [3], avec la notation

$$\theta : G \xrightarrow{\sim} G' .$$

Deux groupes isomorphes ont les propriétés algébriques. Par exemple, la fonction $\theta : \mathbb{Z}_2 \to \{+1, -1\}$ définie en posant $\theta(0) := 1$ et $\theta(1) := -1$ est un isomorphisme de groupes. En effet, on a

$$\begin{array}{rclcrcrcl} \theta(0+1) & = & \theta(1) & = & -1 & = & 1 \cdot (-1) & = & \theta(0)\theta(1), \\ \theta(0+0) & = & \theta(0) & = & 1 & = & 1 \cdot 1 & = & \theta(0)\theta(0), \\ \theta(1+1) & = & \theta(0) & = & 1 & = & (-1) \cdot (-1) & = & \theta(1)\theta(1). \end{array}$$

Autrement dit, « additionner » dans $\mathbb{Z}_2$ revient au même que de « multiplier » dans $\{+1, -1\}$. De manière plus imagée, la Figure 3.1 illustre comment le groupe des symétries du triangle est isomorphe au groupe S_3. Les premières propriétés générales des morphismes de groupes sont les suivantes.

Proposition 3.1. *Si $\theta : G \to G'$ et $\psi : G' \to G''$ sont des morphismes de groupes, alors*

(1) $\theta(e) = e$;
(2) $\theta(x^{-1}) = \theta(x)^{-1}$ *pour tout* $x \in G$;
(3) $H \leqslant G$ *entraîne* $\theta(H) \leqslant G'$;
(4) $H' \leqslant G'$ *entraîne* $\theta(H') \leqslant G$, *où* $\theta(H') := \{x \in G \mid \theta(x) \in H'\}$.
(5) $\psi \circ \theta : G \to G''$ *est un morphisme de groupes.*

Démonstration. Pour montrer (1), considérons $x \in G$. On a [4]

$$\theta(x)\, e = \theta(x) = \theta(xe) = \theta(x)\theta(e),$$

1. La structure de groupe sur $\{+1, -1\}$ correspond à l'opération de multiplication.
2. Avec une flèche spéciale qui indique la surjectivité
3. Du grec « ισος » (isos) pour « même », et « μορφη » (morphè) pour « forme ».
4. Ne pas oublier que le sens de e dépend du groupe sous-jacent au produit considéré.

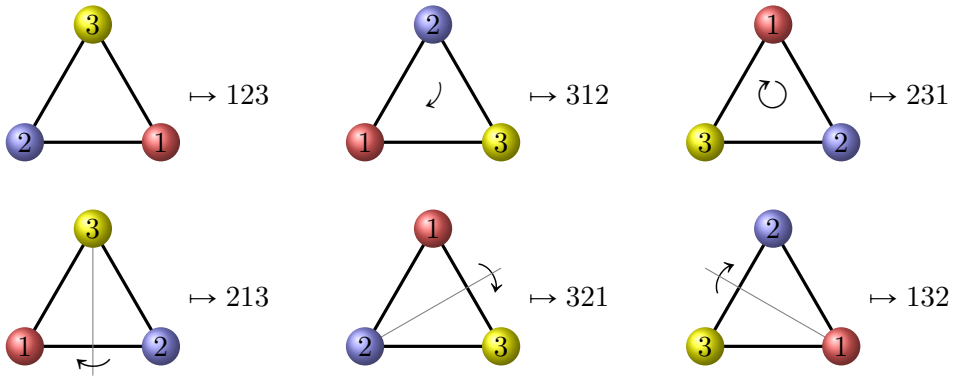


FIGURE 3.1 – Isomorphisme entre les symétries du triangle et S_3.

et donc $\theta(x)\theta(e) = \theta(x)\, e$. Multipliant à gauche par l'inverse de $\theta(x)$, on trouve $\theta(e) = e$. On établit ensuite (2) facilement. En effet, comme

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

on en déduit que $\theta(x^{-1}) = \theta(x)^{-1}$. Ensuite, pour prouver (3), soit H un sous-groupe de G, et soit $y_1, y_2 \in \theta(H)$. Alors il existe $x_1, x_2 \in H$ tel que $\theta(x_1) = y_1$ et $\theta(x_2) = y_2$. Comme $x_1 x_2^{-1} \in H$ on obtient, en vertu de (2), que

$$y_1 y_2^{-1} = \theta(x_1)\theta(x_2)^{-1} = \theta(x_1)\theta(x_2^{-1}) = \theta(x_1 x_2^{-1}) \in \theta(H).$$

Puisque $e = \theta(e) \in \theta(H)$, on conclut que $\theta(H) \leqslant G'$. La preuve de (4) est laissée en exercice. Pour (5), soit $x, y \in G$, posons $\eta := \psi \circ \theta$, et donc $\eta(x) = \psi(\theta(x))$. Montrons que $\eta(x \cdot y) = \eta(x) \cdot \eta(y)$. Puisque θ et ψ sont des morphismes de groupes on calcule que

$$\eta(x \cdot y) = \psi(\theta(x \cdot y)) = \psi(\theta(x) \cdot \theta(y)) = \psi(\theta(x)) \cdot \psi(\theta(y)) = \eta(x) \cdot \eta(y),$$

ce qui montre l'assertion. ■

On en déduit immédiatement le résultat suivant :

Corollaire 3.2. $(\mathrm{End}(G), \circ)$ *est un monoïde.*

3.2 Noyau d'un morphisme de groupes

Le **noyau** d'un morphisme $\theta : G \to G'$, noté $\ker(\theta)$, est le sous-groupe de G formé de l'image inverse de e par θ, c.-à-d.

$$\ker(\theta) := \{g \in G \mid \theta(g) = e\}.$$

La terminologie viens du terme allemand « kern », qui signifie noyau. C'est une notion naturelle qui apparaît dans de nombreux contextes algébriques (voir Exercice 3.14).

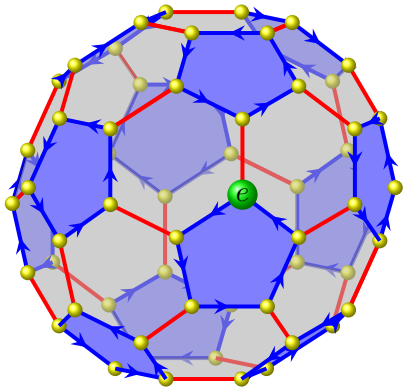


FIGURE 3.2 – Graphe de Cayley de A_5, pour les générateurs (12345) et (12)(34).

Ainsi, on obtient le **groupe alterné**, noté A_n, comme sous-groupe de S_n, en considérant le morphisme de groupes qui associe à une permutation son signe, $\varepsilon : S_n \to \{+1, -1\}$. On a donc

$$A_n := \ker(\varepsilon) = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\},$$

On dit aussi des éléments de A_n que ce sont des permutations **paires**. Par exemple, A_5 admet comme générateurs les permutations paires (12345) et (12)(34) ; et le graphe de Cayley correspondant est celui de la Figure ci-contre. Les flèches bleues correspondent à la composition avec le cycle (12345), et les arêtes rouges correspondent à la composition avec la permutation (12)(34), qui est d'ordre 2. Ces dernières arêtes ne sont pas orientées ; elles vont dans les deux sens. Le composé des deux générateurs donne une permutation d'ordre 3, qui correspond à suivre en alternance les arêtes rouges et les arêtes bleues autour des faces hexagonales de la figure. Les pentagones sont les classes à gauche du sous-groupe engendré par (12345). Ignorant l'orientation des arêtes, on constate que le graphe est celui qui décrit la molécule de C_{60} du chapitre 1. On montre, voir l'exercice 3.2, que les éléments de A_5 sont d'ordre 1, 2, 3, ou 5.

D'autre part, on considère aussi **l'image** d'un morphisme θ

$$\mathrm{Im}(\theta) := \theta(G) = \{\theta(x) \mid x \in G\}.$$

Il découle de la Proposition 3.1, que $\mathrm{Im}(\theta)$ est aussi un sous-groupe de G'. Comme l'indique la proposition suivante, la nature du noyau et de l'image d'un morphisme détermine certaines propriétés fondamentales du morphisme.

Proposition 3.3. *Si $\theta : G \to G'$ est un morphisme de groupes, alors*

(1) *le noyau $\ker(\theta)$ est un sous-groupe normal de G ;*

(2) *θ est injectif si et seulement si $\ker(\theta) = \{e\}$; et*

(3) *θ est surjectif si et seulement si $\mathrm{Im}(\theta) = G'$.*

Démonstration. Si g est dans $\ker(\theta)$, alors

$$\theta(x^{-1}gx) = \theta(x)^{-1}\, e\, \theta(x) = e,$$

et donc $x^{-1}gx$ est dans le noyau, pour tout x dans G. Ceci montre que $\ker(\theta)$ est normal. Supposons maintenant que θ injectif. Soit $x \in \ker(\theta)$, alors $\theta(x) = e = \theta(e)$. Comme θ est injectif, $x = e$. Supposons maintenant que $\ker(\theta) = \{e\}$. Soit $x_1, x_2 \in G$ tel que $\theta(x_1) = \theta(x_2)$, alors $e_{G'} = \theta(x_1) \cdot \theta(x_2)^{-1} = \theta(x_1 \cdot x_2^{-1})$. Donc $x_1 \cdot x_2^{-1} \in \ker(\theta) = \{e\}$, d'où $x_1 = x_2$. ■

3.3 Isomorphismes de groupes

Comme on l'a déjà mentionné, un morphisme de groupes $\theta \in \mathrm{Hom}(G, G')$ est un isomorphisme de groupes si la fonction θ est inversible. On dit d'un isomorphisme de G dans G que c'est un **automorphisme** de G. L'ensemble des automorphismes est noté $\mathrm{Aut}(G)$. Par exemple, si $\theta : G \to G'$ un monorphisme alors les groupes G et $\mathrm{Im}(\theta)$ sont isomorphes.

Proposition 3.4. *Pour tous groupes G et G'.*

1. *Si $\theta : G \to G'$ est un isomorphisme, alors $\theta^{-1} : G' \to G$ est aussi un isomorphisme.*
2. *$\mathrm{Aut}(G)$ est un groupe pour la composition.*
3. *$\mathrm{Aut}(G)$ est un sous-groupe de S_G.*

Démonstration. Il faut seulement montrer que θ^{-1} est un morphisme de groupes. À cette fin, soit $x, y \in G'$. Comme θ est un morphisme de groupes, et $\theta \circ \theta^{-1} = \mathrm{Id} = \mathrm{Id}_{G'}$, on a

$$x \cdot y = \mathrm{Id}(x) \cdot \mathrm{Id}(y) = \theta(\theta^{-1}(x)) \cdot \theta(\theta^{-1}(y)) = \theta(\theta^{-1}(x) \cdot \theta^{-1}(y)).$$

Appliquant θ^{-1} à chaque membre de cette égalité, on trouve

$$\theta^{-1}(x \cdot y) = \theta^{-1}(x) \cdot \theta^{-1}(y).$$

Les énoncés (2) et (3) sont des conséquences immédiates de ce qui précède. ■

En associant ceci aux résultats précédents, on conclut qu'un morphisme de groupes θ est un isomorphisme, si et seulement si $\mathrm{Im}(\theta) = G$ et $\ker(\theta) = \{e\}$. On dit que deux groupes G et G' sont **isomorphes** s'il existe au moins un isomorphisme de groupes $\theta : G \to G'$. On dit alors aussi que G et G' sont dans la même **classe d'isomorphisme** et on note ce fait $G \simeq G'$. La relation $\simeq$ est une relation d'équivalence (sur l'ensemble des groupes contenus dans un « univers » donné). Deux groupes isomorphes ont exactement les mêmes propriétés algébriques. Ainsi, G est abélien si et seulement si G' est abélien (à vérifier en exercice). Pour tout $x \in G$, et tout isomorphisme θ, on a que $\mathrm{ord}(\theta(x)) = \mathrm{ord}(x)$. Si $G \simeq G'$, alors pour tout $n \in \mathbb{N}$, le nombre d'éléments de G d'ordre n est égal au nombre d'éléments de G' d'ordre n. De plus, deux groupes isomorphes ont forcément le même ordre.

Remarque. La réciproque n'est pas vraie, car S_3 et $\mathbb{Z}_6$ ont le même ordre, mais ne sont pas isomorphes. En effet, $\mathbb{Z}_6$ possède 2 éléments d'ordre 6, tandis que S_3 n'en possède pas. Une autre différence significative est que $\mathbb{Z}_6$ est abélien, tandis que S_3 ne l'est pas.

3.4 Automorphismes intérieurs

Pour tout groupe G, et $g \in G$, la fonction

$$\varphi_g : G \longrightarrow G \qquad \text{définie par} \qquad \varphi_g(x) := gxg^{-1},$$

est un automorphisme de G qu'on dit être **intérieur**. On note $\mathrm{Int}(G)$ le groupe des automorphismes intérieurs de G. Pour voir que φ_g est un automorphisme on calcule d'abord, pour $x, y \in G$ que

$$\begin{aligned} \varphi_g(x)\varphi_g(y) &= (gxg^{-1})\,(gyg^{-1}) \\ &= gx\,(g^{-1}g)\,yg^{-1} \\ &= gx\,e\,yg^{-1} \\ &= g\,xy\,g^{-1} \\ &= \varphi_g(xy). \end{aligned}$$

De plus, φ_g inverse admet comme inverse $\varphi_{g^{-1}}$. En effet,

$$\begin{aligned} \varphi_{g^{-1}} \circ \varphi_g(x) &= \varphi_{g^{-1}}(gxg^{-1}) \\ &= g^{-1}(gxg^{-1})(g^{-1})^{-1} \\ &= g^{-1}(gxg^{-1})g \\ &= x. \end{aligned}$$

Donc $\varphi_{g^{-1}} \circ \varphi_g = \mathrm{Id}_G$. De même, on vérifie que $\varphi_{g^{-1}}$ est inverse à droite de φ_g. On observe que $\mathrm{Int}(G)$ peut être bien plus petit que G. Par exemple, si G est abélien, alors $\mathrm{Int}(G) = \{e\}$.

Proposition 3.5. *Soit G un groupe. Alors* $\mathrm{Int}(G) \leqslant \mathrm{Aut}(G)$.

Démonstration. Exercice. ■

3.5 Théorème de Cayley

Nous allons voir dans cette section que le groupe symétrique joue un rôle central en théorie des groupes. Dans le cas fini, la proposition suivante montre qu'on peut toujours se ramener aux groupes S_n. Une façon d'interpréter le théorème principal de la section est alors de dire que tous les groupes finis se retrouvent (à isomorphisme près) à l'intérieur d'un des groupes S_n, pour un certain n. Autrement dit, bien connaître S_n permet de connaître tous les groupes finis.

Proposition 3.6. *Soit E un ensemble non vide.*

(1) *Si E et F ont même cardinal, alors $S_E \simeq S_F$;*
(2) *Si $|E| = n$, alors $S_E \simeq S_n$.*

Démonstration. Si E et F ont même cardinal, alors il existe une bijection $f : E \to F$. Il suffit de montrer que la fonction

$$\alpha : S_E \to S_F, \qquad \text{avec} \qquad \alpha(g) := f \circ g \circ f^{-1},$$

est un isomorphisme de groupes. Procédant presque exactement comme à la section précédente, on vérifie facilement que l'inverse de α est $\alpha^{-1} := S_F \to S_E$, avec $\alpha^{-1}(h) := f^{-1} \circ h \circ f$. Ne reste plus qu'à montrer que α est un morphisme de groupe. À cette fin, soit $g, g' \in S_E$, alors

$$\begin{aligned} \alpha(g \circ g') &= f \circ g \circ g' \circ f^{-1} \\ &= f \circ g \circ \mathrm{Id}_E \circ g' \circ f^{-1} \\ &= f \circ g \circ \mathrm{Id}_E \circ g' \circ f^{-1} \\ &= (f \circ g \circ f^{-1}) \circ (f \circ g' \circ f^{-1}) \\ &= \alpha(g) \circ \alpha(g'). \end{aligned}$$

La proposition est donc démontrée. ∎

Le théorème qui suit est conceptuellement d'une grande importance. Il est dû au mathématicien anglais Arthur Cayley (1821-1895), un des pionniers de la théorie des groupes.

Théorème 3.7 (Théorème de Cayley)**.** *Tout groupe G est isomorphe à un sous-groupe de S_G, le groupe de ses permutations.*

Démonstration. Il suffit de construire un morphisme de groupes injectif $\Phi : G \to S_G$. Pour chaque $g \in G$, on considère la fonction $\Phi_g : G \to G$, définie en posant $\Phi_g(x) := g \cdot x$. C'est une bijection, appelée **translation à gauche** par g (exercice). En outre, $\Phi_g \in S_G$ et son inverse est $(\Phi_g)^{-1} = \Phi_{g^{-1}}$. Donc la fonction $\Phi : G \to S_G$, avec $\Phi(g) := \Phi_g$, est bien définie. En calculant comme suit, on vérifie que Φ est un morphisme de groupes. En effet, pour $g, h \in G$, on a (exercice)

$$\begin{aligned} \Phi(g) \circ \Phi(h) &= \Phi_g \circ \Phi_h \\ &= \Phi_{gh} \\ &= \Phi(gh). \end{aligned}$$

D'autres parts, Φ est injectif. En effet, si $g \in \ker(\Phi)$ alors $\Phi_g = \mathrm{Id}$. Donc $\Phi_g(x) = gx = x$ pour tout $x \in G$, et donc $g = e$. On conclut donc que Φ est un monomorphisme de groupe, de G vers S_G. ∎

Par exemple, comme $|\mathbb{Z}_3| = 3$, la conjonction de la Proposition 3.6 et du Théorème de Cayley permet de conclure que $\mathbb{Z}_3$ est isomorphe à un sous-groupe de S_3. Il suffit de prendre celui engendré par $\sigma_1 = 231 = (123)$. C'est en fait le seul sous-groupe d'ordre 3 dans S_3.

3.6 Actions et morphismes de groupes

On reformule souvent les actions de groupes en terme de morphismes de groupes. Ainsi, à une action $\alpha : G \times E \to E$ on fait correspondre le morphisme de G dans le groupe S_E des permutations de E, en considèrant la fonction $\widetilde{\alpha} : G \to S_E$, défini par

$$\widetilde{\alpha}(g) = \alpha_g,$$

avec $\alpha_g : E \to E$ la fonction définie en posant $\alpha_g(x) := g \cdot x$. La vérification que cette fonction est bien défini, et qu'elle constitue bien un morphisme de groupes est laissée en exercice (voir 3.3). Inversement, à un morphisme $\varphi : G \to S_E$ on fait correspondre l'action $\overline{\varphi} : G \times E \to E$, définie par $\overline{\varphi}(g, x) = \varphi(g)(x)$. Ceci établie une bijection entre actions de G sur E, et morphismes de G vers S_E.

Dans le cas où l'action est linéaire, on considère plutôt un morphisme de G vers le groupe $\mathrm{GL}(V)$. Si $\dim(V) = d$, on dit que la représentation est de **dimension** d. De manière très explicite, si $V = \mathbb{C}^n$, une représentation linéaire de G est donc une fonction $\rho := G \to \mathrm{GL}_n$ qui associe à chaque élément g de G une matrice $n \times n$ à coefficients complexes $\rho(g)$, avec les conditions

(1) $\rho(e) = \mathrm{Id}$, et

(2) $\rho(gh) = \rho(g)\rho(h)$, avec à droite le produit matriciel.

Ainsi, on a la représentation linéaire de S_3 définie en posant

$$\rho(e) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho(213) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho(132) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$
$$\rho(321) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \rho(231) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \rho(312) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Plus généralement, on a une représentation de S_n obtenue en posant que $\rho(\sigma)$ est la matrice $(a_{ij})_{1 \leqslant i,j \leqslant n}$, avec

$$a_{ij} := \begin{cases} 1 & \text{si } \sigma(j) = i, \\ 0 & \text{sinon.} \end{cases}$$

Le signe d'une permutation est égal au déterminant de la matrice ainsi obtenue, c.-à-d. $\det(\rho(\sigma)) = \varepsilon(\sigma)$. Un autre exemple est la représentation de GL_2, telle que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^2 & ab & ab & b^2 \\ ac & ad & bc & bd \\ ac & bc & ad & bd \\ c^2 & cd & cd & d^2 \end{pmatrix}.$$

Bien entendu, les représentations de dimension 1 (sur le corps des complexes) sont des morphismes de groupes $\rho : G \to \mathbb{C}^*$, le groupe des nombres complexes non nuls avec la multiplication. Si $g \in G$ est d'ordre n, alors on doit avoir

$$\rho(g)^n = \rho(g^n) = \rho(e) = 1.$$

La valeur de $\rho(g)$ est donc

$$\rho(g) = e^{2ki\pi/n} = \cos(2k\pi/n) + i\,\sin(2k\pi/n),$$

pour un certain k. C'est une des racines n^{e} de l'unité. Plus généralement, on a la proposition suivante.

Proposition 3.8. *Si G est un groupe d'ordre n, et si $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ est un morphisme de groupes (une représentation linéaire), alors les valeurs propres de $\rho(g)$ sont des racines n^{e} de l'unité, pour tout g dans G.*

Démonstration. Comme $g^n = e$, il s'ensuit que $\rho(g)^n = 1$. On a donc que la matrice[5] $\rho(g)$ est annulée par le polynôme $x^n - 1$. Ses valeurs propres sont donc des racines de ce polynôme, et on a prouvé l'assertion. ∎

3.7 Tous les groupes finis

La classification des groupes finis peut maintenant prendre un sens précis. En effet, on peut chercher à donner la liste de tous les groupes d'un ordre donné, à isomorphisme près. Pour $n \leqslant 16$, on en trouve une liste complète sur le site suivant : Liste des petits groupes. La suite donnant le nombre de groupes d'ordre n se trouve dans « On-line Encyclobedia of Integer Sequences ». Les premiers termes sont :

$$0, 1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, 5, 1, 2, 1, 14, 1, 5, 1, 5, 2, 2, 1, 15, 2, 2, 5, 4, 1, 4, 1, 51, 1, \ldots$$

Les valeurs qui « ressortent » dans cette suite correspondent aux nombres de groupes d'ordre 2^n. La suite des nombres de groupes en question (voir https ://oeis.org/A000679) est

$$1, 1, 2, 5, 14, 51, 267, 2328, 56092, 10494213, 49487365422, \ldots$$

Nous verrons au Chapitre 6 comment on peut construire tous les groupes abéliens fins, et donc (en principe) les compter.

On a maintenant une classification complète des groupes simples finis, qu'on trouve ici : Liste des groupe finis simples. En principe, cela permet de construire tous les groupes finis. Parmi ceux-ci, on a des familles infinies :

5. C'est plutôt une transformation linéaire, mais on peut reformuler en terme de matrice.

- La famille les groupes $\mathbb{Z}_p$ pour p premier, qui n'ont aucun sous-groupe non trivial.
- La famille des groupes alternés A_n, avec $n \geqslant 5$. Le fait que ces groupes soit simples entre dans l'explication de Galois du fait qu'il n'y a pas de formule par radicaux pour les racines de polynômes de degré supérieur ou égal à 5.
- Avec 16 familles de groupes de Lie.

Puis on a 26 groupes dits « exceptionnels », qui ne font pas partie de ces familles infinies. Le plus petit est le groupe de Mathieu M_{11}, d'ordre 7920, et le plus grand est le Monstre (voir Section 1.7). Bien entendu, du fait cette classification, il y a un groupe simple d'ordre p pour tout nombre premier p ; et il y a un groupe d'ordre $n!/2$ pour tout entier $n \geqslant 5$. Pour les autres entiers k, il plus rare d'avoir un groupe simple d'ordre k. Excluant les nombres premiers et les nombres de la forme $n!/2$, la liste des entiers k pour lesquels il existe un groupe simple d'ordre k débute comme suit :

$$168, 504, 660, 1092, 2448, 3420, 4080, 5616, 6048, 6072, 7800, \mathbf{7920}, 9828, 12180, 14880, 25308, \ldots$$

3.8 Exercices

Exercice 3.1. On utilise ici la notation $[k]_6$ pour désigner la classe de l'entier k modulo 6, et la notation $[k]_3$ pour désigner la classe de l'entier k modulo 3. On considère les groupes $(\mathbb{Z}_6, +)$ et $(\mathbb{Z}_3, +)$ et la fonction

$$\theta : (\mathbb{Z}_6, +) \longrightarrow (\mathbb{Z}_3, +) \ , \qquad \text{définie en posant} \qquad \theta([k]_6) := [k]_3.$$

(a) Montrer que θ est bien définie, à savoir qu'on a toujours que si $[k]_6 = [m]_6$ alors $[k]_3 = [m]_3$.

(b) Montrer que θ est un morphisme surjectif.

(c) Déterminer le noyau de θ.

(d) Généraliser ces énoncés à $(\mathbb{Z}_n, +)$ et $(\mathbb{Z}_d, +)$, pour d divisant n ; et les démontrer.

Exercice 3.2. Montrer que la décomposition en cycles disjoints des éléments de A_5 est : soit de type 11111, soit de type 221, soit de type 311, ou de type 5. Donner un règle calculatoire simple pour déterminer quels sont les types des permutations dans A_n, pour n quelconque.

Exercice 3.3 (Voir solution 10). Soit G un groupe et E un ensemble. Vérifier qu'une action de G sur E correspond à un morphisme de G dans le groupe S_E des permutations de E, de la manière suivante.

(a) Soit $\alpha : G \times E \to E$ une action de G sur E. Vérifier que l'application $\tilde{\alpha} : G \to S_E$, définie par $\tilde{\alpha}(g) = \alpha_g$, est un morphisme, où $\alpha_g(x) = g \cdot x$.

(b) Soit $\varphi : G \to S_E$ un morphisme. Vérifier que l'application $\overline{\varphi} : G \times E \to E$, définie par $\overline{\varphi}(g, x) = (\varphi(g))(x)$ donne une action de G sur E.

(c) Vérifier que les correspondances $\alpha \mapsto \tilde{\alpha}$ et $\varphi \mapsto \overline{\varphi}$ établies en (a) et (b) sont inverses l'une de l'autre.

Exercice 3.4. Soit $\theta \in \mathrm{Hom}(G, G')$ et $H' \leqslant G'$. Montrer que $\theta(H') \leqslant G'$.

Exercice 3.5. Soit G, G' et G'' trois groupes, montrer que

(a) $G \simeq G$;

(b) $G \simeq G' \iff G' \simeq G$;

(c) si $G \simeq G'$ et $G' \simeq G''$ alors $G \simeq G''$.

Exercice 3.6. Soit $\theta : G \to G'$ un morphisme de groupes injectif.

(a) Montrer que $G \simeq \theta(G) = \mathrm{Im}(\theta)$.

(b) Montrer que $\mathrm{ord}(\theta(x)) = \mathrm{ord}(x)$, pour tout $x \in G$.

(c) Si $G \simeq G'$ et $n \in \mathbb{N}$. Montrer que le nombre d'éléments de G d'ordre n est égal au nombre d'éléments de G' d'ordre n, et définissant une bijection entre les deux ensembles correspondants.

Exercice 3.7. Soit $G = \langle x \rangle$ un groupe monogène. On considère la fonction $\theta : \mathbb{Z} \to G$, telle que $\theta(k) := x^k$.

(a) Montrer que θ est un morphisme de groupes surjectif.

(b) Montrer qu'il existe $n \in \mathbb{N}$ tel que $\ker(\theta) = n\mathbb{Z}$.

(c) Si G est infini, montrer que $G \simeq \mathbb{Z}$.

(d) Si G est fini d'ordre n, montrer que $G \simeq \mathbb{Z}_n$.

Exercice 3.8. (Translation à gauche) Soit G un groupe. Pour chaque $g \in G$, on considère la fonction $\Phi_g : G \to G$, définie en posant $\Phi_g(x) := g \cdot x$.

(a) Montrer que $\Phi_g \in S_G$ et que $(\Phi_g)^{-1} = \Phi_{g^{-1}}$.

(b) Est-ce que Φ_g est un morphisme de groupes ?

(c) Montrer que $\Phi_g \circ \Phi_h = \Phi_{gh}$ pour tout $g, h \in G$.

Exercice 3.9. Soit G un groupe. On utilise ici les notations de la section 3.4.

(a) Montrer que l'ensemble $\mathrm{Int}(G)$ des morphismes intérieurs du groupe G est un sous-groupe de $\mathrm{Aut}(G)$.

(b) Soit $g, h \in G$, montrer que $\varphi_g = \varphi_h$ si et seulement si $g^{-1}h$ appartient à $Z(G)$, le centre du groupe G.

(c) Montrer que si G est fini, alors $|\mathrm{Int}(G)| \leqslant |G|$.

(d) Calculer $\mathrm{Int}(S_3)$ et $\mathrm{Int}(\mathbb{Z}_n)$.

Exercice 3.10. Montrer que

(a) le groupe diédral D_m est isomorphe à un sous-groupe de S_m.

(b) $\mathbb{Z}_n$ est isomorphe à un sous-groupe de S_n.

Exercices exploratoires

Exercice 3.11. Définir la notion de morphisme, de monomorphisme, d'épimorphisme, et d'isomorphisme de monoïdes. Pour toute bijection $f : E \to F$, on considère la fonction

$$\Phi_f : \mathrm{Fonct}(E, E) \to \mathrm{Fonct}(F, F),$$

qui envoie $g \in \mathrm{Fonct}(E, E)$ sur $f \circ g \circ f^{-1}$. Montrer que Φ_f est un isomorphisme de monoïde. Comme pour les groupes, on désigne respectivement par $\ker(\theta)$ et $\mathrm{Im}(\theta)$, le noyau et l'image d'un morphisme de monoïde $\theta : M \to M'$, avec les définitions évidentes. Montrer qu'on a

(a) Le noyau $\ker(\theta)$ est un sous-monoïde de M.

(a) L'image $\mathrm{Im}(\theta)$ est un sous-monoïde de M'.

(b) θ est injectif si et seulement si $\ker(\theta) = \{e\}$;

(c) θ est surjectif si et seulement si $\mathrm{Im}(\theta) = M'$.

Exercice 3.12. Rappelons (voir Exercice 1.41) que le monoïde libre $\mathcal{A}^*$ est constitué de l'ensemble des mots $a_1 a_2 \cdots a_n$, et que sa loi de composition est la concatenation. On considère ici le cas où A est un ensemble fini.

(a) Soit $f : \mathcal{A}^* \to M$ un morphisme de monoïde (et donc M est un monoïde). Montrer que f est entièrement caractérisée par sa valeur sur chaque lettre. Autrement dit, si f et g sont deux tels morphismes, alors on a $f = g$ si et seulement si $f(a) = g(a)$ pour tout $a \in \mathcal{A}$.

(b) Soit M un monoïde fini. En imitant la preuve du théorème de Cayley, montrer qu'il existe un monomorphisme de monoïdes $\varphi : M \to \mathrm{Fonct}(M, M)$, où l'opération pour ce dernier monoïde est la composition de fonctions. Est-ce que la démonstration demeure valable si M est infini ?

(c) Définir la notion d'action d'un monoïde M sur un ensemble E. Montrer que la donnée d'une action $M \times E \to E$ est équivalente à la donnée d'un morphisme de monoïde $M \to \mathrm{Fonct}(E, E)$.

(d) Pour une action d'un monoïde M sur E, et tout élément x de E, montrer que l'ensemble des éléments de M qui fixent x est un sous-monoïde (définition ?) de M.

(e) Montrer que la donnée d'une action du monoïde libre $\mathcal{A}^*$ sur un ensemble E est équivalente à la donnée d'une fonction (quelconque) $A \times E \to E$. Voir la notion de monoïde syntaxique en théorie des automates.

Exercice 3.13. On rappelle que le groupe $\mathrm{SL}_2(\mathbb{Z})$ est un groupe infini engendré par les matrices

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \text{et} \qquad R := \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

et qu'on a les relations $S^4 = \mathrm{Id}$ et $R^3 = S^2$. Pour toute représentation linéaire $\rho : \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}^*$,

(a) Montrer que

$$\rho\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{12} = 1, \qquad \text{pour tout} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

En conclure que $\rho(A) = \exp(2ki\,\pi/12)$ pour un certain $0 \leqslant k < 12$, pour tout A dans $\mathrm{SL}_2(\mathbb{Z})$.

(b) Montrer qu'il y a un nombre fini de représentations linéaires de $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathbb{C}^*$. Les trouver toutes.

Exercice 3.14. Définir les notions de noyau et d'image pour les morphismes d'anneaux commutatifs et les morphismes d'espaces vectoriels (alias transformations linéaires). Puis montrer que

(a) Le noyau d'un morphisme d'anneaux commutatifs est un **idéal**. Rappelons qu'un ideal J d'un anneau commutatif A, est un sous-groupe additif de A, tel que $a \cdot x$ est dans J, pour tout $x \in J$ et tout $a \in A$.

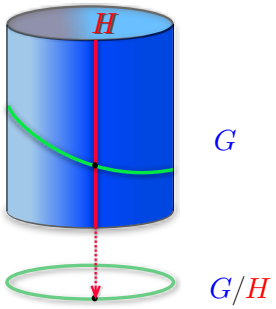
(b) Le noyau d'un morphisme d'espace vectoriel est un sous-espace vectoriel.

(c) Dans les deux cas, montrer qu'un morphisme θ est injectif, si et seulement si $\ker(\theta) = \{0\}$.

En théorie des catégories, on donne des définitions qui unifient tout ces concepts.

Chapitre 4

Goupes quotients, et théorème d'isomorphie



Dans ce chapitre, nous allons développer d'autres outils importants pour la construction et l'étude de groupes, la notion de groupes quotients ; et le premier théorème d'isomorphisme. Nous généraliserons ainsi la construction de la structure de groupe sur le quotient $(\mathbb{Z}, +)$ par son sous-groupe $(n\mathbb{Z}, +)$. Nous montrerons alors que l'étude des groupes cycliques et monogènes se réduit à celle des groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}_n, +)$.

4.1 Groupes quotients

Pour que l'ensemble quotient G/H admette une structure de groupe héritée de celle G, comme c'est le cas pour $\mathbb{Z}_n$ qui hérite sa de celle de $\mathbb{Z}$, il faut imposer à H certaines conditions. C'est la notion de « normalité ». Rappelons qu'un sous-groupe H d'un groupe G est dit normal si $xH = Hx$ pour tout $x \in G$. On écrit alors $H \lhd G$. Par exemple, le centre du groupe $Z(G)$ est normal dans G. En effet, si $x \in G$, alors $xg = gx$ pour tout $g \in Z(G)$. Donc $xZ(G) = Z(G)x$. Le groupe $\mathrm{Int}(G)$, des automorphismes internes de G, est un sous-groupe normal de son groupe d'automorphisme $\mathrm{Aut}(G)$. Tout sous-groupe d'un groupe abélien G est normal. Enfin, l'intersection de sous-groupes normaux est un sous-groupe.

Attention, la relation « $\lhd$ » n'est pas transitive. Autrement dit, on peut avoir $K \lhd H$ et $H \lhd G$, sans que $H \lhd G$. On trouve un exemple de cette non-transitivité dans S_4 (exercice). Par contre, si K

est sous-groupe de H, lui-même sous-groupe de G, alors

$$K \lhd G \quad \Longrightarrow \quad K \lhd H.$$

En effet, on a $xK = Kx$ pour tout $x \in G$ donc aussi pour tout $x \in H$. En un certain sens, l'intérêt principal des sous-groupes normaux est leur rôle dans la proposition suivante, qui décrit la construction de « groupe quotient ».

Proposition 4.1. *Soit G un groupe, et N un sous-groupe normal de G, alors l'opération*

$$G/N \times G/N \longrightarrow G/N \qquad \text{telle que} \qquad (xN)\cdot(yN) := xyN \tag{4.1}$$

muni G/N d'une structure de groupe. On l'appelle le groupe **quotient** *de G par N. L'élément neutre est la classe à gauche N, et l'inverse de $x\,N$ est $(xN)^{-1} = x^{-1}N$. La fonction $\pi : G \to G/N$ définie en posant $\pi(x) = xN$ est un épimorphisme de groupes dit* **canonique**, *et son noyau est* $\ker(\pi) = N$.

Démonstration. En fait, le seul élément un peu moins évident dans la preuve de ce théorème est de montrer que le produit est **bien défini**, c.-à-d. que pour $xN, x'N, x'N, y'N$ tel que $xN = x'N$ et $yN = y'N$, il faut montrer que $xyN = x'y'N$. Puisque $N \lhd G$, on calcule que

$$x'y'N = x'Ny' = (x'N)y' = (xN)y' = xy'N = x(y'N) = xyN.$$

Le reste est ensuite direct. On a l'associativité, parce que

$$(xN \cdot yN)\cdot zN = (xyN)\cdot zN = (xy)zN = x(yz)N = xN \cdot (yN \cdot zN);$$

l'élément neutre est bien N, puisque

$$xN \cdot N = xN = N \cdot xN;$$

et l'inverse est bien celui qui été annoncé, puisque

$$xN \cdot x^{-1}N = xx^{-1}N = N = x^{-1}N \cdot xN.$$

Calculant que $\pi(xy) = xyN = xN \cdot yN = \pi(x)\cdot\pi(y)$, on constate que π est un morphisme de groupes clairement surjectf. De plus, on a déjà vérifié l'égalité suivante

$$\ker(\pi) := \{x \in G \,|\, xN = N\} = N.$$

Ce qui achève la preuve. ∎

La proposition suivante souligne que les sous-groupes normaux coïncident avec les noyaux de morphismes de groupes.

Proposition 4.2. *Soit G un groupe et $H \leqslant G$, alors $H \lhd G$ si et seulement si il existe un morphisme de groupes $\theta : G \to G'$ tel que $H = \ker(\theta)$. En particulier, $\ker(\theta) \lhd G$, pour tout morphisme de groupes $\theta : G \to G'$.*

Démonstration. Si $H \lhd G$, il suffit de prendre $\theta = \pi : G \to G/H$. Réciproquement, il suffit de montrer que $\ker(\theta) \lhd G$: soit $x \in G$ et $g \in \ker(\theta)$, alors $\theta(xgx^{-1}) = \theta(x)\theta(g)\theta(x)^{-1}\theta(x)e\theta(x)^{-1} = e$ car $g \in \ker(\theta)$ et θ est un morphisme de groupes. Ainsi $xgx^{-1} \in \ker(\theta)$, le noyau est donc normal dans G. ■

Les groupes quotients permettent, entre autres, de faire des arguments par récurrence dans les groupes finis. Pour en donner un exemple, rappelons que l'ordre d'un élément x est le plus entier naturel n (s'il existe) tel que $x^n = e$, où e désigne l'élément neutre de G.

Lemme 4.3. *Si G est un groupe abélien fini dont tous les éléments ont une puissance de 3 comme ordre. Alors le cardinal de G est aussi une puissance de 3.*

Démonstration. On procède par récurrence $|G|$ sur le cardinal de G. Soit G tel que $\mathrm{ord}(g)$ est une puissance de 3, pour tout $g \in G$. Choisissons un élément $h \in G$, autre que e, ayant l'ordre $\mathrm{ord}(h) = 3^k$. Puisque $g \neq 0$, on a $k \neq 0$. Posons $H = \{e, h, \ldots, h^{3^k-1}\}$. Si $G = H$ alors on a fini, puisque $|G| = |H| = 3^k$. Autrement, on a $H \subset G$, avec $2 \leqslant |H| < |G|$. L'hypothèse de récurrence est que le résultat est vrai pour tous les groupes abéliens finis dont le cardinal est plus petit que $|G|$. Or, $|G/H| = |G|/|H|$ ce qui est plus petit que $|G|$, puisque $|H| \geqslant 2$. De plus, comme G est abélien, et donc H est normal, on a bien que G/H est un groupe abélien. Pour pouvoir utiliser l'hypothèse de récurrence, il faut vérifier que l'ordre de tout élément de G/H est une puissance de 3. À cette fin, considérons l'épimorphisme naturel $G \to G/H$, pour lequel $g \mapsto gH$. Par hypothèse, $g^{3^n} = e$ pour un certain n. On a alors $(gH)^{3^n} = g^{3^n}H = eH = H$, le neutre de G/H. En conséquence, 3^n est un multiple de $\mathrm{ord}(gH)$, et donc $\mathrm{ord}(gH)$ est une puissance de 3. L'hypothèse de récurrence s'applique donc àG/H, et $|G/H|$ est une puissance de 3. Disons $|G/H| = 3^\ell$. On calcule alors que

$$|G/H| = |G|/|H| = |G|/3^k = 3^\ell$$

ce qui entraîne $|G| = 3^{k+\ell}$, et donc que $|G|$ est une puissance de 3. Cela complète la récurrence. ■

4.2 Théorème d'isomorphisme

Les « théorèmes d'isomorphie » ont pour but de décrire la structure et les propriétés générales des morphismes de groupes. Ils en donnent des décompositions canoniques. Dans une autre terminologie plus moderne, on dit l'énoncé suivant correspond à décrire la **propriété universelle** du quotient de groupes.

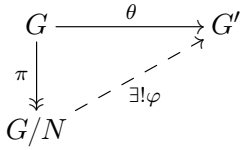
Théorème 4.4 (d'isomorphisme). *Soit G un groupe, $N \lhd G$ et $\pi : G \to G/N$ la surjection canonique. Si $\theta : G \to G'$ est un morphisme de groupes tel que $N \subseteq \ker(\theta)$, alors il existe un unique morphisme $\varphi : G/N \to G'$ tel que $\theta = \varphi \circ \pi$. De plus*

(1) *si $N = \ker(\theta)$ alors φ est un monomorphisme ;*

(2) *si θ est un épimorphisme, alors φ l'est aussi.*

Plus spécifiquement, si θ est un épimorphisme, et $N = \ker(\theta)$, alors φ est un isomorphisme.

On peut formuler ce résultat en terme du diagramme commutatif suivant



Si $\theta : G \to G'$ est un morphisme de groupes, alors $G/\ker(\theta) \simeq \mathrm{Im}(\theta)$ (exercice).

Par exemple, en vertu du théorème de Lagrange, le groupe alterné $A_n = \ker(\varepsilon)$ est d'ordre $|A_n| = n!/2$. Pour un autre exemple, on a $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$. En effet, on observe d'abord que $\mathbb{R} \lhd \mathbb{C}$, car $(\mathbb{C}, +)$ est abélien. De plus, on a un épimorphisme de groupes $\theta : \mathbb{C} \to \mathbb{R}$, défini par $\theta(a + ib) = b$. Son noyau est $\ker(\theta) = \mathbb{R}$. En vertu du théorème d'isomorphisme, il existe donc un isomorphisme $\varphi : \mathbb{C}/\mathbb{R} \to \mathbb{R}$, comme annoncé.

Démonstration du théorème 4.4. L'unicité de φ se vérifie comme suit. Soit φ et φ', tels que $\theta = \varphi \circ \pi = \varphi' \circ \pi$. Pour $x \in G$ on a $\theta(x) = \varphi \circ \pi(x) = \varphi' \circ \pi(x)$, donc $\varphi(\pi(x)) = \varphi'(\pi(x))$. Donc pour tout $xN \in G/N$ on a $\varphi(xN) = \varphi'(xN)$, et donc $\varphi = \varphi'$.

Pour l'existence, on débute en montrant que la fonction $\varphi : G/N \to G'$, définie par $\varphi(xN) := \theta(x)$, est bien définie. Autrement dit, si $xN = yN$ alors on veut vérifier que $\theta(x) = \theta(y)$. Or, l'hypothèse implique que $x^{-1}yN = N$, et donc $x^{-1}y \in N \subseteq \ker(\theta)$. Il s'ensuit que $\theta(x^{-1}y) = e$. Puisque θ est un morphisme, il en découle que $\theta(x)\theta(y)^{-1} = e$, et donc que $\theta(x) = \theta(y)$. La fonction φ est donc bien définie. Pour le reste de l'énoncé du théorème, on montre d'abord que φ est un morphisme de groupes. En effet, pour $xN, x'N \in G/N$ on constate que

$$\varphi(xN \cdot x'N) = \varphi(xx'N) = \varphi \circ \pi(xx') = \theta(xx') = \theta(x)\theta(x') = \varphi \circ \pi(x)\varphi \circ \pi(x') = \varphi(xN)\varphi(x'N).$$

Maintenant, si pour tout $y \in G'$ on a $x \in G$ tel que $\theta(x) = y$ (θ est un épimorphisme), alors

$$\varphi(xN) = \varphi \circ \pi(x) = \theta(x) = y;$$

et donc φ est un épimorphisme. D'autre part, lorsque $N = \ker(\theta)$, on a $\ker(\varphi) = \{N\}$. En effet, si $\varphi(xN) = e$, alors $\theta(x) = e$ et donc $x \in N$; mais alors $x \in N$ et $xN = N$. On en conclut que φ est bien un monomorphisme. ∎

Corollaire 4.5. *Si G est un groupe simple, alors les morphismes de groupes non-trivaux $\theta : G \to H$ sont forcément des monomorphismes.*

Démonstration. Si θ n'est pas trivial, alors son noyau n'est pas égal à G. Comme G est simple, la seule autre possibilité est que $\ker(\theta) = \{e\}$, et donc θ est un monomorphisme. ∎

4.3 Présentations (finies) de groupes

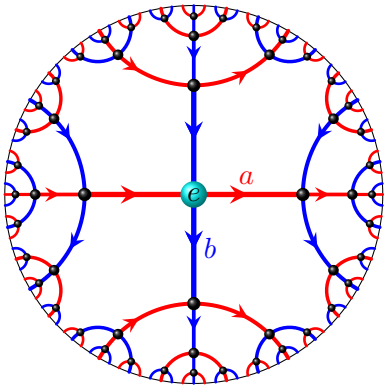


FIGURE 4.1 – Une portion du graphe de Cayley du groupe libre $F_{\{a,b\}}$.

Une autre conséquence des résultats précédents est de permettre les constructions suivantes. Comme l'illustrent les groupes engendrés par des réflexions, plusieurs groupes se décrivent naturellement en terme de générateurs et de relations. Plus explicitement, pour chaque ensemble fini S, on construit d'abord le **groupe libre** F_S sur l'ensemble S des **générateurs**. Les éléments de F_S sont les suites finies $x_1x_2\cdots x_n$, de « lettres » $x_i = s$ ou $x_i = s^{-1}$ pour $s \in S$; avec la condition que $x_i \neq x_{i+1}^{-1}$. Autrement dit, deux lettres consécutives dans le « mot » $x_1x_2\cdots x_n$ ne sont pas l'inverse l'une de l'autre. Par exemple,

$$F_{\{a,b\}} = \{e, a, \overline{a}, b, \overline{b}, ab, ba, a\overline{b}, \overline{b}a, \overline{a}b, b\overline{a}, \overline{a}\overline{b}, \overline{b}\overline{a}, aba, \ldots\}.$$

où e désigne la suite vide, qui est l'élément neutre de ce groupe ; et où on écrit $\overline{a}$ à la place de a^{-1} pour faire plus joli. Le produit de deux suites $\alpha = x_1x_2\cdots x_n$ et $\beta = y_1y_2\cdots y_k$ s'obtient simplement par concaténation de celles-ci : $\alpha\cdot\beta := x_1x_2\cdots x_n\, y_1y_2\cdots y_k$, modulo les simplifications nécessaires, dues au fait que les dernières lettres de α et les premières de β sont telles qu'on doive simplifier. Ces simplifications s'effectuent en effaçant (récursivement) deux lettres consécutives, si elles sont l'inverse l'une de l'autre. Ainsi, on a

$$\begin{aligned}(ab\overline{a}\overline{b}ab)\cdot(\overline{b}ab\overline{a}\overline{b}) &= ab\overline{a}\overline{b}\,\overline{a}\,\overline{b}\,ab\overline{a}\overline{b} \\ &= ab\overline{a}\overline{b}\,\overline{a}a\,ba\overline{a}\overline{b} \\ &= ab\,\overline{b}\overline{b}\,ab\overline{a}\overline{b} \\ &= abab\overline{a}\overline{b}.\end{aligned}$$

Pour S de cardinal plus grand ou égal à 1, le groupe libre est d'ordre infini. Si S n'a qu'un élément, alors F_S s'identifie à $\mathbb{Z}$ (avec l'addition). Dans tous les autres cas, le groupe résultant n'est pas commutatif. Le début du graphe de Cayley du groupe $F_2 = F_{\{a,b\}}$, avec les générateurs a et b, est illustré ci-haut. En principe, on continue le branchement à l'infini.

Bien qu'on interprète les **relations** comme un ensemble d'identités $\alpha = e$, pour α dans F_S ; on les présente plutôt comme un ensemble (fini) dont les éléments sont les membres de gauche de ces identités. Techniquement donc, on se donne R un sous-ensemble fini de F_S, en comprenant que $\alpha \in R$ correspond à l'identité $\alpha = e$. Une **présentation** d'un groupe G prend la forme $\langle S \mid R \rangle$, avec $R \subset F_S$; et le groupe $\langle S \mid R \rangle$ est le groupe quotient

$$\langle S \mid R \rangle := F_S / N_R,$$

où N_R est le plus petit sous-groupe normal de F_S qui contient R. Une façon de « construire » N_R est de considérer le sous-groupe engendré par tous les conjugués $\gamma^{-1}\alpha\gamma$, pour α dans R et γ dans F_S. Le groupe diédral D_m admet la présentation

$$D_m := \langle r, s \mid r^m,\ s^2,\ (r\,s)^2 \rangle,$$

ce qui « signifie » que $r^m = e$, $s^2 = e$, et $(r\,s)^2 = e$. On peut alors vérifier (exercice) que D_m contient exactement $2m$ éléments. On a aussi les présentations suivantes

$$\begin{aligned}
\mathbb{Z}_n &= \big\langle z \mid z^n \big\rangle, \\
\mathrm{SL}_2(\mathbb{Z}) &= \big\langle s, r \mid s^4,\ r^6 \big\rangle, \\
S_n &= \big\langle s_1, \ldots, s_{n-1} \mid s_i^2,\ (s_i s_{i+1})^3,\ (s_i s_j)^2 \text{ pour } |i-j| > 1 \big\rangle, \\
A_n &= \big\langle c_1, \ldots, c_{n-2} \mid c_i^3,\ (c_i c_j)^2 \text{ pour } i \neq j \big\rangle.
\end{aligned}$$

Un même groupe peut avoir plusieurs présentations. Par exemple, on a

$$A_5 = \big\langle a, b \mid a^2,\ b^3,\ (ab)^5 \big\rangle = \big\langle c, d \mid c^2,\ d^4,\ (cd)^5,\ (c^{-1}d^{-1}cd)^3 \big\rangle.$$

On a souvent des relations qui font intervenir le **commutateur**, $[a, b] := a^{-1}b^{-1}ab$, de deux éléments. On observe que

$$[a, b] = e \qquad \text{ssi} \qquad a^{-1}b^{-1}ab = e \qquad \text{ssi} \qquad ab = ba,$$

ce qui explique la terminologie. On peut montrer que tout groupe fini admet une présentation finie. Bien qu'on puisse parfois déterminer l'ordre d'un groupe à partir de sa présentation, c'est souvent un problème difficile. En fait le **problème du mot**, qui consiste à déterminer si deux mots donnent le même élément du groupe, est un problème **indécidable**. Informellement, cela signifie qu'il n'existe pas d'algorithme qui permette de décider (en toute généralité) si deux mots sont égaux. C'est le théorème de Novikov [1]. Cependant, on peut déterminer certaines classes de présentations de groupes pour lesquelles le problème du mot est décidable.

4.4 Sous-groupes d'un groupe quotient

Pour mieux circonscrire la structure du groupe quotient G/N, en particulier en ce qui concerne ses sous-groupes, la proposition suivante est fondamentale.

1. Voir Petr Novikov (1901-1975)

Proposition 4.6. *Soit G un groupe, $N \lhd G$ et $\pi : G \to G/N$ l'épimorphisme canonique. Alors la fonction $K \mapsto \pi(K)$ est une bijection de l'ensemble des sous-groupes de G contenant N sur l'ensemble des sous-groupes de G/N.*

Autrement dit, $L \leqslant G/N$ si et seulement si il existe $N \leqslant K \leqslant G$ tel que $\pi(K) = L$. De plus, on a $N \lhd K$ (puisque $N \lhd G$), et donc un groupe quotient K/N. D'autre part, grâce au théorème ci-dessus on sait que $\pi(K) \leqslant G/N$. Ainsi, en vertu du théorème d'isomorphisme que $\pi(K) \simeq K/N$ (exercice) ; et donc, par le théorème de Lagrange, $|\pi(K)| = |K|/|N|$ (exercice). Ceci mène à la formule

$$|G/N| = |G/K| \cdot |K/N|.$$

Enfin, pour $K = \langle S \rangle$, on a $\pi(K) = \langle \pi(S) \rangle$ (exercice).

Démonstration de la proposition 4.6. Soit $K \leqslant G$ contenant N. Pour voir que $\pi(K)$ est un sous-groupe de G/N, on observe d'abord $N \in \pi(K)$ car $N \subseteq K$ implique $\pi(N) = N \subseteq \pi(K)$. D'autre part, pour $xN, yN\pi(K)$ on a $x, y \in K$, et donc $xN(yN)^{-1} = xy^{-1}N = \pi(xy^{-1}) \in \pi(K)$. Il s'ensuit que $\pi(K) \leqslant G/N$. Autrement dit, la fonction $K \to \pi(K)$ est bien définie. Reste à montrer qu'elle est bijective.

Surjectivité : Soit $L \leqslant G/N$, posons $K = \pi^*(L) = \{g \in G \,|\, \pi(g) \in L\}$. Alors $e \in K$ car $\pi(e) = N \in L$. Si $x, y \in K$ alors puisque π est un morphisme de groupes on a $\pi(xy^{-1}) = \pi(x)\pi(y)^{-1} \in L$ car $L \leqslant G/N$, donc $xy^{-1} \in K$. Donc $K \leqslant G$. L'application est surjective.

Injectivité : Soit K, K' deux sous-groupes de G contenant N tel que $\pi(K) = \pi(K')$. Par symétrie, il suffit de montrer que $K \subseteq K'$ pour montrer que $K = K'$ et donc son injectivité. Soit $x \in K$ alors $\pi(x) \in \pi(K) = \pi(K')$. Donc $xN = yN$ avec $y \in K'$. Ce qui implique qu'il existe $h \in N$ tel que $x = yh$. Puisque $N \subseteq K'$, $y, h \in K'$. En outre, puisque $x = yh$ et $K' \leqslant G$, on obtient que $x \in K'$. ∎

4.5 Groupes monogènes et cycliques

Un autre des résultats fondamentaux de la théorie des groupes ramène l'étude des groupes abéliens aux groupes monogènes et cycliques. À leur tour, on montre que ceux-ci sont forcément, à isomorphisme près, soit $\mathbb{Z}$, soit $\mathbb{Z}_n$, pour $n \in \mathbb{Z}$. Plus précisément, on a le résultat suivant.

Proposition 4.7. *Soit $G = \langle x \rangle$ un groupe monogène, alors*

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

Démonstration. On considère $\theta : \mathbb{Z} \to G$ définie par $\theta(n) = x^n$. Alors θ est un morphisme de groupes : $\theta(n + m) = x^{n+m} = x^n x^m = \theta(n)\theta(m)$ (on notera que $\mathbb{Z}$ est un groupe noté additivement tandis que

G est noté multiplicativement). Il est clair que θ est surjectif. Si $\ker(\theta) = \{0\}$ alors $G \simeq \mathbb{Z}$. Si $\ker(\theta)$ n'est pas 0 alors il existe $n \in \mathbb{Z}$ tel que $\ker(\theta) = n\mathbb{Z}$ car $\ker(\theta)$ est un sous-groupe de $\mathbb{Z}$ et les seuls sous-groupes de $\mathbb{Z}$ sont les ensembles de multiples. Donc en vertu du théorème d'isomorphismes, $G \simeq \mathbb{Z}_n$. Puisque $n = |G| = |\mathbb{Z}_n = n$, on en déduit le théorème. ■

Corollaire 4.8. *Tout sous-groupe d'un groupe cyclique est cyclique.*

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

Exemples.

(a) Soit $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$. On a $\mathbb{U} \leqslant (\mathbb{C}^*, \cdot)$ et $\mathbb{U} \simeq (\mathbb{R}, +)/ < 2\pi >$.

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

4.6 A_5 comme groupe des rotations du dodécaèdre

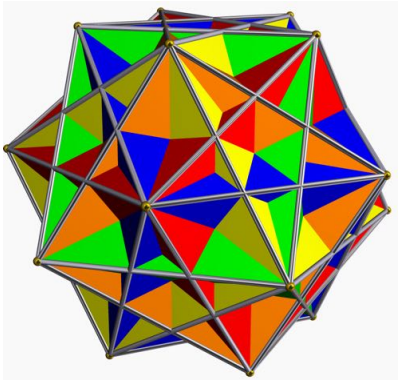


FIGURE 4.2 – Les cinq cubes inscrits dans le dodécaèdre.

Le groupe des rotations du dodécaèdre est isomorphe au groupe alterné A_5. Pour le voir, on raisonne comme suit. Pour chaque diagonale d'une face (joignant un sommet à un sommet de cette face qui ne lui est pas immédiatement voisin), on a un et un seul cube inscrit dans le dodécaèdre dont un côté correspond à cette diagonale. En fait, les 12 côtés de ce cube correspondent à une diagonale dans chacune des 12 faces du dodécaèdre. Comme chaque face (pentagonale) du dodécaèdre contient 5 diagonales, il y a 5 cubes différents inscrits dans le dodécaèdre (voir Figures 4.3 et 4.4). On les nomme $\{1, 2, 3, 4, 5\}$, et cela se répercute en une façon d'étiquetter les diagonales ; en donnant à chaque coté d'un cube l'étiquette du cube. Chaque rotation du dodécaèdre envoie un cube inscrit dans un cube inscrit, puisqu'elle respecte les longueurs et les angles, et cela donne une permutation des 5 valeurs des étiquettes des diagonales. D'autre part, deux rotations sont différentes si et seulement si elles font effectuer des permutations différentes aux 5 cubes. Manifestement, le composé de rotations correspond au composé des permutations de cubes correspondantes. On a donc un monomorphisme du groupe des rotations du dodécaèdre vers le groupe S_5, et on cherche à montrer que l'image de ce monomorphisme est le sous-groupe alterné A_5. Par le premier théorème d'isomorphisme, on pourra alors conclure que le groupe des rotations du dodécaèdre est isomorphe au groupe alterné A_5.

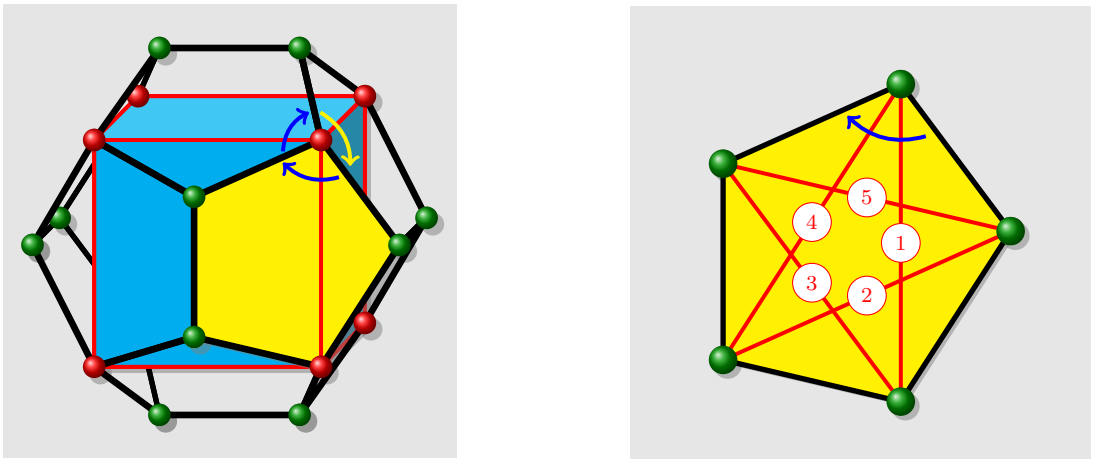


FIGURE 4.3 – Une rotation du dodécaèdre autour de l'axe joignant deux sommets opposés, et la permutation des 5 cubes correspondante.

On considère une rotation horaire de $2\pi/3$ autour de l'axe joignant un sommet au sommet diamétralement opposé dans le dodécaèdre. Cette rotation laisse fixes (en leur faisant effectuer une rotation) exactement deux des 5 cubes inscrits. En effet, ce sont les deux cubes pour lesquels cet axe est aussi une grande diagonale ; ou encore, ce sont les deux cubes dont l'un des sommets est sur l'axe de rotation. Les 3 autres cubes sont permutés entre eux, et la seule possibilité est que c'est selon une permutation cyclique de longueur 3. Pour la rotation de la figure 4.3, les cubes numérotés 1 et 4, selon les diagonales du pentagone de la partie droite de la figure, sont laissés fixes. Les 3 autres cubes sont permutés selon la permutation cyclique (235).

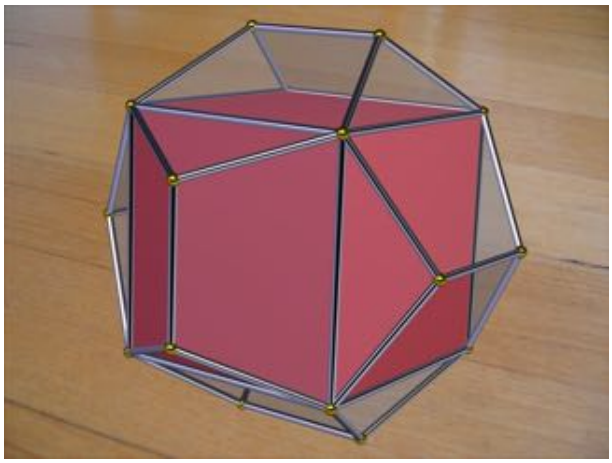


FIGURE 4.4 – Version réaliste d'un cube inscrit dans le dodécaèdre.

Le dodécaèdre possède 20 sommets, et il leurs correspond 20 rotations horaires de $2\pi/3$, comme celle décrite ci-dessus. À chacune de ces 20 rotations, on associe une permutation cyclique de longueur 3, et il y en a 20 différentes (puisque les 20 rotations sont différentes). Or, il y a exactement $20 = 2\binom{5}{3}$ permutations cycliques de longueur 3 dans S_5, qui correspondent à choisir 3 des éléments de $\{1, 2, 3, 4, 5\}$ avec deux cycles pour chaque choix. Il s'ensuit qu'on obtient exactement toutes les permutations cycliques de longueur 3 de S_5, en considérant les rotations décrites ci-haut. Bien entendu, en composant ces rotations on obtient d'autres rotations du dodécaèdre qui permutent les cubes selon d'autres permutations. Nous voulons voir qu'il en a 60, et qu'elles correspondent aux soixante permutations dans A_n.

Le fait qu'il y a (au plus) 60 rotations du dodécaèdre est facile à établir. On choisit deux sommets adjacents A et B, et on « suit leurs traces ». Une rotation θ envoie le sommet A sur n'importe lequel des 20 autres sommets, et le sommet B sur l'un des 3 voisins de l'image de $\theta(A)$. Le choix de ce second sommet fixe la rotation. Il y a donc (au plus) 60 rotations possibles du dodécaèdre. Nous allons montrer ci-dessous (voir Lemme 4.9) que le sous-groupe A_5 est engendré par les permutations cycliques de longueur 3. En vertu de notre raisonnement ci-haut, il y a donc exactement 60 rotations du dodécaèdre,

qui constituent (pour la composition) un groupe isomorphe à A_5.

Lemme 4.9. *Le sous-groupe alterné A_n, du groupe des permutations S_n, est engendré par les permutations cycliques de longueur* 3.

Démonstration. Par définition A_n contient toutes les permutations cycliques de longueur 3, puisque leur signe est positif. Pour voir qu'elles engendrent tout A_n, on rappelle que toute permutation peut s'exprimer comme produit de transpositions de la forme $(1a)$ (voir Exercice 1.37), et que celles qui sont dans A_n s'expriment (par définition) comme un produit d'un nombre pair de ces transpositions, qui peuvent donc être regroupées deux par deux. Or, le produit $(1a)(1b)$ est égal à la permutation cyclique $(1ba)$. On a donc bien une expression de tout élément de A_n comme produit de cycles de longueur 3, tel qu'annoncé. ∎

La proposition suivante découle du fait que A_5 est le groupe des rotations du dodécaèdre.

Proposition 4.10. *A_5 est un groupe simple.*

Démonstration. Soit $\varphi : A_5 \to G$ un morphisme de group qui n'est pas injectif. Autrement dit, on suppose que $\ker(\varphi)$ contient au moins un élément de A_5, autre que l'identité. Nous allons voir que la classe de conjugaison de g engendre forcément tout A_5, et donc que A_5 n'a pas de sous-groupe normal propre. On rappelle d'abord (voir Exercice 3.2) que g est soit d'ordre 2, soit d'ordre 3, soit d'ordre 5, puis on utilise l'interprétation de A_5 comme groupe de rotation du dodécaèdre pour conclure que la classe de conjugaison de g engendre tout A_5. En fait, nous l'avons déjà fait pour le cas où l'ordre de g est 3, puisque cela correspond aux permutations cycliques d'ordre 3. Ne reste plus qu'à faire de même pour les deux autres cas.

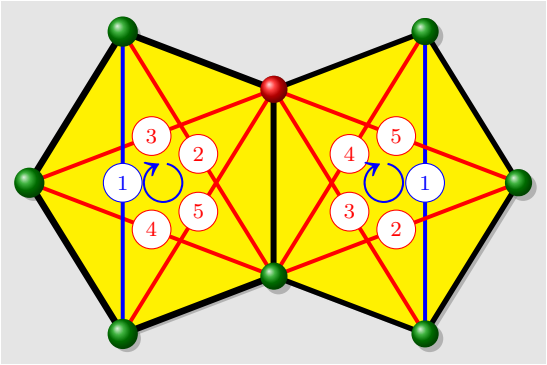


FIGURE 4.5 – Permutation des 5 cubes, pour une rotation du dodécaèdre selon des faces.

Les rotations d'ordre 5 du dodécaèdre correspondent aux rotations autour de l'axe perpendiculaire à l'une des faces du dodécaèdre, qui est aussi perpendiculaire à la face opposée. Ces rotations permutent de façon circulaire les cinq cubes inscrits. On a exactement 24 telles rotations, qui correspondent aux 6 façons de choisir deux faces opposées, avec 4 rotations (différentes de l'identité) pour chacun de ces choix. Or, il y a 24 permutations cycliques dans S_5, toutes appartenant à A_5. Pour deux faces adjacentes, comme à la figure ci-contre, le produit des permutations en question est une permutation cyclique d'ordre 3, ce qui nous ramène au cas déjà montré. L'exemple ci-contre illustre ce fait, avec

$$(13254) \circ (12345) = (153).$$

Enfin, les rotations d'angle π autour de l'axe reliant le centre d'un côté du dodécaèdre au côté opposé, sont celles qui correspondent au type cyclique 221 (d'ordre 2). Par exemple, avec les deux faces de la figure ci-dessus et la rotation selon le centre du côté qu'elles partagent, on obtient la permutation des diagonales (23)(45), avec la diagonale 1 laissée fixe (puisqu'on fait tourner le cube correspondant à 1 d'un angle π autour de l'axe qui relie le centre d'une de ses faces au centre de la face opposée). En composant deux telles rotations, pour des côtés issus d'un même sommet, on trouve une permutation cyclique d'ordre 5. On est encore une fois réduit au cas précédent. Par exemple, prenant le côté à la droite du sommet rouge de la figure, on trouve la rotation correspondant à la permutation (15)(34), et le composé donne (13524). ■

4.7 Groupes résolubles

Un groupe fini G est dit **résoluble** s'il existe une chaîne de groupes

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G,$$

où chaque G_i est un sous-groupe normal de G_{i+1}, avec l'ordre de G_{i+1}/G_i un nombre premier. On dit alors que la chaîne ci-haut est une résolution du groupe G. Un groupe simple dont l'ordre n'est pas un nombre premier n'est donc pas résoluble. C'est le cas pour tout A_n, pour tout $n \geqslant 5$.

En théorie de Galois, on associe à chaque polynôme un groupe fini, et on montre qu'il existe une formule par radicaux pour les racines du polynôme si et seulement si le groupe du polynôme est résoluble. On montre aussi qu'il y a des polynômes pour lesquels le groupe de Galois associé est A_n. Il s'ensuit qu'il n'existe pas de formule par radicaux donnant les racines d'un polynôme de degré plus grand ou égal à 5. On connaît de telles formules pour les degrés 2, 3 et 4.

Un autre aspect intéressant de la théorie de Galois est qu'une résolution du groupe de Galois d'un polynôme donne une façon explicite de calculer ses racines. On a donc ainsi des résultats positifs, pour les polynômes dont le groupe est résoluble. En particulier, on peut trouver ainsi les formules générales pour les polynômes de degré 3 et 4. Tout cela est au menu du cours Théorie de Galois.

4.8 Exercices

Exercice 4.1. Soit G un groupe et $H \leqslant G$, montrer que les énoncés suivants sont équivalents.

(a) $H \lhd G$;

(b) $xHx^{-1} = H$, pour tout $x \in G$;

(c) $x^{-1}Hx = H$, pour tout $x \in G$;

(d) $xhx^{-1} \in H$, pour tout $x \in G$ et tout $h \in H$;

(e) $x^{-1}hx \in H$, pour tout $x \in G$ et tout $h \in H$.

Exercice 4.2. Soit G un groupe et $H \leqslant G$ d'indice 2, montrer que H est normal dans G.

Exercice 4.3. Soit G un groupe, montrer que $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$.

Exercice 4.4. Soit G un groupe et $S \subseteq G$. Posons $H = \langle S \rangle$.

(a) Montrer que si $xSx^{-1} \subseteq H$ pour tout $x \in G$, alors $H \lhd G$.

(b) Si $f : G \to G'$ est un isomorphisme, montrer que $f(H) = \langle f(S) \rangle$.

Exercice 4.5. Dans le groupe symétrique S_4, on considère

$$H = \langle (1,2)(3,4) \rangle \quad \text{et} \quad K = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

(a) Vérifier que $K = \langle (1,2)(3,4), (1,3)(2,4) \rangle$.

(b) Montrer que $H \lhd K$ et $K \lhd S_4$, mais que H n'est pas normal dans S_4.

Exercice 4.6. Trouver tous les sous-groupes de S_3, et déterminer ceux qui sont normaux.

Exercice 4.7. Soit G un groupe et $H, K \leqslant G$, montrer que

(a) si $H \lhd G$ et $K \leqslant G$ contenant H alors $H \lhd K$;

(b) $H \lhd G \Longrightarrow H \cap K \lhd G$;

(c) En déduire que l'intersection de sous-groupes normaux de G est un sous-groupe normal de G.

Exercice 4.8. Soit G un groupe et $H, K \leqslant G$.

(a) Montrer que $HK \leqslant G \iff HK = KH$.

(b) Montrer que si $HK \leqslant G$ alors $HK = \langle H \cup K \rangle$. Est-ce que dans ce cas HK est abélien ?

(c) Montrer que si $H \lhd G$ alors $HK \leqslant G$ et $H \lhd HK$.

Exercice 4.9. Soit $\theta : G \to G'$ un morphisme de groupes, montrer que

(a) si $H \lhd G$ alors $\theta(H) \leqslant \theta(G)$, et que si θ est surjectif alors $\theta(H) \lhd G'$. Est-ce vrai dans le cas où θ n'est pas surjectif ?

(b) Si $H' \lhd G'$ alors $\theta^{-1}(H') \lhd G$.

Exercice 4.10. Si $\theta : G \to G'$ est un morphisme de groupes, montrer que $G/\ker(\theta) \simeq \mathrm{Im}(\theta)$.

Exercice 4.11. Soit $n \in \mathbb{N}$ et d qui divise n.

(a) Montrer qu'il existe un morphisme de groupes injectif $\iota : (\mathbb{Z}_d, +) \to (\mathbb{Z}_n, +)$.

(b) Montrer qu'il existe un morphisme de groupes surjectif $\varphi : (\mathbb{Z}_n, +) \to (\mathbb{Z}_d, +)$.

Exercice 4.12. Soit G un groupe, $H \lhd G$ et K est un sous-groupe de G contenant H. On note $\pi : G \to G/H$ le morphisme surjectif canonique. Montrer que

(a) $\pi(K) \simeq K/H$;

(b) si $K = \langle S \rangle$ alors $\pi(K) = \langle \pi(S) \rangle$;

(c) si K est fini, alors $|\pi(K)| = |K|/|H|$.

Exercice 4.13. Donner tous les sous-groupes de $(\mathbb{Z}_{20}, +)$.

Exercice 4.14. (Deuxième et troisième théorèmes d'isomorphisme)

Soit G un groupe et $H \lhd G$ et $K \leqslant G$.

(a) Montrer que $H \cap K \lhd G$ et $K/(K \cap H) \simeq HK/H$.

(b) Si de plus $K \lhd G$ et $K \subseteq H$, montrer que $H/K \lhd G/K$ et $(G/K)/(H/K) \simeq G/H$.

Indice : Se servir du premier théorème d'isomorphisme.

Exercice 4.15. Soit G un groupe, montrer que si $G/Z(G)$ est un groupe monogène, alors G est abélien.

Exercice 4.16. Justifier les isomorphismes suivants :

(a) $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$;

(b) $(\mathbb{R}/\mathbb{Z}, +) \simeq (\mathbb{U}, \cdot)$;

(c) $(\mathbb{C}^*/\mathbb{R}^{+*}, \cdot) \simeq (\mathbb{U}, \cdot)$;

(d) $(\mathbb{C}^*/\mathbb{R}^*, \cdot) \simeq (\mathbb{U}, \cdot)$;

(e) $(\mathbb{U}/\mathbb{U}(n), \cdot) \simeq (\mathbb{U}, \cdot)$;

(f) $(\mathbb{C}^*/\mathbb{U}(n), \cdot) \simeq (\mathbb{C}^*, \cdot)$.

Exercice 4.17. Soit G un sous-groupe d'indice fini dans $(\mathbb{C}^*, \cdot)$, montrer que $G = (\mathbb{C}^*, \cdot)$.

Exercices exploratoires

Exercice 4.18. Les **groupes de Coxeter** sont les groupes qui admettent une présentations $W = \langle S \mid R \rangle$, avec les relation dans R de la forme $(st)^{m(s,t)}$ pour toute paire s, t d'éléments de S. On demande que les $m(s,t)$ soient des entiers ; et que

(1) $m(s,s) = 1$,

(2) $m(s,t) \geqslant 2$ si s est différent de t,

(3) $m(s,t) = m(t,s)$.

Pour que le groupe W soit fini, il y a de fortes contraintes sur les entiers $m(s,t)$, et Coxeter a pu classifier toutes les possibilités de tels groupes qui soient irréductibles pour le produit (voir exercice (b) et (c)). Montrer que :

(a) Deux générateurs s et t commutent si et seulement si $m(s,t) = 2$.

(b) Si $S = S_1 + S_2$ avec $m(s_1, s_2) = 2$ pour tout $s_1 \in S_1$ et $s_2 \in S_2$, alors

$$W = W_1 \times W_2,$$

pour $W_1 = \langle S_1 \mid R_1 \rangle$ et $W_2 = \langle S_2 \mid R_2 \rangle$, avec des choix judicieux de R_1 et R_2.

(c) Si W_1 et W_2 sont deux groupes de Coxeter, alors on peut présenter $W_1 \times W_2$ comme un groupe de Coxeter.

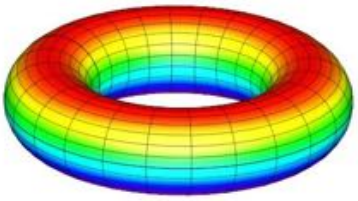
(d) Les groupes diédraux sont des groupes de Coxeter.

(e) Le groupe symétrique S_n est un groupe de Coxeter.

(f) Le groupe de Coxeter avec 3 générateurs s, t, r et les relations $m(s, r) = 3$, $m(r, t) = 3$ et $m(s, t) = 3$ est infini.

Chapitre 5

Produits de groupes



Le « produit direct » permet de construire de nouveaux groupes, à partir de groupes donnés. À l'inverse, on peut « décomposer » un groupe en produit direct, ce qui révèle sa structure. Nous allons décrire ces constructions et leurs propriétés.

5.1 Le produit direct

Pour deux groupes G, H, on considère sur le produit cartésien

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

l'opération de groupe obtenue en posant

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

L'élément neutre est (e, e), et l'inverse se calcule comme suit

$$(g, h)^{-1} = (g^{-1}, h^{-1}).$$

En effet, on vérifie que

$$\begin{aligned}
(g, h) \cdot (e, e) &= (ge, he) = (g, h) \\
(e, e)(g, h) &= (eg, eh) = (g, h) \\
(g, h) \cdot (g^{-1}, h^{-1}) &= (gg^{-1}, hh^{-1}) = (e, e) \\
(g^{-1}, h^{-1}) \cdot (g, h) &= (g^{-1}g, h^{-1}h) = (e, e).
\end{aligned}$$

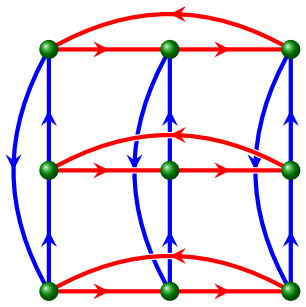


FIGURE 5.1 – Graphe de Cayley de $\mathbb{Z}_3 \times \mathbb{Z}_3$.

L'associativité se vérifie aussi de même façon. C'est le **produit direct** (ou **produit direct externe**), de G avec H. On obtient ainsi, par exemple, le groupe $\mathbb{Z} \times \mathbb{Z}$; ou encore le groupe $\mathbb{Z}_n \times \mathbb{Z}_k$, d'ordre $n\,k$. On observe que $\mathbb{Z}_2 \times \mathbb{Z}_2$ (d'ordre 4) n'est pas isomorphe à $\mathbb{Z}_4$. En effet, dans $\mathbb{Z}_2 \times \mathbb{Z}_2$ on a $g + g = e$ pour tout g, ce qui n'est pas le cas dans $\mathbb{Z}_4$. Par contre, $\mathbb{Z}_6$ est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_3$. Plus généralement, comme on va le voir plus tard , $\mathbb{Z}_n \times \mathbb{Z}_k$ n'est isomorphe à $\mathbb{Z}_{nk}$, que si n et k sont premiers entre eux, c.-à-d. $\text{pgcd}(n, k) = 1$.

La construction du produit direct se généralise aisément à plusieurs facteurs. Ainsi, pour n groupes $G_1, \ldots, G_n$, on a le produit direct de groupes $G_1 \times \cdots \times G_n$ avec l'opération

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) := (x_1 y_1, x_2 y_2, \ldots, x_n y_n) \qquad (5.1)$$

On écrit aussi parfois $\Pi_{i=1}^n G_i$, pour ce produit. On vérifie facilement (exercice) la proposition suivante.

Proposition 5.1. *Si $\theta_i : G_i \longrightarrow G_i'$, pour $1 \leqslant i \leqslant n$, sont des morphismes de groupes, alors on a un morphisme de groupe*

$$\theta_1 \times \cdots \times \theta_n : G_1 \times \cdots \times G_n \longrightarrow G_1' \times \cdots \times G_n'$$

définie en posant

$$(\theta_1 \times \cdots \times \theta_n)(x_1, \ldots, x_n) = (\theta_1(x_1), \ldots, \theta_n(x_n)),$$

pour $(x_1, \ldots, x_n)$ dans $G_1 \times \cdots \times G_n$. Si les θ_i sont des monomorphismes (resp. épimorphisme, ou isomorphisme), alors $\theta_1 \times \cdots \times \theta_n$ est un monomorphisme (resp. épimorphisme, ou isomorphisme). Dans le cas où les θ_i sont des isomorphismes, l'inverse de $(\theta_1 \times \cdots \times \theta_n)$ est $(\theta_1^{-1} \times \cdots \times \theta_n^{-1})$, et c'est donc un isomorphisme.

Pour chaque k, entre 1 et n, on a un monomorphisme de groupes $\iota_k : G_k \to G_1 \times \cdots \times G_n$, défini en posant

$$\iota_k(x) := (\underbrace{e, \ldots, e}_{k-1}, x, e, \ldots, e),$$

et un épimorphisme de groupes $\pi_k : G_1 \times \cdots \times G_n \to G_k$, simplement définis en posant

$$\pi_k(x_1, \ldots, x_n) := x_k.$$

On dit de ι_k que c'est **l'inclusion** de G_k dans le produit, et de π_k que c'est la k^{e} **projection** sur la composante G_k. On vérifie aisément que $\pi_k \circ \iota_k = \text{Id}$, ou formulé en terme diagramme commutatif :

$$\begin{array}{ccc} G_k & \xrightarrow{\iota_k} & G_1 \times \cdots \times G_n \\ & \searrow^{\text{Id}} & \downarrow{\scriptstyle \pi_k} \\ & & G_k \end{array}$$

De plus, l'image de G_k par ι_k est un sous-groupe normal du produit. Plus généralement, pour des sous-groupes H_i des G_i, le produit direct $H_1 \times \cdots \times H_n$ est un sous-groupe de $G_1 \times \cdots \times G_n$, qui est normal si chacun des H_i l'est. On a alors (exercice)

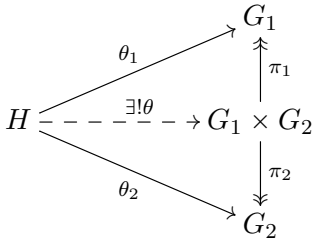
$$(G_1 \times G_2)/(H_1 \times H_2) \simeq (G_1/H_1) \times (G_2/H_2). \tag{5.2}$$

La propriété **universelle**[1] qui caractérise le produit direct de groupes fait l'objet de la proposition suivante.

Proposition 5.2. *Pour tout groupe H, et des morphismes $\theta_1 : H \to G_1$ et $\theta_2 : H \to G_2$, il existe un unique morphisme $\theta : H \to G_1 \times G_2$, tel que*

$$\pi_1 \circ \theta = \theta_1, \qquad \text{et} \qquad \pi_2 \circ \theta = \theta_2.$$

On écrit alors $\theta = (\theta_1, \theta_2)$, puisque $f(h) = (\theta_1(h), \theta_2(h))$. Formulé en terme de diagramme commutatif, ceci prend la forme



5.2 Le produit direct interne

Les observations précédentes entraînent que le groupe $G = G_1 \times G_2$ peut se décrire sous la forme

$$G = HK := \{xy \mid x \in H \text{ et } y \in K\},$$

où $H := G_1 \times \{e\}$,et $K := \{e\} \times G_2$ sont des sous-groupes normaux de G d'intersection vide, c.-à-d. $H \cap K = \{e\}$. Ainsi, le produit est « réalisé » à l'intérieur de G. Cela mène à une version « interne » de la notion de produit directe, dont le définition passe par la proposition suivante.

Proposition 5.3. *Dans un groupe G, si H et K sont des sous-groupes normaux de G tels que*

$$H \cap K = \{e\}, \qquad \text{et} \qquad G = HK,$$

alors $G \simeq H \times K$.

1. Cela explique le « rôle » du produit direct.

Démonstration. Considérons la fonction $\varphi : H \times K \to G$, avec $\varphi(x, y) := xy$. La condition $G = HK$ dit précisément que cette fonction est surjective. C'est aussi un morphisme puisqu'on a les deux égalités

$$\begin{aligned} \varphi((x_1, y_1) \cdot (x_2, y_2)) &= \varphi(x_1x_2, y_1y_2) = x_1x_2\, y_1y_2 \\ \varphi(x_1, y_1) \cdot \varphi(x_2, y_2) &= (x_1y_1) \cdot (x_2y_2) = x_1y_1x_2y_2 \end{aligned}$$

Pour voir que les deux expressions résultantes sont égales, on observe que $x_2y_1 = y_1x_2$, ou autrement dit $x_2y_1\, x_2^{-1}y_1^{-1} = e$. En effet, on a d'abord $x_2\, y_1\, x_2^{-1} \in K$, car K est normal dans G, et donc $x_2y_1x_2^{-1}y_1^{-1}$ est dans K. De mêmes façons, on vérifie que $x_2y_1x_2^{-1}y_1^{-1}$ appartient à H. On a donc que $x_2y_1x_2^{-1}y_1^{-1}$ est dans l'intersection $H \cap K = \{e\}$, d'où l'assertion. Le morphisme φ est injectif, car $\varphi(x, y) = e$ implique $xy = e$, alors $y = y^{-1} \in H \cap K$; d'où $x = e$, $y^{-1} = e$, et donc $y = e$. D'où $(x, y) = (e, e)$. On conclut donc que φ est un isomorphisme. ∎

Cette proposition suggère de dire, pour un groupe G contenant deux sous-groupes normaux H et K satisfaisant les conditions de la proposition H, K, que G est le **produit direct interne** des sous-groupes H et K. Lorsque ceci est le cas, on dit que G se **décompose** comme produit direct de ses sous-groupes H et K. On dit aussi que H et K sont les **facteurs** de cette décomposition. Par exemple, $\mathbb{Z}_6$ est produit direct interne de ses sous-groupes $\langle 3\rangle$ et $\langle 2\rangle$. Bien entendu, la notion de produit direct interne se généralise à plus de deux facteurs. Ainsi, G est le produit direct interne de ses sous-groupes normaux $H_1 \ldots, H_n$, si on a

$$H_i \cap \langle H_1 \cup \ldots \cup \widehat{H_i} \cup \ldots \cup H_n\rangle = \{e\},$$

pour tout $1 \leqslant i \leqslant n$, et

$$G = H_1H_2 \ldots H_n.$$

Ainsi, $\mathbb{Z}_{30}$ est produit direct interne de ses sous-groupes $\langle 15\rangle$, $\langle 10\rangle$ et $\langle 6\rangle$. On montre facilement une généralisation de la Proposition 5.3, à savoir que, si G est produit direct interne des H_i, avec $1 \leqslant i \leqslant n$, alors

$$G \simeq H_1 \times H_2 \times \cdots \times H_n.$$

Bien entendu, comme dans le cas $n = 2$, lorsque G est un tel produit direct interne des H_i, on dit qu'il se décompose en produit direct des H_i, et que les H_i sont les facteurs de cette décomposition.

On peut facilement déterminer une présentation du produit direct de deux groupes, pour lesquels on a des présentations. On montre la proposition suivante.

Proposition 5.4. *Pour des présentations $G_1 = \langle S_1 \mid R_1\rangle$ et $G_2 = \langle S_2 \mid R_2\rangle$, avec $S_1 \cap S_2 = \varnothing$, on a la présentation*

$$G_1 \times G_2 = \langle\, S_1 + S_2 \mid R_1 + R_2 + C\,\rangle,$$

ou l'ensemble de relations suplémentaires

$$C := \{a^{-1}b^{-1}a\, b \mid a \in S_1,\ b \in S_2\},$$

assure que tous les générateurs de G_1 commutent avec les générateurs de G_2.

5.3 Produits semi-directs

Dans la foulée de la section précédente, il peut sembler naturel d'affaiblir les conditions de la proposition 5.3, en supposant que l'un des deux sous-groupes n'est pas nécessairement normal. La pratique montre que c'est une excellente idée. Ainsi, pour un groupe G, on considère deux sous-groupes N et H, avec seulement N supposé normal, et tels que

$$N \cap H = \{e\}, \qquad \text{et} \qquad G = NH.$$

Si tel est le cas, on dit que G est un produit **semi-direct interne** des sous-groupes H et N. On note[2] alors $G = N \rtimes H$, et on montre que tout élément g de G s'écrit de manière unique comme $g = n\,h$, avec $n \in N$ et $h \in H$. On a l'énoncé suivant, dont la preuve est laissée en exercice.

Proposition 5.5. *Le composé de l'inclusion $N \hookrightarrow G$ avec la projection $G \twoheadrightarrow G/N$ donne un isomorphisme $H \xrightarrow{\sim} G/N$. De plus, la fonction*

$$\varphi : H \to \mathrm{Aut}(N), \qquad \textit{telle que} \qquad \varphi_h(n) := h\,n\,h^{-1},$$

est un morphisme de groupes. Ici, on désigne par φ_h l'image de h par φ, c'est donc un automorphisme $\varphi_h : N \to N$.

Cette proposition ouvre la porte à la version « externe » du produit semi-direct, qui elle-même mène à plusieurs domaines de recherche contemporains (algèbre homologique, topologie combinatoire, cohomologie de groupes, extensions de groupes, etc.) dépassant tous le niveau d'un premier cours sur la théorie des groupes. Elle se décrit comme suit, et correspond essentiellement à « oublier » que N et H sont des sous-groupes de G. Rappelons qu'à la Section 3.6, on a montré qu'un morphisme $\varphi : H \to \mathrm{Aut}(K)$ est équivalent à la donnée d'une action $\varphi : H \times K \to K$ de H sur K, aussi désignée ici par φ.

On considère deux groupes K et H, et une action (arbitraire) $\varphi : H \times K \to K$. Ces trois ingrédients permettent de construire une structure de groupe sur l'ensemble $K \times H$ (pas le groupe, l'ensemble), en posant

$$(k_1, h_1) \cdot (k_2, h_2) := (k_1 \cdot \varphi(h, k_2)\,,\; h_1 \cdot h_2).$$

Ainsi, φ « tord » le produit dans sa première composante. Le résultat est le produit **semi-direct (externe)**, noté $G = K \rtimes_\varphi H$. IL est clair qu'on récupère le produit direct usuel en choisissant pour φ l'action **triviale** $\varphi(h, k) := k$. On peut vérifier alors que $K \times \{e\}$ et $\{e\} \times H$ sont sous-groupes de $K \rtimes_\varphi H$, avec $K \times \{e\}$ normal.

Par exemple, on peut montrer que le groupe diedral D_{2n} est isomorphe au produit semidirect $\mathbb{Z}_n \rtimes_\varphi C_2$, avec $\varphi : C_2 \to \mathbb{Z}_n$ le morphisme $\varphi_i(k) := i\,k$; considérant que $C_2 = \{\pm 1\}$ est muni de

2. L'ordre de N et H est important, puisqu'il indique quel est le sous-groupe (le premier) qui est forcément normal.

la multiplication. Autrement dit, $\varphi_1(k) = k$, et $\varphi_{-1}(k) = -k$. Comme $\mathbb{Z}_n$ est abélien, on a bien $\varphi_{-1}(k_1\, k_2) = \varphi_{-1}(k_1)\varphi_{-1}(k_2)$. Plus explicitement, la loi de composition de $\mathbb{Z}_n \rtimes_\varphi C_2$ est comme suit :

$$\begin{aligned}(k,1)\cdot(\ell,1) &= ((k+\ell \bmod n),1),\\ (k,1)\cdot(\ell,-1) &= ((k-\ell \bmod n),-1),\\ (k,-1)\cdot(\ell,1) &= ((k+\ell \bmod n),-1),\\ (k,-1)\cdot(\ell,-1) &= ((k-\ell \bmod n),1).\end{aligned}$$

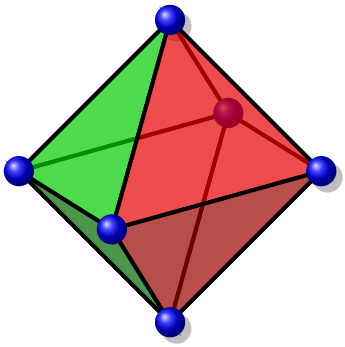


FIGURE 5.2 – L'octaèdre.

Le groupe hyperoctaédral, B_n. Un exemple classique de produit semi-direct est le groupe B_n des matrices $n \times n$ qui contiennent une et une seule valeur non nulle sur chaque colonne et sur chaque ligne, avec cette valeur égale soit à $+1$ soit à -1. Ainsi, il y a 48 telles matrices pour $n = 3$, par exemple celle-ci

$$g = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Ce groupe est isomorphe au produit semi-direct $(\mathbb{Z}^2)^n \rtimes_\varphi S_n$, où

$$\varphi(\sigma,(k_1,k_2,\ldots,k_n)) := (k_{\sigma^{-1}(1)}, k_{\sigma^{-1}(2)}, \ldots, k_{\sigma^{-1}(n)}).$$

Ici, on considère que $\mathbb{Z}_2 = \{+1,-1\}$ avec la multiplication comme opération. Ainsi, les 48 éléments de $(\mathbb{Z}^2)^3 \rtimes_\varphi S_3$ sont des couples comme $((-1,1,-1),213)$. La bijection, entre ces couples et les matrices décrites plus haut, associe au couple $(\mathbf{k},\sigma)$ la matrice $(a_{ij})_{1\leqslant i,j\leqslant n}$, telle que

$$a_{ij} := \begin{cases} k_j & \text{si } \sigma(j) = i,\\ 0 & \text{sinon.}\end{cases}$$

Le groupe hyperoctaédral correspond aux symétries de l'hyperoctaèdre. Rappelons que **l'hyperoctaèdre** HO_n est l'enveloppe convexe des $2\,n$ points de la forme $(0,\ldots,0,\pm1,0\ldots,0)$, dans $\mathbb{R}^n$. Le groupe B_n agit sur ces points, en permutant les coordonnées et changeant le signe. Ainsi, les sommets de l'octaèdre sont les six points

$$A = (1,0,0),\quad A^- = (-1,0,0),\quad B = (0,1,0),\quad B^- = (0,-1,0),\quad C = (0,0,1),\text{ et } C^- = (0,0,-1).$$

Les sommets portant le même nom (au signe près) sont opposés dans l'octaèdre. Avec l'élément g de B_3 ci-haut, on calcule que

$$g\cdot A = B,\quad g\cdot A^- = B^-,\quad g\cdot B = A^-,\quad g\cdot B^- = A,\quad g\cdot C = C,\text{ et } g\cdot C^- = C^-.$$

On constate donc que les sommets opposés sont envoyés dans des sommets opposés. Bien entendu, c'est toujours le cas pour l'action de B_n sur HO_n.

5.4 Exercices

Exercice 5.1. Montrer que le produit direct de groupes abéliens donne un groupe abélien.

Exercice 5.2. Montrer que le centre $Z(G \times H)$, du produit direct de groupes, coïncide avec le produit direct des centres : $Z(G) \times Z(H)$.

Exercice 5.3. Soient G, H des groupes. Selon l'ordre choisi pour faire le produit cartésien, on obtient deux groupes, $G \times H$ et $H \times G$. Vérifier que l'application $\theta : G \times H \to H \times G$ définie par $\theta(g, h) = (h, g)$ est un isomorphisme.

Exercice 5.4. Soient G, H des groupes abéliens. Alors $G \times H$ est aussi un groupe abélien.

Exercice 5.5. Soit $G_1, \ldots, G_n$ des groupes

(a) Vérifiez que l'opération que nous avons définie en (5.1) sur $G_1 \times \ldots \times G_n$ est associative.

(b) Pour σ une permutation dans S_n. Vérifier que l'application

$$\varphi_\sigma : G_1 \times \ldots \times G_n \to G_{\sigma(1)} \times \ldots \times G_{\sigma(n)}$$

définie par

$$\varphi_\sigma(g_1, \ldots, g_n) = (g_{\sigma(1)}, \ldots, g_{\sigma(n)})$$

est un isomorphisme.

Exercice 5.6. Soit H, K des groupes et $G = H \times K, A = \{e_H\} \times K$ et $B = H \times \{e_K\}$. Vérifiez que $A \lhd G, B \lhd G$, et que G/A est isomorphe à H et G/B isomorphe à K.

Exercice 5.7. Soit G un groupe et $H_i \trianglelefteq G$[3],$i = 1, \ldots, n$ tels que $G = H_1 H_2 \ldots H_n$. Vérifiez que les énoncés suivants sont équivalents :

(a) Pour tout i, $H_i \cap \langle \bigcup_{j \neq i} H_j \rangle = \{e\}$.

(b) Tout élément $g \in G$ s'exprime de façon unique comme un produit d'éléments des H_i, à savoir $g = h_1 h_2 \ldots h_n, h_i \in H_i$.

Exercice 5.8. Soit A un groupe abélien, B un sous-groupe de A, et $\theta : A \to B$ un morphisme tel que $\theta(x) = x$ si $x \in B$ (N.B. ceci n'entraîne pas que θ est une bijection.)

(a) Montrer que si pour $a \in A$ on pose $b = \theta(a^{-1})$, alors $a \cdot b \in \ker(\theta)$.

(b) Montrer que A est produit direct interne de $\ker(\theta)$ et B.

Exercices exploratoires

Exercice 5.9. (Voir Exercice 3.12) On dit d'un sous-ensemble L, du monoïde libre $\mathcal{A}^*$, qu'il est un **langage reconnaissable** s'il existe un morphisme de monoïde $\theta : \mathcal{A}^* \to M$, vers un monoïde fini M,

3. C'est-à-dire que H_i est un sous-groupe normal de G.

et K un sous-ensemble de M tels que $L = \theta^{-1}(K)$. Ici le terme langage est employé de manière tout à fait formelle, les éléments de L sont des mots (sans signification).

(a) Montrer que le complément d'un langage reconnaissable est reconnaissable.

(b) Définir la notion de produit direct de monoïdes, et utiliser cette notion pour montrer que l'intersection de deux langages reconnaissables est un langage reconnaissable.

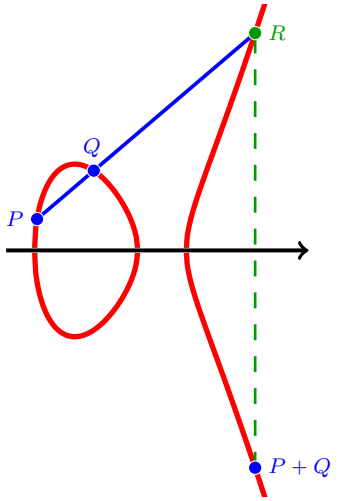
(c) En conclure que l'union de deux langages reconnaissables est un langage reconnaissable.

Exercice 5.10. Montrer que le groupe de transformation du Cube de Rubik se décrit comme (voir Rubik's Cube group)

$$(\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11}) \rtimes ((A_8 \times A_{12}) \rtimes \mathbb{Z}_2).$$

Chapitre 6

Groupes abéliens finis



Un groupe cyclique est abélien, et un produit direct de groupes finis cycliques est donc abélien. En fait, les groupes abéliens finis s'obtiennent tous de cette façon comme l'affirme le théorème suivant.

Théorème 6.1. *Tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques.*

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

6.1 Groupes cycliques

Un groupe G est dit cyclique s'il peut être engendré par un seul élément, c'est-à-dire s'il existe au moins un $g \in G$ tel que $G = \langle g \rangle$. Ainsi, le groupe additif des entiers $(\mathbb{Z}, +)$ peut être engendré par 1, mais n'est pas fini. De même, le groupe additif $(\mathbb{Z}_n, +)$ est cyclique puisqu'il peut être engendré par 1. Le groupe multiplicatif $\{1, -1\}$ est cyclique puisqu'il est engendré par -1. Enfin, groupe multiplicatif μ_n des racines complexes n^e de 1

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

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

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

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

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

Proposition 6.2. *Soient G un groupe et $a \in G$.*

(1) *Si $a^m = e$, alors m est un multiple de* $\mathrm{ord}(a)$.

(2) $\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$.

Démonstration.

(1) Supposons que $\mathrm{ord}(a) = t$, et que $a^m = e$. On peut supposer que $m \geqslant 0$, car $a^{-m} = (a^m)^{-1}$. Faisons la division euclidienne $m = qt + r$, $q, t \in \mathbb{N}, 0 \leqslant r < t$. On obtient $e = a^m = a^{qt+r} = a^{qt}a^r = (a^t)^q a^r = ea^r = a^r$. Ainsi on ne peut avoir $r > 0$ car cela contredirait la minimalité de t. Donc $r = 0$ et m est un multiple de t.

(2) En effet, on a la relation $(x^{-1})^n = x^{-1} \ldots x^{-1} = (x \ldots x)^{-1} = (x^n)^{-1}$. Donc $x^n = e$ si et seulement si $x^{-n} = e$.

6.2 Groupes abéliens primaires

Pour un groupe abélien G, et p un nombre premier qui divise $|G|$, la **composante p-primaire** de G, notée $G(p)$, est définie comme

$$G(p) := \{x \in G \mid \text{il existe } n \in \mathbb{N},\ \mathrm{ord}(x) = p^n\}.$$

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

Proposition 6.3. *Pour p premier, et G un groupe abélien. Alors $G(p)$ est un sous-groupe de G.*

Démonstration. On a $e \in G(p)$ puisque $\mathrm{ord}(e) = 1 = p^0$. D'autre part, si $x \in G(p)$, alors $x^{-1} \in G(p)$ car $\mathrm{ord}(x^{-1}) = \mathrm{ord}(x)$. Pour x et y dans $G(p)$, en vue de montrer que $xy \in G(p)$, on pose $n = n_1 + n_2$, où n_1 et n_2 sont tels que $\mathrm{ord}(x) = p^{n_1}$ et $\mathrm{ord}(y) = p^{n_2}$. On calcule alors que

$$(xy)^{(p^n)} = \underbrace{xy \cdot xy \cdot \ldots \cdot xy}_{p^n \text{ fois}} = \underbrace{xx \ldots x}_{p^n \text{ fois}} \cdot \underbrace{yy \ldots y}_{p^n \text{ fois}} = x^{(p^n)} y^{(p^n)},$$

car G est abélien. Il s'ensuit donc que

$$(xy)^{(p^n)} = x^{(p^n)}y^{(p^n)} = x^{(p^{n_1+n_2})}y^{(p^{n_1+n_2})} = (x^{(p^{n_1})})^{(p^{n_2})}(y^{(p^{n_2})})^{(p^{n_1})} = ee = e.$$

On conclut que p^n est un multiple de $\mathrm{ord}(xy)$, de sorte que $\mathrm{ord}(xy)$ est forcément une puissance de p. ■

Considérons par exemple $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$. On a évidemment $\mathrm{ord}(1) = 6$, $\mathrm{ord}(2) = 3$, $\mathrm{ord}(3) = 2$, $\mathrm{ord}(4) = 3$, $\mathrm{ord}(5) = 6$, et $|G| = 2 \cdot 3$. On constate que $G(2) = \{0,3\}$, $G(3) = \{0,2\}$. D'autre part, pour $\mathbb{Z}_{24} = \{0,1,2,\ldots,24\}$. On a $|G| = 2^3 \cdot 3$. On obtient $G(2) = \{0,3,6,9,12,15,18,21\}$, $G(3) = \{0,8,16\}$. Par définition même, $G(p)$ est constitué de tous les éléments de G dont l'ordre une puissance de p.

Proposition 6.4. *Soit p un nombre premier et G un groupe abélien fini dont tous les éléments sont d'ordre une puissance de p. Alors le cardinal de G est une puissance de p.*

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

Notons que, réciproquement, si $|G| = p^n$ alors tous les éléments de G sont d'ordre une puissance de p. On dit d'un groupe que c'est un **p-groupe** si son cardinal est une puissance de p, un nombre premier. On dit aussi des p-groupes, que ce sont des **groupes primaires**, si on ne désire pas mettre en évidence le rôle du nombre premier p. Ainsi, les groupes $\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_3^n$, et $\mathbb{Z}_3 \times \mathbb{Z}_{27}$ sont des 3-groupes.

6.3 Décomposition primaire

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

Théorème 6.5. *Soit G un groupe abélien fini et $|G| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ où les p_i sont premiers. Alors G est produit direct interne de ses composantes primaires $G(p_i)$, en particulier $G \simeq G(p_1) \times \ldots \times G(p_k)$.*

Par exemple, comme on là déjà vu pour $G = \mathbb{Z}_{30}$, sous une autre forme, on a que

$$G = G(2)\, G(3)\, G(5),$$

c.-à-d. G est produit direct interne des sous-groupes $G(2)$, $G(3)$, et $G(5)$. En préparation de la preuve du théorème, on a besoin de certains résultats préliminaires.

Lemme 6.6. *Soit G un groupe abélien fini, dans lequel on a des éléments $y_1, \ldots, y_n \in G$, respectivement tels que $\mathrm{ord}(y_i) = m_i$, avec les m_i relativement premiers deux à deux. Alors $\mathrm{ord}(y_1 \ldots y_n) = m_1 \ldots m_n$.*

Démonstration. Nous n'allons faire que le cas $n = 2$; le cas général peut se faire par récurrence. Donc disons y_1, y_2 avec $\mathrm{ord}(y_1) = m_1$ et $\mathrm{ord}(y_2) = m_2$. À voir : $\mathrm{ord}(y_1y_2) = m_1m_2$. Il suffit de voir que si $(y_1y_2)^m = e$ alors m est un multiple de m_1m_2. Notons que $\langle y_1\rangle \cap \langle y_2\rangle = \{e\}$; en effet posons $H = \langle y_1\rangle \cap \langle y_2\rangle$, alors H est un sous-groupe de $\langle y_1\rangle$ et $\langle y_2\rangle$, donc $|H|$ divise m_1 et m_2, d'où $|H| = 1$ car m_1 et m_2 sont premiers entre eux. Supposons $(y_1y_2)^m = e$. On a $(y_1y_2)^m = y_1^m y_2^m$ car G est abélien. On obtient $y_1^m = y_2^{-m} \in H$, donc $y_1^m = e$ et $y_2^{-m} = e = y_2^m$. Il s'ensuit que m est un multiple de m_1 et m_2, donc un multiple de m_1m_2, car m_2 et m_2 sont premiers entre eux. ∎

Lemme 6.7. *Soient G un groupe abélien et $H_1, \ldots, H_n$ des sous-groupes de G. Alors*

$$\langle H_1 \cup \ldots \cup H_n\rangle = H_1H_2 \ldots H_n.$$

Démonstration. On a

$$H_1H_2 \ldots H_n = \{g \in G \mid \exists h_i \in H_i, g = h_1h_2 \ldots h_n\}$$

Il est immédiat que chaque élément $h_1h_2 \ldots h_n$, $h_i \in H_i$, appartient à tout sous-groupe de G qui contient $H_1 \cup \ldots \cup H_n$. Il suffit donc de voir que $H_1H_2 \ldots H_n$ forme un sous-groupe de G qui contient $H_1 \cup \ldots \cup H_n$. Or si $h_i \in H_i$, alors $h_i = e \ldots eh_ie \ldots e \in H_1H_2 \ldots H_n$. Donc on a bien $H_1 \cup \ldots \cup H_n \subseteq H_1H_2 \ldots H_n$. Puisque $e \in H_i$, on a $e = e \ldots e \in H_1H_2 \ldots H_n$. Par ailleurs, si $x \in H_1H_2 \ldots H_n$, disons $x = h_1 \ldots h_n$, $h_i \in H_i$, alors $x^{-1} = h_n^{-1} \ldots h_1^{-1} = h_1^{-1} \ldots h_n^{-1}$, car G est abélien, et comme $h_i^{-1} \in H_i$ on a bien $x^{-1} \in H_1H_2 \ldots H_n$. Finalement, si $x, y \in H_1H_2 \ldots H_n$, disons $x = a_1 \ldots a_n$, $a_i \in H_i$, $y = b_1 \ldots b_n$, $b_i \in H_i$, alors $xy = a_1 \ldots a_nb_1 \ldots b_n = a_1b_1 \ldots a_ib_i \ldots a_nb_n$, car G est abélien, et $a_ib_i \in H_i$, de sorte que $xy \in H_1H_2 \ldots H_n$. ∎

Démonstration du théorème 6.5. On a déjà vu que les $G(p_i)$ sont des sous-groupes normaux. Par le lemme précédent, on a

$$\left\langle \bigcup_{1 \leqslant i \neq j \leqslant k} G(p_j) \right\rangle = \prod_{i \neq j}^{n} G(p_j).$$

Reste donc à voir que $G(p_i) \cap \prod_{i\neq j}^n G(p_j) = \{e\}$, puis que $G = G(p_1) \ldots G(p_k)$. À cette fin, soit $x \in G(p_i) \cap \prod_{i\neq j}^n G(p_j)$. D'une part, comme $x \in G(p_i)$, on a que $\mathrm{ord}(x) = p_i^{t_i}$ pour un certain $t_i \leqslant \alpha_i$. D'autre part, on peut écrire x comme un produit

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

avec les $x_j \in G(p_j)$, et donc ayant $\mathrm{ord}(x_j) = p^{t_j}$, pour certains $t_j \leqslant \alpha_j$. Par un des lemmes ci-dessus on a

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

Puisque les p_i sont premiers deux à deux, la seule façon de réconcilier ces énoncés est que $t_i = 0$ et $t_j = 0$, pour tout j. On conclut donc que $x = e$.

Maintenant, pour $x \in G$, on cherche à construire des $x_i \in G(p_i)$ tels on a $x = x_1 x_2 \cdots x_k$. Pour ce faire, rappelons que $\mathrm{ord}(x)$ divise $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, et donc

$$\mathrm{ord}(x) = n = p_1^{t_1} \dots p_k^{t_k}, \qquad \text{pour} \qquad 0 \leqslant t_i \leqslant \alpha_i.$$

Ainsi, si on pose $n_i := n/p_i^{t_i}$, on a que $\mathrm{pgcd}(n_1, \dots, n_k) = 1$. Il existe donc des entiers λ_i tels que

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

Il s'ensuit que

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

Mais alors, par définition de n_i,

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

on trouve donc l'expression désirée en posant $x_i := x^{\lambda_i n_i}$, qui est bien dans $G(p_i)$ par l'égalité ci-dessus. Ceci achève la démonstration. ∎

Corollaire 6.8. *Soit G comme ci-dessus, $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Alors $|G(p_i)| = p_i^{\alpha_i}$.*

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

Le théorème précédent ramène l'étude de la structure des groupes abéliens finis, à celle des groupes abéliens finis primaires. Le théorème suivant décrit entièrement la structure de ceux-ci.

Théorème 6.9. *Tout p-groupe abélien fini est produit direct interne de groupes cycliques.*

Démonstration. Soit p premier. On procède par récurrence sur l'ordre des p-groupes abéliens finis. Soit G un p-groupe abélien fini, disons $|G| = p^n$. Si $|G| = p$; mais alors $G \simeq \mathbb{Z}_p$ et on a fini. Sinon, on a $|G| = p^n$, avec $n \geqslant 2$. Notons que $G = G(p)$. Soit $a \in G$ d'ordre maximal, disons $\mathrm{ord}(a) = p^m$ avec $m \geqslant 1$. Par définition de m, on a évidemment $\mathrm{ord}(g) = p^\alpha$ avec $\alpha \leqslant m$, pour tout $g \in G$. Il s'ensuit que $g^{p^m} = e$. Si $\mathrm{ord}(a) = p^n$, alors $G = \langle a \rangle$ et on a terminé. Sinon, on a $\langle a \rangle \subset G$; et le groupe abélien fini $\overline{G} := G/\langle a \rangle$ est d'ordre

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

L'hypothèse de récurrence s'applique donc, et $\overline{G}$ est produit direct interne de sous-groupes cycliques, nommons-les $\overline{G_i} \leqslant \overline{G}$. Posant $H = \langle a \rangle$, on a $\overline{G_i} = \langle \beta_i \rangle$ pour certains $\beta_i = b_i H$, et $|\overline{G_i}| = \mathrm{ord}(\beta_i) = p^{m_i}$. Pour tout $b \in G$, posant $\beta = bH$, on a $\beta = \beta_1^{k_1} \dots \beta_r^{k_r}$, pour certains entiers k_i, et alors

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

En particulier,

$$b = b_1^{k_1} \dots b_r^{k_r} a^k,$$

pour une certaine puissance k de a. Si on pose $K_i = \langle b_i \rangle$, on a donc

$$G = K_1 K_2 \dots K_r H,$$

(presque) comme voulu. Malheureusement, rien n'assure qu'on ait là un produit direct interne. Exploitant le fait que $b_i a^{n_i} H = b_i H$, nous allons trouver des « ajustements » $a^{n_1}, \dots, a^{n_r}$ de façon à rendre le produit ci-haut un produit direct interne.

Puisque (par définition) $\beta_i^{(p^{m_i})} = e$, ou encore $b_i^{(p^{m_i})} H = H$, on a $b_i^{(p^{m_i})} \in H$. C'est donc dire que $b_i^{(p^{m_i})} = a^{s_i}$, pour certains s_i, et donc

$$(b_i^{(p^{m_i})})^{(p^{m-m_i})} = (a^{s_i})^{p^{m-m_i}}, \qquad \text{c.-à-d.} \qquad b_i^{(p^m)} = (a^{(p^{m-m_i})})^{s_i} = e$$

Mais alors,

$$\operatorname{ord}(a^{(p^{m-m_i})}) = p^{m_i},$$

car $\operatorname{ord}(a) = p^m$. Il s'ensuit donc que s_i est un multiple de p^{m_i}, disons $s_i = t_i p^{m_i}$. On trouve ainsi que

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

Nous allons constater qu'on peut maintenant corriger les b_i, en posant $b_i' = b_i a^{-t_i}$, et $H_i := \langle b_i' \rangle$. Observons que l'on conserve $b_i' H = \beta_i$, et donc on a bien

$$G = H_1 \dots H_r H,$$

comme auparavant. Reste plus qu'à vérifier que G est bien un produit direct interne de $H_1, \dots, H_r, H_{r+1}$, écrivant $H_{r+1} = H$ pour simplifier la présentation. il s'agit de voir que

$$\bigcap_{i=1}^{r+1} H_i = \{e\}.$$

Autrement dit, pour $x \in H_i \cap \prod_{j \neq i} H_j$, on doit montrer que $x = e$. Autrement dit, on peut écrire x sous la forme $x = x_1 \dots \widehat{x_i} \dots x_{r+1}$, sachant que $x \in H_i$ et que les $x_j \in H_j$ lorsque $j \neq i$. Désignons par γ_j les classes $x_j H$, pour j allant de 1 à $r+1$, et par γ la classe xH. Les identités ci-dessus se traduisent alors en identités pour γ et les γ_i :

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

dans le groupe quotient $\overline{G}$, avec $\gamma \in \overline{G_i}$, et les $\gamma_j \in \overline{G_j}$, pour $i \neq j$. En particulier, on a $\gamma_{r+1} = e$, puisque $H_{r+1} = H$. Encore une fois, on utilise l'hypothèse de récurrence qui s'applique à $\overline{G}$ pour conclure que $\gamma = e$, et $\gamma_j = e$, car on a un produit direct interne pour $\overline{G}$. Autrement dit,

$$x \in H, \qquad \text{et} \qquad x_j \in H$$

Il ne suffit donc plus que de voir que $H \cap H_i = \{e\}$, pour tout $i = 1, \ldots, r$. Écrivant n_i pour $\mathrm{ord}(b'_i)$, on a

$$\beta_i^{n_i} = b'_i H^{n_i} = b_i'^{n_i} H = eH = e,$$

de sorte que n_i est un multiple de $\mathrm{ord}(\beta_i) = p^{m_i}$. Mais $(b'_i)^{(p^{m_i})} = e$, donc p^{m_i} est un multiple de $\mathrm{ord}(b'_i)$. D'où l'égalité $\mathrm{ord}(b'_i) = p^{m_i} = \mathrm{ord}(\beta_i)$ [1]. Considérant ensuite $x \in H \cap H_i$, avec $x = b_i'^k$, $k < p^{m_i}$. On trouve $xH = e$, et $xH = b_i'^k H = (b'_i H)^k = \beta_i^k$. La seule possibilité est donc $k = 0$, car $p^{m_i} = \mathrm{ord}(\beta_i)$. D'où $x = e$, tel que voulu. ■

6.4 Théorème principal

Théorème 6.10. *Tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques. Plus précisément, il est produit direct interne de sous-groupes cycliques.*

Démonstration. Découle des deux théorèmes précédents. ■

Notons qu'on n'a pas une unicité directe : par exemple le groupe cyclique $\mathbb{Z}_6$ est aussi isomorphe au produit direct $\mathbb{Z}_2 \times \mathbb{Z}_3$. Par contre, on peut noter que la décomposition d'un groupe abélien en produit direct interne de ses composantes primaires est unique puisque les composantes primaires sont complètement déterminées. D'autre part on a le résultat suivant.

Proposition 6.11. *La décomposition d'un p-groupe abélien fini en produit direct de groupes cycliques est unique au sens suivant. Soit G un p-groupe abélien fini et G_i, H_i des p-groupes cycliques tels que*

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

et

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

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

Démonstration. ■

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

Théorème 6.12. *Tout groupe abélien fini possède une décomposition en produit direct interne de sous-groupes cycliques primaires, et cette décomposition est unique au sens où deux telles décompositions comportent le même nombre de facteurs de chaque ordre.*

1. C'était le but de l'ajustement.

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

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

Une conséquence de l'unicité dans le théorème précédent est que tout p-groupe abélien fini qui est cyclique est **indécomposable**, c'est-à-dire qu'il ne peut pas être représenté comme produit direct de groupes plus petits. Une autre conséquence est qu'on peut produire la liste exacte (à isomorphisme près) de tous les groupes abéliens finis d'un cardinal donné. Par exemple, les seuls groupes abéliens finis d'ordre 8 sont (à isomorphisme près) l'un des trois suivants

$$\mathbb{Z}_8, \qquad \mathbb{Z}_2 \times \mathbb{Z}_4, \qquad \text{et} \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

De façon similaire, pour $180 = 2^2 \cdot 3^2 \cdot 5$, on trouve de décomposition ne pouvant contenir que des 2-groupes de cardinal 2 ou 4, des 3-groupes de cardinal 3 ou 9, et des 5-groupes de cardinal 5. Les possibilités sont donc

$$\begin{aligned}
&\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5, \\
&\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5, \\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5.
\end{aligned}$$

On ne trouve donc que 4 tels groupes. En y réfléchissant correctement, on peut trouver une formule qui donne (toujours à isomorphisme près) le nombre de groupes abéliens finis d'un cardinal donné n.

6.5 Exercices

Exercice 6.1. Désignons par $\mathrm{ord}(z)$ l'ordre de l'élément z dans un groupe donné. Donnez un contre-exemple pour vérifier que la relation $\mathrm{ord}(xy) = \mathrm{ppcm}(\mathrm{ord}(x), \mathrm{ord}(y))$ n'est pas valide en général.

Exercice 6.2. Montrer que dans un groupe abélien fini A, il existe pour tout diviseur d de $|A|$, un sous-groupe d'ordre d. (N.B. C'est en quelque sorte une réciproque du théorème de Lagrange pour les groupes abéliens.)

Exercice 6.3. Soit $n > 1$ un entier qui n'est pas divisible par le carré d'un autre entier plus grand que 1. Montrez alors que tout groupe abélien fini d'ordre n est cyclique.

Exercice 6.4. Énumérer tous les groupes abéliens d'ordre 72, à isomorphisme près.

Exercice 6.5. Les groupes $\mathbb{Z}_{12} \times \mathbb{Z}_{72}$ et $\mathbb{Z}_{18} \times \mathbb{Z}_{48}$ sont-ils isomorphes ?

Exercice 6.6. Soit G un groupe abélien, $H_1, \dots, H_n$ des sous-groupes, et $H = H_1 H_2 \cdots H_n$.

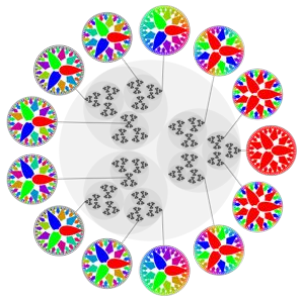
(a) Montrer que $H \leqslant G$.

(b) Montrer que H est le plus petit sous-groupe de G qui contienne $H_1 \cup \cdots \cup H_n$.

Exercice 6.7. Faire la liste de tous les groupes abéliens finis d'ordre 252, à isomorphisme près. Justifier.

Chapitre 7

Les p-groupes, et théorèmes de Sylow



Les théorèmes de Sylow[1] permettent de prédire l'existence de certains sous-groupes dans un groupe fini, seulement en considérant le cardinal du groupe.

7.1 Les p-groupes

Un p-groupe fini est un groupe fini qui possède p^n éléments pour un certain n, avec p est un nombre premier.

Proposition 7.1. *Tout p-groupe fini possède un centre non trivial.*

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

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

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

$$p^n = |C(G)| + p\,t$$

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

1. Ludwig Sylow, (1832-1918).

7.2 Théorèmes de Sylow

Plusieurs des notions et résultats précédents permettent de caractériser les sous-groupes d'un groupe fini donné. En particulier, on a vu que l'ordre d'un sous-groupe doit diviser l'ordre du groupe, ce qui réduit considérablement les possibilités. Cependant, cette contrainte n'est pas suffisante en général[2] pour caractériser l'ordre possible des sous-groupes. Par exemple, pour le groupe alterné A_4 d'ordre $12 = 2 \cdot 6$, on n'a pas de sous-groupe d'ordre 6 (voir l'exercice 2.2). Nous allons chercher à déterminer (en partie) quand un groupe donné admet un sous-groupe d'ordre d, pour d divisant son ordre. En toute généralité, cette question est peut-être trop difficile. Cependant, en la restreignant au cas où $d = p^n$, avec p premier, on a les résultats remarquables de Sylow. Afin de les énoncer, on se donne la définition suivante. Pour un groupe fini G d'ordre $|G| = p^n m$, avec p premier ne divisant pas m, on dit qu'un sous-groupe de G est de **Sylow** si son ordre est p^n. Autrement dit, c'est un p-sous-groupe d'ordre le plus grand possible.

Théorème 7.2 (Premier théorème de Sylow)**.** *Soit G un groupe fini d'ordre $|G| = k$. Alors, pour tout nombre premier p divisant k, le groupe G possède un sous-groupe d'ordre p^s pour toute puissance s de p, telle que p^s divise k. En particulier, G contiens un p-sous-groupe de Sylow.*

Théorème 7.3 (Deuxième théorème de Sylow)**.** *Soit G un groupe fini. Pour chaque diviseur premier p de $|G|$, les p-sous-groupes de Sylow sont conjugués.*

Théorème 7.4 (Troisième théorème de Sylow)**.** *Soit G un groupe fini, et p un diviseur premier de $|G|$. Soit N_p le nombre de p-sous-groupe de Sylow de G. Alors $N_p = [G : N(S)]$, où S est n'importe quel p-sous-groupe de Sylow, et $N_p \equiv 1 \pmod{p}$.*

Nous n'allons démontrer que les deux premiers théorèmes de Sylow. Pour le premier, on procède par récurrence sur l'ordre du groupe $|G| = p^n m$, et on utilise le cas particulier connu d'un sous-groupe d'ordre p pour les groupes abéliens.

Démonstration du théorème 7.2. On suppose que $|G| > 1$. Considérons l'action de G sur lui-même par conjugaison, et soit $G = \mathrm{Orb}(x_1) + \ldots + \mathrm{Orb}(x_r)$ la partition de G en orbites, avec les orbites ordonnées en ordre croissant de cardinalité. Considérons la relation déjà vue

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

On distingue deux cas. Premièrement, p ne divise pas $|Z(G)|$. Alors p ne divise pas $[G : C(x_i)]$ pour un certain i. D'où p^s divise $|C(x_i)|$, puisque $|G| = [G : C(x_i)] \cdot |C(x_i)|$, et on a aussi $|C(x_i)| < |G|$, car $x_i \notin Z(G)$. Par récurrence, $C(x_i)$ possède un sous-groupe H d'ordre p^s, qui est en même temps un

2. Bien qu'elle le soit pour les groupes abéliens. Voir l'exercice 6.2.

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

Démonstration du théorème 7.3. Fixons un p-sous-groupe de Sylow S, avec G d'ordre $p^n\, m$, et considérons un autre p-sous-groupe de Sylow S'. Rappelons qu'on désigne par G/S l'ensemble des translatés de S, et qu'alors $|G/S| = m$ avec le groupe G agissant transitivement, par translation, sur G/S. On a donc aussi une action par translation (pas nécessairement transitive) de S' sur G/S, obtenue par restriction de l'action de G aux éléments de S'. On obtient donc

$$|G/S| = \sum_i [S' : \mathrm{Stab}_{S'}(T_i)]$$

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

Quelques remarques s'imposent sur ces théorèmes de Sylow. Si p est un facteur premier de $|G|$, alors G possède au moins un p-sous-groupe de Sylow, avec N_p divisant $|G|$ et $N_p \equiv 1 \bmod (p)$. Les p-sous-groupes de Sylow forment une orbite pour l'action de G sur $\mathcal{P}(G)$ par conjugaison et N_p est le cardinal de cette orbite qui est égale à $[G : N(S)]$. Un groupe fini G possède un seul p-sous-groupe de Sylow si et seulement si il possède un p-sous-groupe de Sylow qui soit un sous-groupe normal. Si $N_{p,s}$ désigne le nombre de sous-groupes d'ordre p^s, alors on peut montrer que $N_{p,s} \equiv 1 \bmod (p)$.

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

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

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

Exemple. Tout groupe d'ordre 30 possède au moins un sous-groupe normal propre. En effet, il suffit de voir qu'au moins un parmi N_2, N_3, N_5 vaut 1. On a déjà vu que $N_2 = 1$ ou 3 ou 5 ou 15, $N_3 = 1$ ou 10, $N_5 = 1$ ou 6. Montrons que $N_3 = 1$ ou $N_5 = 1$. Sinon, on aurait $N_3 = 10$ et $N_5 = 6$. Disons

$K_1, \ldots, K_{10}$ les 3-sous-groupes de Sylow, d'ordre 3, et $H_1, \ldots, H_6$ les 5-sous-groupes de Sylow, d'ordre 5. Puisqu'une intersection $H_i \cap H_j$ est un sous-groupe de H_i et H_j et que son ordre est un facteur de 5, on a $H_i \cap H_j = \{e\}$ si $i \neq j$. De façon semblable $K_i \cap K_j = \{e\}$ si $i \neq j$. Les H_i fourniraient donc au moins 24 éléments différents de e et les K_i au moins 20, ce qui donneraient au moins 44 éléments différents dans G, ce qui est absurde. Donc on doit avoir $N_3 = 1$ ou $N_5 = 1$, tel que voulu.

Proposition 7.5. *Soit G un groupe fini et H, K des sous-groupes de G. Alors on a la relation*

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

Démonstration. Déjà vu dans un exercice. ■

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

7.3 Exercices

Exercice 7.1. En s'appuyant sur le fait que tout p-groupe possède un centre qui ne se réduit pas à l'élément identité, démontrez que tout groupe d'ordre p^2 est abélien. (Aide : passez à un groupe quotient.)

Exercice 7.2. Soit p un nombre premier et G l'ensemble suivant de matrices à coefficients dans le corps $\mathbb{Z}_p$ des entiers modulo p

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$$

(a) Vérifier que G est un sous-groupe de $GL_3(\mathbb{Z}_p$, qu'il a p^3 éléments, et qu'il n'est pas abélien.

(b) Vérifier que le centre de G est formé des matrices suivantes

$$C(G) = \left\{ \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : t \in \mathbb{Z}_p \right\}$$

Exercice 7.3. Montrez que tout groupe d'ordre 96 possède au moins un sous-groupe normal propre.

Exercice 7.4. Soient A et B deux sous-groupes d'un groupe G. On considère l'action de B sur $\mathcal{P}(G)$ par translation à gauche. Montrez que $\mathrm{Stab}_B(A) = A \cap B$.

Exercice 7.5. Soit G un groupe fini opérant sur un ensemble E. Montrez que si G n'est pas isomorphe au groupe additif $\mathbb{Z}_2$ et que E possède un élément dont l'orbite possède exactement deux éléments, alors G possède au moins un sous-groupe normal propre.

Exercice 7.6. Si un groupe d'ordre 104 ne contient pas de sous-groupe normal d'ordre 8, combien a-t-il de sous-groupes d'ordre 8 ?

Exercice 7.7. Soit G un groupe fini et $T \lhd G$. Soit p un nombre premier et supposons que p ne divise pas $[G : T]$. Montrez que T contient tous les p-sous-groupes de Sylow de G.

Exercice 7.8. Soit p un nombre premier.

(a) Montrer que dans un groupe d'ordre $4p$, un p-sous-groupe de Sylow est toujours normal si $p \geqslant 5$.

(b) Est-ce vrai pour $p = 3$? Justifier.

Exercice 7.9. Montrer que tous les groupes d'ordre plus petit que 60 possède au moins un sous-groupe normal propre, sauf les groupes dont l'ordre est un nombre premier.

Exercice 7.10.

(a) Montrer que tout groupe d'ordre 20 possède au moins un sous-groupe normal propre.

(b) Vérifier que l'opération de $\mathbb{R}^* \times \mathbb{C}$ dans $\mathbb{C}$ définie par $r \cdot z = rz$ constitue une action du groupe multiplicatif $\mathbb{R}^*$ sur l'ensemble des nombres complexes $\mathbb{C}$. Pour chaque $z \in \mathbb{C}$ calculer $\mathrm{Stab}(z)$ et décrire géométriquement $\mathrm{Orb}(z)$ dans le plan complexe.

(c) Vérifier que le groupe des isométries de l'icosaèdre possède un sous-groupe d'ordre 2 qui est normal.

Exercices exploratoires

Exercice 7.11. Soit G un groupe fini, et soit p le plus petit diviseur premier de $|G|$. Supposons que G possède un sous-groupe H tel que $[G : H] = p$. Le but est de montrer que $H \lhd G$. Rappelons que (voir (2.8)) G opère par translation à gauche sur l'ensemble $E := G/H = \{H, x_1H, \ldots, x_{p-1}H\}$, et qu'il s'ensuit (voir Proposition 2.14) qu'on a un morphisme de groupes $\varphi : G \to S_E$.

(a) Montrer que $\ker(\varphi) \subseteq H$.

(b) Soit $K := \{f \in S_E : f(H) = H\}$. Montrer que K est un sous-groupe de S_E et que $|K| = (p-1)!$.

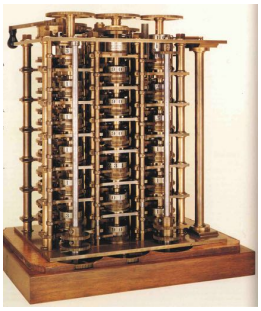
(c) Soit $L = \{\varphi(h) : h \in H\}$ l'image de H par φ. Vérifier que L est un sous-groupe de K et en déduire que $|L|$ divise $(p-1)!$. En particulier, $|L|$ est relativement premier à p.

(d) Montrer que $|L|$ divise $|H|$.

(e) En déduire que $|L| = 1$, et que $H = \ker(\varphi)$. Conclure que $H \lhd G$.

Annexe A

Théorie des groupes avec le calcul formel



Pour se familiariser avec des notions mathématiques, le calcul formel est des plus efficace. L'idée est de rester le plus près possible de la présentation mathématique, et d'utiliser l'ordinateur comme un outil de manipulation d'objets mathématiques abstraits. Bien que nous n'allons montrer dans ce chapitre comment le faire qu'avec le système de calcul Maple, plusieurs autres outils sont accessibles. Le système « open source » Sage est un bon exemple, et on accède au tutoriel qui montre la façon d'utiliser Sage pour la théorie des groupes à l'endroit suivant doc.sagemath.org.

Comme la grande majorité des systèmes de calcul formel, Maple est un système interactif fonctionnant sous le mode « question/instruction–réponse/résultat ». Une introduction générale à Maple est disponible dans le texte Calcul formel (avec Maple) (F. Bergeron 2014). En mode d'intercation classique (worksheet mode), un symbol « > » indique que le système est prêt à recevoir une instruction. Pour avoir accès aux outils de manipulation de groupes, on donne l'instruction suivante (qui se termine par « : » pour signifier qu'on ne s'attend pas à une réponse).

```
> with(GroupTheory) :
```

On peut obtenir de l'aide sur les outils alors rendu disponible avec l'instruction :

```
> ?GroupTheory
```

On peut construire des groupes classiques (groupe alterné, groupe diédral, groupe général linéaire, groupe de permutations, etc.), en trouver des propriétés (ordre, transitivité, primitivitée, calculer le treillis des sous-groupes). On peut construire de nouveaux groupes à partir de groupes donnés (produit direct), trouver tous les groupes d'un certain ordre, etc. Par exemple, on peut définir le groupe alterné, trouver son ordre, et vérifier s'il est transitif de la façon suivante :

```
> G :=AlternatingGroup(7)) :
```

G=**A**[7]

> GroupOrder(G) ;

2520

> IsTransitiveG ;

true

Pour obtenir la suite dont les termes donnent le nombre de groupes de « petite » cardinalité, on fait comme suit :

> [seq(nops(AllSmallGroups(k)),k=1..32)] ;

[1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, 5, 1, 2, 1, 14, 1, 5, 1, 5, 2, 2, 1, 15, 2, 2, 5, 4, 1, 4, 1, 51]

Ces groupes peuvent être décrits de plusieurs façon, par défaut ils sont présentés comme sous-groupes d'un certain S_n, avec leur générateurs écrits en notation cyclique. Ainsi, on obtient

> AllSmallGroups(8) :map(print,%) :

$$\langle\ (1,2,4,6,8,7,5,3)\ \rangle$$
$$\langle\ (1,2,5,3)(4,6,8,7),\ (1,4)(2,6)(3,7)(5,8)\ \rangle$$
$$\langle\ (1,2)(3,7)(4,6)(5,8),\ (1,3)(2,5)(4,8)(6,7),\ (1,4)(2,6)(3,8)(5,7)\ \rangle$$
$$\langle\ (1,2,6,3)(4,8,5,7),\ (1,4,6,5)(2,7,3,8),\ (1,6)(2,3)(4,5)(7,8)\ \rangle$$
$$\langle\ (1,2)(3,5)(4,6)(7,8),\ (1,3)(2,5)(4,7)(6,8),\ (1,4)(2,6)(3,7)(5,8)\ \rangle$$

Pour les groupes de permutations, comme le groupe du cube de Rubic :

> RubiksCubeGroup() ;

$$\begin{aligned} G\ :=\ \langle\ & (6,25,43,16)(7,28,42,13)(8,30,41,11)(17,19,24,22)(18,21,23,20),\\ & (1,14,48,27)(2,12,47,29)(3,9,46,32)(33,35,40,38)(34,37,39,36),\\ & (1,17,41,40)(4,20,44,37)(6,22,46,35)(9,11,16,14)(10,13,15,12),\\ & (3,38,43,19)(5,36,45,21)(8,33,48,24)(25,27,32,30)(26,29,31,28),\\ & (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19),\\ & (14,22,30,38)(15,23,31,39)(16,24,32,40)(41,43,48,46)(42,45,47,44)\ \rangle \end{aligned}$$

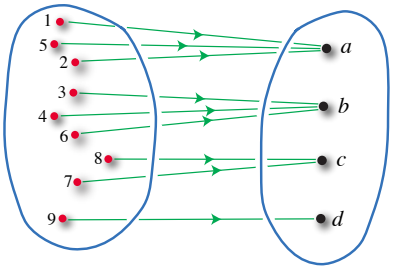
on peut calculer le stabilisateur et l'orbites d'éléments. Le groupe général linéaire, sur un corps fini à q éléments, correspond à $GL(n,q)$. Son ordre dépend de q de manière polynomiale, et on obtient son ordre comme suit :

> GroupOrder(GL(3, q)) ;

$$\left(q^6-1\right)\left(q^6-q\right)\left(q^6-q^2\right)\left(q^6-q^3\right)\left(q^6-q^4\right)\left(q^6-q^5\right)$$

Annexe B

Rappels sur les ensembles et fonctions



La théorie des ensembles a été introduite par Georg Cantor. On peut en donner une axiomatique rigoureuse qui n'est pas discutée ici. Un **ensemble** est une collection d'objets. La théorie suppose que les ensembles contiennent des **éléments**, et on écrit $a \in A$ pour dire que « a est un élément de A » ou que « a appartient à A ». Si a n'est pas un élément de A, on écrit $a \notin A$ et on lit « a n'appartient pas à A » ou « a n'est pas dans A ». L'appartenance (ou pas) à un ensemble doit être claire. Autrement dit, cette appartenance ne doit pas être question de point de vue, on d'interprétation. Comme pour tout concept mathématique, il est important de bien comprendre quand deux ensembles sont égaux. La règle est toute simple (mais on l'oublie parfois) :

« Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments. »

Autrement dit, pour « connaître » un ensemble il faut savoir dire quels en sont les éléments.

Deux façons typiques de décrire un ensemble consistent à : soit, donner la liste de tous ses éléments (quand il n'en contient pas trop), soit via la description d'une propriété qui caractérise ses éléments. L'écriture $E = \{x_1, x_2, ..., x_m\}$ signifie donc que E est composé des éléments $x_1, x_2, \ldots, x_m$; il peut y avoir des répétitions d'éléments : par exemple, $\{a, b, a\}$ représente le même ensemble que $\{a, b\}$. On a donc les présentations équivalentes

$$\{a, b, c\} = \{c, a, b\} = \{a, b, a, b, c, a, b, a\},$$

d'un même ensemble qui contient les trois éléments : a, b et c. L'ordre dans lequel on écrit les éléments n'importe pas : par exemple, $\{b, a\}$ représente le même ensemble que $\{a, b\}$. Fréquemment, on se donne une propriété P pour définir un ensemble. On écrit $A = \{x \in E \,|\, x \text{ possède } P\}$ pour dire que A est l'ensemble des éléments de E qui possèdent la propriété P. Pour montrer qu'un élément x de E est en fait dans A, il suffira donc de montrer que x a la propriété P.

Typiquement, on commence par considérer des ensembles de base comme

$$\begin{aligned}
\mathcal{A} &:= \{a, b, c, d, \ \ldots\ , z\},\\
\mathbb{N} &:= \{0, 1, 2, 3, \ \ldots\ \},\\
\mathbb{Z} &:= \{\ldots\ , -3, -2, -1, 0, 1, 2, 3, \ \ldots\ \},\\
\mathbb{Q} &:= \{a/b \mid a \in \mathbb{Z}, \quad b \in \mathbb{N}, \text{ et } b \neq 0\ \},\\
\mathbb{C} &:= \{x + i\,y \mid x, y \in \mathbb{R}\},
\end{aligned}$$

où $\mathbb{R}$ désigne l'ensemble ds **nombres réels**, ou encore des ensembles d'objets divers comme

$$\{\bullet, \bullet, \bullet\}, \qquad \text{ou} \qquad \{\clubsuit,\ \diamondsuit,\ \heartsuit,\ \spadesuit\}.$$

L'ensemble qui ne contient aucun élément est, par définition, l'ensemble **vide**, et on le représente par le symbole $\varnothing$. Un **singleton** est un ensemble à un élément. Si $a \neq b$, alors on dit de l'ensemble $\{a, b\}$ que c'est une **paire**. Rappelons que $\{a, b\} = \{b, a\}$, et que $\{a, a\} = \{a\}$ n'est pas une paire.

Remarque. Il a été historiquement bien établi que l'imprécision de la définition d'un ensemble peut engendrer des paradoxes (voir par exemple le paradoxe de Bertrand Russell (1872-1970) dans tout bon livre de logique). Pour éviter cela, nous ne travaillerons qu'avec un petit nombre d'ensembles bien étudiés et stables. Tous les ensembles considérés s'obtiennent à partir de l'ensemble vide et d'axiomes de construction d'ensembles.

Un ensemble E est **fini** si on peut écrire $E = \{x_1, \ldots, x_n\}$, avec $n \in \mathbb{N}$ fixé. Si les éléments x_i sont tous distincts, alors on dit que l'entier n est le **cardinal** de E et on le note : $n = |E|$. Par convention $|\varnothing| = 0$. Un ensemble E est **infini** s'il n'est pas fini. Par exemple, $\{1, 3, 6, 7, 8, 9, 10, 34\}$ est fini, mais $\mathbb{N}$ ne l'est pas. On dit que A est un **sous-ensemble** de E, si tous les éléments de A appartiennent à E. On dit aussi que A est **contenu** dans E et on écrit $A \subseteq E$. C'est la relation **d'inclusion**. Les ensembles $\varnothing$ et E sont des sous-ensembles particuliers de E. Tout autre sous-ensemble de E est un **sous-ensemble propre**. Si A n'est pas un sous-ensemble de E, on écrit $A \nsubseteq E$. Par exemple, on a $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Ce qui signifie que $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$, etc., mais aussi que $\mathbb{N} \subseteq \mathbb{Q}$. On dit que l'inclusion est **transitive**. Il est clair que tout sous-ensemble d'un ensemble fini est fini.

On note $\mathcal{P}(E)$ l'ensemble des sous-ensembles de l'ensemble E :

$$\mathcal{P}(E) = \{A \mid A \subseteq E\}.$$

Par exemple, pour $E = \{1, 2, 3\}$, on a $\mathcal{P}(E) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, E\}$. Si $|E| = n$, alors $|\mathcal{P}(E)| = 2^n$. Pour montrer qu'un ensemble A est inclus dans un ensemble E, on doit montrer qu'un élément quelconque de A est forcément aussi un élément de E. Autrement dit que : $x \in A \Rightarrow x \in E$. Montrer que $A = E$ équivaut à montrer que $A \subseteq E$ et $E \subseteq A$. La **différence** de deux ensembles A et B, notée $A \backslash B$, est l'ensemble défini par

$$A \backslash B = \{x \in A \mid x \notin B\}.$$

Si le contexte fait en sorte que l'ensemble E est clair, et si $A \subseteq E$, alors on écrit parfois $A^c := E \backslash A$. On dit que A^c est le **complément** de A (dans E). Dans le cas d'un ensemble de nombres E, qui contient 0, on écrit souvent E^* pour l'ensemble $E \backslash \{0\}$.

Deux **couples** (a, b) et (a', b') sont égaux, si et seulement si $a = a'$ et $b = b'$. On admet le cas $a = b$, pour obtenir le couple (a, a). Soulignons que l'ordre gauche droite est important, c.-à-d. $(a, b) \neq (b, a)$ sauf si $a = b$. Pour deux ensembles A et B, le **produit cartésien** de A et B est l'ensemble

$$A \times B = \{(a, b) \,|\, a \in A, b \in B\}.$$

On observe que $\varnothing \times E = E \times \varnothing = \varnothing$. En effet, il n'existe pas de couple (a, b) tel que $a \in E$ et $b \in \varnothing$. En général $A \times B \neq B \times A$. Le cardinal de $A \times B$ est le produit du cardinal de A et du cardinal de B. Par exemple, le plan cartésien est $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Pour $n \in \mathbb{N}$, et E est un ensemble, le produit cartésien n fois de E est l'ensemble défini par récurrence

$$E^n = E \times E^{n-1},$$

avec $E^0 := \{E\}$ (c'est un singleton, un ensemble à un seul élément), dont les éléments sont appelés **n-uplets**. On écrit d'habitude

$$x = (x_1, x_2, \ldots, x_n), \qquad \text{où} \qquad x_i \in E,$$

pour un élément de E^n, et alors l'unique élément de E^0 s'écrit $x = (\,)$. Il est facile de voir qu'il y a une bijection (naturelle) entre $E^n \times E^k$ et E^{n+k} ; mais, à strictement parler, ces deux ensembles ne sont pas « égaux ». En effet, les éléments du premier ensemble sont de la forme

$$((x_1, \ldots, k_k), (y_1, \ldots, y_n)),$$

tandis que ceux du deuxième sont de la forme (très similaire, mais différente)

$$(x_1, \ldots, k_k, y_1, \ldots, y_n).$$

Il est souvent « correct » de les identifier, mais il faut parfois faire attention. On peut donner un sens mathématique précis à au terme « naturel », mais intuitivement cela signifie que la notion s'impose. Pour tout ensemble E et tout singleton $\{\star\}$, on a aussi une bijection naturelle

$$\eta : E \longrightarrow E \times \{\star\}, \qquad \text{avec} \qquad \eta(x) := (x, \star).$$

L'union, de deux ensembles A et B, est l'ensemble formé de tous les éléments qui appartiennent à A **ou** à B (ou aux deux). On le note $A \cup B$, et donc

$$A \cup B := \{x \,|\, x \in A \text{ ou } x \in B\}.$$

L'intersection de deux ensembles A et B l'ensemble des éléments communs à A **et** B. On le note $A \cap B$ et donc

$$A \cap B = \{x \,|\, x \in A \text{ et } x \in B\}.$$

Pour tout A et B, on a l'inclusion $A \subseteq A \cup B$. De plus, $A \cap B$ est un sous-ensemble de A et de B. D'autre part, $A \cap B = A$ si et seulement si $A \subseteq B$. Si $A \cap B = \varnothing$, on dit que A et B sont **disjoints**. Si A et B sont disjoints, on écrit souvent $A + B$ pour l'union de A et de B. On dit que c'est **l'union disjointe** [1]. Les principales propriétés de ces opérations sur les suivantes sont les suivantes. Pour A, B, C des ensembles, alors

1. $A \cap A = A$ et $A \cup A = A$ (idempotence) ;
2. $A \cup B = B \cup A$ et $A \cap B = B \cap A$ (commutativité) ;
3. $A \cup \varnothing = A$ et $A \cap \varnothing = \varnothing$; et si $A \subseteq B$ alors $A \cup B = B$ et $A \cap B = A$ (existence d'éléments neutres).

Bien que ce soit l'une des notions les plus importantes des mathématiques, la définition rigoureuse moderne de la notion de fonction n'apparaît qu'au XIX^{e}(en 1837). Elle est due à Johann Dirichlet (1805-1859). Dans le langage de la théorie des ensembles, elle prend la forme suivante. Soit A et B deux ensembles. Une **fonction** f, de A vers B (on écrit $f : A \to B$), est une règle qui associe à chaque élément de a un unique élément de B. Plus techniquement, f est un sous-ensemble de $A \times B$, et on écrit $f(a) = b$ si et seulement si le couple (a, b) appartient à ce sous-ensemble. Pour que f soit une fonction, il suffit que

1. pour tout $a \in A$, il existe un b tel que $f(a) = b$, et
2. si $f(a) = b$ et $f(a) = c$, alors $b = c$.

Une fonction f de A vers B, est une **bijection**, si on a une fonction **inverse** $f^{-1} : B \to A$, pour la composition, c.-à-d. :

$$f^{-1} \circ f = \mathrm{Id}_A, \text{ et } f \circ f^{-1} = \mathrm{Id}_B. \tag{B.1}$$

Une fonction $f : A \to B$ est injective si et seulement si, pour tout a et tout b dans A

$$a \neq b \qquad \Longrightarrow \qquad fa) \neq f(b), \tag{B.2}$$

ce qui équivaut (c'est la contraposée) à dire aussi que

$$f(a) = f(b) \quad \text{entraine forcément} \quad b = b. \tag{B.3}$$

Une fonction $f : A \Rightarrow B$ est dite **surjective** si et seulement si pour chaque élément y de B, il existe au moins un élément x de A tel que $f(x) = y$. On montre qu'une fonction qui est à la fois surjective et injective est une fonction bijective, et inversement. Par définition [2], deux ensembles ont le même cardinal si et seulement si il existe une bijection entre les deux ensembles.

Pour A et B donnés, on désigne par B^A ou $\mathrm{Fonct}(A, B)$ **l'ensemble des fonctions** de A dans B.

1. On préfère ici la notation $A + B$ pour l'union disjointe de A et de B, plutôt que les notations $A \cup B$ ou $A \uplus B$.
2. La définition est nécessaire pour des ensembles infinis.

Solutions de certains exercices

Exercices du chapitre sur les groupes

Solution 1. Soit G un groupe et $Z(G)$ son centre de G. On veut vérifier que $Z(G)$ est un sous-groupe. Notons que $e \in C(G)$. Ensuite, si g_1 et $g_2$sont dans $Z(G)$, pour chaque $h \in G$ on aa

$$\begin{aligned} g_1 g_2 h &= g_1 h g_2, \qquad \text{car} \qquad g_2 \in Z(G) \\ &= h g_1 g_2, \qquad \text{car} \qquad g_1 \in Z(G), \end{aligned}$$

et donc $g_1 g_2 \in C(G)$. De plus, pour $g \in Z(G)$ et $h \in G$, on a par définition de $Z(G)$ que $hg = gh$, d'où $hg^{-1} = g^{-1}h$. On conclut que $g^{-1} \in Z(G)$, ce qui achève de montrer que $Z(G)$ est un sous-groupe. ■

Exercices du chapitre sur les actions de groupes

Solution 2 (Exercice 2.1). Pour G qui sur E, et F un sous-ensemble invariant pour cette action. On observe d'abord que toute orbite est un sous-ensemble invariant pour l'action de G. En effet, si $y \in \mathrm{Orb}(x)$ on a $y = h \cdot x$ pour un certain $h \in G$; et alors, pour tout $g \in G$, on a $g \cdot y = g \cdot (h \cdot x) = (gh) \cdot x$, d'où $g \cdot y$ est dans $\mathrm{Orb}(x)$. Ensuite, si $x \in F$, comme $g \cdot x \in F$ pour tout g, il s'ensuit que $\mathrm{Orb}(x) \subseteq F$. Clairement, on a

$$F \subseteq \bigcup_{x \in F} \mathrm{Orb}(x),$$

puisque $x \in \mathrm{Orb}(x)$. D'autre part, l'inclusion $\mathrm{Orb}(x) \subseteq F$, pour tout $x \in \Gamma$, entraîne que

$$\bigcup_{x \in F} \mathrm{Orb}(x) \subseteq F,$$

d'où l'égalité, et F est bien une réunion d'orbites.

On a observé ci-haut que $\mathrm{Orb}(x)$ est un sous-ensemble invariant auquel appartient x. De plus, $\mathrm{Orb}(x)$ est contenu dans tout sous-ensemble invariant contenant x. Donc $\mathrm{Orb}(x)$ est le plus petit sous-ensemble invariant auquel x appartient. ■

Solution 3 (Exercice 2.2). Pour voir que A_4 n'a pas de sous-groupe d'ordre 6, on rappelle qu'il contient les 12 éléments

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}.$$

Ces éléments de A_4 sont d'ordre 1,2 ou 3, et donnent les groupes cycliques suivants :

$$\begin{array}{rclrcl} T &=& \{e\}, & H_1 &=& \{e, (12)(34)\}, \\ H_2 &=& \{e, (13)(24)\}, & H_3 &=& \{e, (14)(23)\} \\ K_1 &=& \{e, (123), (132)\}, & K_2 &=& \{e, (124), (142)\}, \\ K_3 &=& \{e, (134), (143)\}, & K_4 &=& \{e, (234)(243)\}. \end{array}$$

Pour avoir un sous-groupe $H \leqslant A_4$ de cardinal 6. Comme A_4 ne possède que des éléments d'ordre 1, 2 ou 3, seulement 4 éléments d'ordre 2, un sous-groupe d'ordre H devrait posséder au moins un élément d'ordre 2, et un élément d'ordre 3. Par exemple, si $(12)(34) \in H$ et $(123) \in H$, devrait aussi contenir les éléments

$$\begin{array}{ll} (132) = (123)(123), & (12)(34)(123) = (243), \\ (12)(34)(132) = (143), & (123)(12)(34) = (134), \end{array}$$

ce qui donne déjà 7 éléments (en comptant e), ce qui serait impossible par hypothèse. De même que H doit contenir au moins un H_i et un K_j, mais on vérifie (cas par cas) qu'on a alors $\langle H_i \cup K_j \rangle = A_4$. ■

Solution 4 (Exercice 2.3). On considère l'action naturelle du groupe symétrique S_n sur l'ensemble $\Omega := \{1, 2, \ldots, n\}$.

Décomposition d'une permutation en cycles disjoints. Pour $\sigma \in S_n$, considérons l'action de $H = \langle \sigma \rangle$ sur Ω. La décomposition de Ω en H-orbites donne

$$\Omega = \Omega_1 + \ldots + \Omega_k, \tag{B.4}$$

où chaque Ω_i peut s'écrire sous la forme $\Omega_i = \{\omega_i, \sigma(\omega_i), \sigma^2(\omega_i), \ldots, \sigma^{\ell(i)-1}(\omega_i)\}$, en supposant que $\omega_i := \min(\Omega_i)$ est le plus petit élément de l'orbite Ω_i. Posons

$$\gamma_i := (\omega_i, \sigma(\omega_i), \ldots, \sigma^{\ell(i)-1}(\omega_i)), \tag{B.5}$$

de sorte que les cycles γ_i sont disjoints (par (B.4)), et respectivement de longueur $\ell(i)$. On constate que

$$\sigma = \gamma_1 \gamma_2 \ldots \gamma_k \tag{B.6}$$

peut s'écrire comme produit de cycles disjoints, par le calcul suivant. Pour $j \in \Omega$, si $j \notin \Omega_i$, alors $\gamma_i(j) = j$ par construction, et donc $\gamma_1 \gamma_2 \ldots \gamma_k(j) = \gamma_i(j)$, pour l'unique i tel que $j \in \Omega_i$. Mais alors $j = \sigma^{(r)}(\omega_i)$, pour un certain $1 \leqslant r < \ell(i)$, et

$$\gamma_i(j) = \gamma_i(\sigma^{(r)}(\omega_i)) = \sigma(\sigma^{(r)}(\omega_i)) = \sigma(j).$$

Ainsi a que $\gamma_1 \dots \gamma_k(j) = \sigma(j)$, pour tout $j \in \Omega$. Soit maintenant $\gamma = (a_1, \dots, a_l)$, et $\rho = (b_1, \dots, b_m)$ des cycles disjoints respectivement de support $A = \{a_1, \dots, a_l\}$ et $B = \{b_1, \dots, b_m\}$. Alors, γ laisse fixe les éléments de B, et ρ laisse fixe ceux de A. De sorte que pour $j \in \Omega$, on a

$$\gamma\rho(j) = \begin{cases} j & \text{si } j \notin A + B, \\ \rho(j) & \text{si } j \in B, \\ \gamma(j) & \text{si } j \in A, \end{cases} \qquad \text{et} \qquad \rho\gamma(j) = \begin{cases} j & \text{si } j \notin A + B, \\ \rho(j) & \text{si } j \in B, \\ \gamma(j) & \text{si } j \in A. \end{cases}$$

On a donc bien $\gamma\rho = \rho\gamma$, donc **les cycles disjoints commutent**. **L'unicité de la décomposition en cycles disjoints**, correspond à l'unicité de la décomposition en orbites.

Les classes de conjugaison de S_n. Considérons, comme en (B.6), la décomposition $\gamma_1 \dots \gamma_k$ de σ en cycles disjoints de longueurs respectives $\ell(\gamma_i) = \mu_i$, qu'on suppose ordonné de façon à ce que $\mu_1 \geqslant \mu_2 \geqslant \dots \geqslant \mu_k$. Désignons encore une fois par Ω_i le support de γ_i. Comme ce sont les H-orbites de Ω pour $H = \langle\sigma\rangle$, on a que $n = \mu_1 + \mu_2 + \dots + \mu_k$ est un partage de n qu'on dénote $\pi(\sigma)$. Inversement, pour tout partage $(\mu_1, \mu_2, \cdots, \mu_k)$ de n, on peut considérer la permutation

$$\sigma = (1, 2 \dots m_1)(m_1 + 1, \dots, m_2) \dots (m_{k-1} + 1, \dots, m_k) \qquad \text{où} \qquad m_i := \mu_1 + \dots + \mu_i.$$

Ainsi donc, les m_i sont les sommes partielles consécutives de μ. En particulier, $m_k = n$. Il s'ensuit qu'on a une surjection $\pi : S_n \twoheadrightarrow \mathbb{P}_n$, où $\mathbb{P}_n$ désigne l'ensemble des partages de n. Pour montrer qu'il y a bijection entre l'ensemble $\mathcal{C}_n$, des classes de conjugaison de S_n, et l'ensemble $\mathbb{P}_n$, il suffit de voir que σ et τ sont conjugués si et seulement si $\pi(\sigma) = \pi(\tau)$. Or, si σ et τ sont conjugués, il y a une permutation ρ telle que $\tau = \rho\sigma\rho^{-1}$. Il s'ensuit que

$$\tau = (\rho\gamma_1\rho^{-1})(\rho\gamma_2\rho^{-1}) \dots (\rho\gamma_k\rho^{-1}),$$

et on constate que les $(\rho\gamma_i\rho^{-1})$ sont des cycles disjoints de même longueur que les γ_i, c'est la décomposition en cycle de τ, et donc $\pi(\sigma) = \pi(\tau)$. En effet, on a

$$\sigma(i) = j \qquad \text{ssi} \qquad \tau(\rho(i)) = \rho(j),$$

comme le montre le calcul

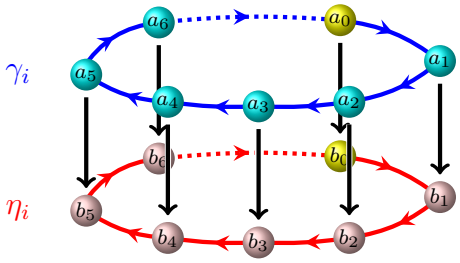
$$\begin{aligned} \tau(\rho(i)) = \rho(j) \qquad &\iff \qquad \rho\sigma\rho^{-1}(\rho(i)) = \rho(j) \\ &\iff \qquad \rho\sigma(i)) = \rho(j) \\ &\iff \qquad \sigma(i) = \rho^{-1}\rho(j) \\ &\iff \qquad \sigma(i) = j. \end{aligned}$$

Les cycles de τ s'obtiennent donc de ceux de σ en remplaçant i par $\rho(i)$.

Inversement, si les partages associés sont égaux, c.-à-d. $\pi(\tau) = \pi(\sigma)$, on cherche à montrer que σ et τ sont conjugués. Pour ce faire on ordonne les décompositions en cycles de chacune des permutations en ordre décroissants de cycles (l'ordre entre deux cycles de même longueur n'importe pas), pour obtenir

$$\begin{aligned} \sigma &= \gamma_1\gamma_2\cdots\gamma_k \\ \tau &= \eta_1\eta_2\cdots\eta_k, \end{aligned}$$

avec $\ell(\gamma_i) = \ell(\eta_i)$, et chaque cycle débutant par le plus petit élément de son support comme on l'a fait plus haut en (B.5). On construit alors une permutation ρ, qui sera telle que $\tau = \rho\sigma\rho^{-1}$ montrant ainsi que σ et τ sont conjugués, de la façon suivante. Par construction ρ est telle que $\eta_i\rho\gamma_i\rho^{-1}$. Pour terminer la description de ρ, soit a_0 le plus petit élément du cycle γ_i, et b_0 le plus petit élément du cycle η_i correspondant, et donc de même longueur ℓ. On défini ρ comme suit, avec $a_r := \sigma^r(a_0)$, et $b_r = \tau^r(b_0)$,



autrement dit $\rho(\sigma^r(a_0)) := \tau^r(b_0)$. Ainsi ρ est bijective, parce qu'on a des décompositions en cycles disjoints, et possède les propriétés voulues par construction.

L'énumération des permutations dans la classe de conjugaison correspondant à un partage μ s'obtient directement en choisissant comment disposer les entiers de 1 à n dans les cycles. Illustrons par un exemple. Considérons le partage $\mu = 22111$ de 7. Une permutation cyclique de ce type prend la forme $(ab)(cd)(e)(f)(g)$, pour $\{a, b, c, d, e, f, g\} = \{1, 2, 3, 4, 5, 6, 7\}$. On considère les 7! permutations $\sigma = \sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6\sigma_7$ de $\{1, 2, 3, 4, 5, 6, 7\}$. Pour chacune de ces permutations, on construit une décomposition cyclique de la forme voulue en prenant

$$(ab) = (\sigma_1\sigma_2), \qquad (cd) = (\sigma_3\sigma_4), \qquad (e) = \sigma_5, \qquad (f) = \sigma_6, \qquad (g) = \sigma_7.$$

Toutes les permutations de la classe de conjugaison saont clairement obtenues ainsi. Cependant, on a plusieurs σ qui donnent la même décomposition cyclique. Ainsi, on a

$$(ab)(cd)(e)(f)(g) = (dc)(ab)(f)(g)(e) = (ba)(dc)(f)(e)(g) = \cdots$$

En fait, dans chaque cas il y a 48 permutations qui donnent la même décomposition cyclique. Ces 48 possibilités correspondent au produit des 8 façons de présenter les deux cycles de longueur 2, par les 8 façons de présenter es 3 point fixes. Une preuve générale plus conceptuelle passe par le calcul du stabilisateur d'une permutation cyclique fixé de type μ, pour l'action par conjugaison. Le nombre de

permutations dans ce stabilisateur est le denominateur de la formule (2.15). Pour le voir, on constate qu'une permutation appartenant au stabilisateur s'obtient en permutant les cycles de même longueur (c'est le facteur $d_i!$), puis en « tournant » chaque sur lui-même (il y a i telles rotations qui donne le même cycle, ce qui donne le facteur i^{d_i}). ■

Solution 5. Pour p un nombre premier, et G un groupe d'ordre p^2, montrons que G est abélien. On sait déjà que le centre de G est non trivial, et on a donc un élément $x \in Z(G)$ distinct du neutre $x \neq e$. Si $\text{ord}(x) = p^2$, alors $G = \langle x \rangle$ est cyclique, et donc G abélien. Sinon, on a forcément $\text{ord}(x) = p$, de plus $H = \langle x \rangle$ est un sous-groupe normal de G, et G/H est un groupe d'ordre p. En particulier, G/H est cyclique, et on a

$$G/H = \langle yH \rangle = \{H, yH, \ldots, y^{p-1}H\},$$

pour un certain y dans G. On adonc la décomposition de G en classes à gauches disjointes

$$G = H + yH + \ldots + y^{p-1}H.$$

Autrement dit, tout élément g de G s'exprime sous la forme $g = y^i x^j$. On calcule alors, pour $g_1 = y^i x^j$, $g_2 = y^k x^l$, que

$$\begin{aligned}
g_1 g_2 &= y^i x^j y^k x^l \\
&= y^i y^k x^j x^l, \qquad \text{car} \qquad x \in Z(G) \\
&= y^{i+k} x^{j+l} \\
&= y^{k+i} x^{l+j} \\
&= y^k y^i x^l x^j \\
&= y^k x^l y^i x^j, \qquad \text{car} \qquad x \in Z(G) \\
&= g_2 g_1,
\end{aligned}$$

ce qui montre que G est abélien. ■

Solution 6. Pour G agissant sur E, et $Y \subseteq E$, on veut montre que

$$H = \{g \in H \mid g \cdot y = y, \text{pour tout } y \in Y\},$$

est un sous-groupe de G. Or,

$$H = \{g \in G \mid g \in \text{Stab}(y), \text{pour tout } y \in Y\} = \bigcap_{y \in Y} \text{Stab}(y),$$

est l'intersection d'une famille de sous-groupes, d'où $H \leqslant G$. ■

Solution 7. Le groupe

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R},\ a \neq 0,\ c \neq 0 \right\}.$$

est un sous-groupe de $GL_2(\mathbb{R})$. En effet, on voit d'abord que $\mathrm{Id} \in G$, en prenant $a = c = 1$ et $b = 0$. Puis, pour

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \qquad \text{et} \qquad B = \begin{pmatrix} e & f \\ 0 & g \end{pmatrix},$$

avec a, c, e et g non-nuls, on constate que la matrice

$$AB = \begin{pmatrix} ae & af + bg \\ 0 & cg \end{pmatrix}$$

est de la forme voulue, et $AB \in G$ puisqu'on a aussi ae et cg non-nuls. On calcule aussi que

$$A^{-1} = \begin{pmatrix} a^{-1} & -ba^{-1}c^{-1} \\ 0 & c^{-1} \end{pmatrix},$$

et donc $A^{-1} \in G$, puisque a^{-1} et c^{-1} sont non-nuls. On conclut que G est un sous-groupe.

On veut ensuite montrer que G agit sur $\mathbb{R}$ par l'opération

$$A \cdot x := \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot x = \frac{ax + b}{c}.$$

Pour ce faire, on calcule aissément que $\mathrm{Id} \cdot x = x$, puis que

$$\begin{aligned} A \cdot (B \cdot x) &= A \cdot \left(\frac{ex + f}{g} \right) \\ &= \frac{a\left((ex + f)/g\right) + b}{c} \\ &= \frac{aex + af + bg}{cg} \\ &= (AB) \cdot x, \end{aligned}$$

ee qui achève de montrer qu'on a une action.

Notons ensuite que

$$A \cdot 0 = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot 0 = \frac{a \cdot 0 + b}{c} = \frac{b}{c}.$$

Clairement b/c prend toutes les valeurs réelles, et donc $\mathrm{Orb}(0) = \mathbb{R}$. De plus, $A \cdot 0 = b/c$ est si et seulement si $b = 0$, d'où

$$\mathrm{Stab}(0) = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^* \right\},$$

ce qui achève la solution. ■

Solution 8. Soit $G := \mathrm{ISO}_{\mathbb{R}^3}$ l'ensemble des isométries de $\mathbb{R}^3$. Par définition, $f \in G$ si et seulement si

$$\mathbf{d}(f(P), f(Q)) = \mathbf{d}(P, Q),$$

pour tous points P et Q dans $\mathbb{R}^3$. Clairement la fonction identité préserve les distance. On observe ensuite que, pour f et g dans G,

$$\mathbf{d}(f(g(P)), f(g(Q))) = \mathbf{d}(g(P), g(Q)) = \mathbf{d}(P, Q),$$

et donc $f \circ g$ est dans G. D'autre part,

$$\mathbf{d}(f^{-1}(P), f^{-1}(Q)) = \mathbf{d}(f(f^{-1}(P)), f(f^{-1}(Q))) = \mathbf{d}(P, Q),$$

et on déduit que G est un sous-groupe du groupe $S_{\mathbb{R}^3}$, des fonctions inversibles de $\mathbb{R}^3$ dans lui-même. Or, on a déjà vu qu'on a l'action naturelle

$$S_{\mathbb{R}^3} \times \mathbb{R}^3 \to \mathbb{R}^3, \qquad \text{avec} \qquad f \cdot P = f(P).$$

Celle-ci induit l'action voulue sur son sous-groupe $G = \mathrm{ISO}_{\mathbb{R}^3}$. ■

Solution 9. Pour p premier on considère

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}_p \right\},$$

le groupe des matrices triangulaires supérieures à coefficients dans le corps $\mathbb{Z}_p$. Prenant $a = b = c = 0$ on constate que G contient la matrice indentité. On calcule ensuite que le produit de deux matrices triangulaires supérieures est aussi une matrice triangulaire supérieure :

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix},$$

de même pour l'inverse

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

Il s'ensuit que G est un sous-groupe de $\mathrm{GL}_3(\mathbb{Z}_p)$. Comme on peut choisir a, b et c librement dans $\mathbb{Z}_p$, l'ordre de G est p^3. On constate que G n'est pas abélien avec l'exemple suivant

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Enfin, on calcule que

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : t \in \mathbb{Z}_p \right\}$$

est le centre de G comme suit. D'abord, on a bien la commutation

$$\begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b+t \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & t+b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

Ne reste plus qu'à voir qu'il n'y a pas d'autres éléments dans $Z(G)$. Pour cela, on cherche x, t, et z tels que les matrices suivantes soient égales

$$\begin{pmatrix} 1 & x & t \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & b+xc+t \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & t \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & t+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{pmatrix}$$

ce qui équivaut à $c\,x = a\,z$, pour tous $a, c \in \mathbb{Z}_p$. La seule solution de ces équations est $x = z = 0$. On a ainsi vérifié que le centre de G est bien tel qu'annoncé. ■

Exercices du chapitre sur les produits directs de groupes

Exercices du chapitre sur les morphismes de groupes

Solution 10 (Exercice 3.3). À une action $\alpha : G \times E \to E$ on fait correspondre un morphisme de G dans le groupe S_E des permutations de E, en considèrant la fonction $\widetilde{\alpha} : G \to S_E$, défini par

$$\widetilde{\alpha}(g) = \alpha_g,$$

avec $\alpha_g : E \to E$ la fonction définie en posant $\alpha_g(x) := g \cdot x$. C'est bien une bijection de E vers E, puisqu'elle admet l'inverse $\alpha_{g^{-1}}$:

$$\alpha_{g^{-1}}(\alpha_g(x)) = \alpha_{g^{-1}}(g \cdot x) = g^{-1} \cdot (g \cdot x) = x.$$

Donc α_g est dans S_E, et $\widetilde{\alpha}$ est bien défini. Vérifier que $\widetilde{\alpha}$ est un morphisme, correspond à voir que les bijections α_{gh} et $\alpha_g \circ \alpha_h$ coïncident. En effet, pour tout $x \in E$, on a

$$\begin{aligned} \alpha_{gh}(x) &= (gh) \cdot x \\ &= g \cdot (h \cdot x) \\ &= \alpha_g(\alpha_h(x)) \\ &= (\alpha_g \circ \alpha_h)(x) \end{aligned}$$

D'autre part, à un morphisme $\varphi : G \to S_E$ on fait correspondre l'action $\overline{\varphi} : G \times E \to E$, définie par $\overline{\varphi}(g, x) = \varphi(g)(x)$. Écrivant $g \cdot_\varphi x$ pour $\varphi(g)(x)$, on vérifie comme suit qu'on a une action de G sur E. En effet, pour $x \in E$, on a

$$\begin{aligned} e \cdot_\varphi x &= \varphi(e)(x) \\ &= \mathrm{Id}(x), \end{aligned}$$

car $\varphi(e) = \mathrm{Id}$. Ensuite, pour $g, h \in G$ et $x \in E$, on calcule que

$$\begin{aligned} g \cdot_\varphi (h \cdot_\varphi x) &= g \cdot_\varphi (\varphi(h)(x)) \\ &= \varphi(g)(\varphi(h)(x)) \\ &= (\varphi(g) \circ \varphi(h))(x) \\ &= \varphi(gh)(x) \\ &= (gh) \cdot_\varphi x, \end{aligned}$$

et donc on a bien une action.

Les correspondances $\alpha \mapsto \widetilde{\alpha}$ et $\varphi \mapsto \overline{\varphi}$ sont inverses l'une de l'autre. En effet, on a

$$\overline{\widetilde{\alpha}}(g, x) = \widetilde{\alpha}(g)(x) = \alpha_g(x) = g \cdot x = \alpha(g, x),$$

pour tout g et x, ce qui montre que $\overline{\widetilde{\alpha}} = \alpha$. Réciproquement,

$$\widetilde{\overline{\varphi}}(g)(x) = \overline{\varphi}_g(x) = \varphi(g)(x),$$

pour tout x et g, et donc $\widetilde{\overline{\varphi}}(g) = \varphi(g)$ pour tout g, d'où $\widetilde{\overline{\varphi}} = \varphi$. On a donc tout montré. ■

Exercices du chapitre sur les groupes quotients

Solution 11 (Exercice 4.6). Dans le groupe symétrique (avec les permutations présentées comme produit de cycles disjoints)

$$S_3 = \{e,\ (12),\ (13),\ (23),\ (123),\ (132)\},$$

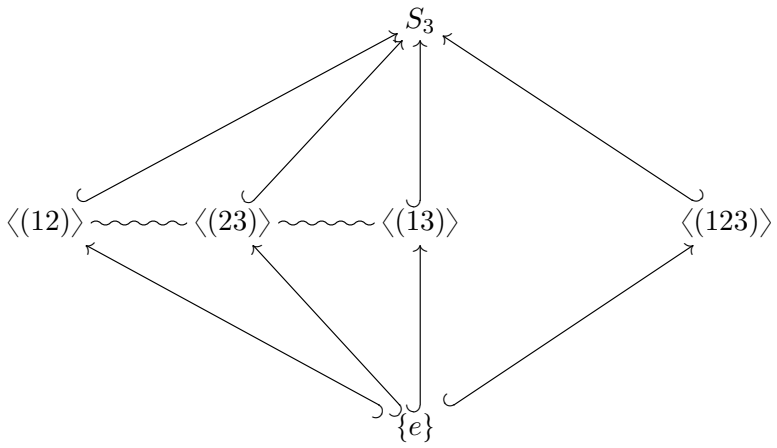
on cherche à trouver tous les sous-groupes ; et, parmi ceux-ci, déterminer ceux qui sont normaux. Par le théorème de Lagrange l'ordre d'un sous-groupe doit être un diviseur de 6 (l'ordre de S_3), les possibilités sont donc 1, 2, 3, et 6. On note que (12), (13), et (23) sont des éléments d'ordre 2, engendrant chacun un sous-groupe d'ordre 2. Ce sont les transpositions. D'autre part (123) et (132) sont des éléments d'ordre 3. Ce sont les permutations cycliques. Comme $(123) \circ (123) = (132)$, ils donnent lieu à un sous-groupe d'ordre 3. Enfin, deux transposition quelconque engendrent tout S_3. C'est le cas aussi pour une transposition et une permutation cyclique. Les seuls sous-groupes possibles sont donc les suivants :

$$\begin{aligned}
&\text{ordre } 1 \;:\; H_1 = \{e\},\\
&\text{ordre } 2 \;:\; H_2 = \{e,(12)\}, \qquad H_3 = \{e,(23)\}, \qquad H_4 = \{e,(13)\},\\
&\text{ordre } 3 \;:\; H_5 = \{e,(123),(132)\}, \qquad \text{et}\\
&\text{ordre } 6 \;:\; S_3.
\end{aligned}$$

Parmi ceux-ci, les seuls qui sont normaux sont H_1, H_5, et S_3. C'est évident pour H_1 et S_3. Pour H_5, cela résulte du fait que le conjugué d'une permutation circulaire est aussi une permutation circulaire (voir solution 4), ce que sont tous les éléments de H_5 (sauf l'identité). Tous les autres (qui sont en fait conjugués les uns des autres) ne sont pas normaux. En effet, on a

$$(13)\, H_2\, (13)^{-1} = H_3, \qquad \text{et} \qquad (12)\, H_3\, (12)^{-1} = H_4.$$

On a le treillis d'inclusion



où $H \rightsquigarrow K$ signifie que les sous-groupes en questions sont conjugués. ■

Exercices du chapitre sur les groupes abéliens finis

Solution 12. Pour un groupe abélien fini A, et d diviseur $|A|$, et on cherche à montrer que A possède un sous-groupe d'ordre d. C'es là la réciproque du théorème de Lagrange pour les groupes abéliens. Pour ce faire, soit $|A| = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ la décomposition de $|A|$ en facteurs premiers distincts. On a donc $d = p_1^{k_1} \dots p_n^{k_n}$ avec $k_i \leqslant \alpha_i$. À cette fin, on considère la décomposition

$$A \simeq A(p_1) \times \cdots \times A(p_n),$$

de A en produit direct des composantes primaires. Il suffit de montrer que chaque $A(p_i)$ admet un sous-groupe d'ordre p^{k_i}. En effet, supposons qu'on ait $H_i < A(p_i)$ tel que $|H_i| = p^{k_i}$. Alors

$$H_1 \times \cdots \times H_n < A(p_i) \times \cdots \times A(p_n)$$

et

$$|H_1 \times \cdots \times H_n| = |H_1| \cdot \cdots \cdot |H_n| = p_1^{k_1} \dots p_n^{k_n} = d.$$

Le sous-groupe H est donc le groupe cherché. On se ramène donc à considérer le cas des p-groupes. Soit donc G un p-groupe, de cardinal $|G| = p^\alpha$, et d un diviseur de $|G|$, c.-à-d. $d = p^k$, pour $1 \leqslant k \leqslant \alpha$. On veut voir que G possède un sous-groupe d'ordre p^k. Considérons la décomposition de G en sous-groupes cycliques :

$$G \simeq G_1 \times \cdots \times G_r, \qquad \text{avec} \qquad |G_i| = p^{\alpha_i},$$

pour certains $\alpha_1 \leqslant \cdots \leqslant \alpha_r$. Si $k = \alpha_i$ pour un certain i alors le sous-groupe G_i fait l'affaire. D'autre part, si $k = \alpha_{i_1} + \cdots + \alpha_{i_s}$ pour certains $\alpha_{i_1} \leqslant \cdots \leqslant \alpha_{i_s}$, alors

$$\{e\} \times \cdots \times \{e\} \times G_{\alpha_{i_1}} \times \{e\} \times \cdots \times G_{\alpha_{i_2}} \times \{e\} \times \cdots \times G_{\alpha_{i_s}} \times \{e\} \times \cdots \times \{e\}$$

est un sous-groupe de $G_1 \times \cdots \times G_r$ qui est d'ordre d. Comme G est isomorphe à $G_1 \times \cdots \times G_r$, il possède aussi un sous-groupe d'ordre d.

Sinon, soit i_0 l'indice maximum tel que $\alpha_1 + \cdots + \alpha_{i_0} < k$. Alors on a

$$\alpha_1 + \cdots + \alpha_{i_0} < k < \alpha_1 + \cdots + \alpha_{i_0} + \alpha_{i_0+1}, \qquad \text{avec} \qquad k - (\alpha_1 + \cdots + \alpha_{i_0}) < \alpha_{i_0+1}.$$

Comme $G_{\alpha_{i_0}+1}$ est cyclique d'ordre $p^{\alpha_{i_0+1}}$, il possède un sous-groupe d'ordre $p^{k-(\alpha_1+\cdots+\alpha_{i_0})}$, disons H_{i_0}. Observons que $G_{\alpha_{i_0+1}} \simeq \mathbb{Z}_{p^{\alpha_{i_0+1}}}$ et $\langle p^{\alpha_1+\cdots+\alpha_{i_0+1}-k} \rangle$ est un sous-groupe d'ordre $p^{k-(\alpha_1+\cdots+\alpha_{i_0})}$ de $\mathbb{Z}_{p^{\alpha_{i_0+1}}}$. Mais alors,

$$G_{\alpha_1} \times \cdots \times G_{\alpha_{i_0}} \times H_{i_0} \times \{e\} \times \{e\} \times \cdots \times \{e\}$$

est un sous-groupe de $G_1 \times \cdots \times G_r$ d'ordre $p^{\alpha_1} p^{\alpha_2} \cdots p^{\alpha_{i_0}} \cdot p^{k-(\alpha_1+\cdots+\alpha_{i_0})} = p^k = d$. Encore une fois, G, étant isomorphe à $G_1 \times \cdots \times G_r$, possède aussi un sous-groupe d'ordre d. ■

Solution 13. Pour un groupe abélien fini G dont l'ordre $|G| = n$ n'est pas divisible par le carré d'un entier plus grand que 1, on cherche à voir que G est cyclique. L'hypothèse assure que $|G| = p_1 \dots p_k$, où les p_i sont des nombres premiers distincts. On a la décomposition de G en produit direct de ses composantes primaires :

$$G \simeq G(p_1) \times \ldots \times G(p_k),$$

pour laquelle $|G(p_i)| = p_i$. Donc

$$G(p_i) \simeq \mathbb{Z}_{p_i}, \qquad \text{et} \qquad G \simeq \mathbb{Z}_{p_i} \times \ldots \times \mathbb{Z}_{p_n}.$$

Par ailleurs, $\mathbb{Z}_n \simeq \mathbb{Z}_{p_i} \times \ldots \times \mathbb{Z}_{p_n}$. D'où $G \simeq \mathbb{Z}_n$ et donc G est cyclique. ■

Solution 14. On cherche à énumérer tous les groupes abéliens non isomorphes d'ordre 72 (à isomorphisme près). On a $72 = 8 \cdot 9 = 2^3 \cdot 3^2$. Pour G abélien d'ordre 72, on a

$$G \simeq G(2) \times G(3), \quad |G(2)| = 2^3, \quad \text{et} \quad |G(3)| = 3^2.$$

Considérant les possibilités pour $G(2)$ et $G(3)$ on trouve la liste suivante (par le théorème d'unicité pour la décomposition en p-groupes cycliques) :

1) $\mathbb{Z}_8 \times \mathbb{Z}_9$,
2) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$,
3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$,
4) $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$,
5) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$,
6) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$,

tous non isomorphes, et il n'y a pas d'autres cas. ■

Solution 15. Pour B un sous-groupe d'un groupe G, on considère l'action de B sur les parties de G par translation à gauche. On veux montrer que, pour tout (autre) sous-groupe A de G, on a $\mathrm{Stab}_B(A) = A \cap B$. On a d'abord que $A \cap B \subseteq \mathrm{Stab}_B(A)$, puisque chaque $g \in A \cap B$ est tel que $gA = A$, étant donné que $g \in A$. D'autre part, par définition, si $g \in B$ appartient à $\mathrm{Stab}_B(A)$ alors $gA = A$. In s'ensuit en particulier que $ge = g \in A$, ce qui montre que $\mathrm{Stab}_B(A) \subseteq A \cap B$. On a donc montré l'égalité cherchée. ■

Exercices du chapitre sur les p-groupes et théorèmes de Sylow

Solution 16. Soit G un groupe d'ordre $96 = 2^5 \cdot 3$. Considérons N_2, le nombre de 2-sous-groupes de Sylow. On a $N_2 \equiv 1$ modulo 2, et N_2 divise 96. Les possibilités sont $N_2 = 1$ et $N_2 = 3$. Si $N_2 = 1$, alors l'unique 2-sous-groupe de Sylow est normal, par le 2^e théorème de Sylow. Si $N_2 = 3$, soient H, K deux 2-sous-groupes de Sylow ; ils sont d'ordre 32. L'intersection $H \cap K$ est un sous-groupe d'ordre $2, 4, 8$ ou 16. Si $|H \cap K| \leqslant 8$, alors

$$\begin{aligned} |HK| &= \frac{|H| \cdot |K|}{|H \cap K|} \\ &\geqslant \frac{32 \cdot 32}{8} = 128 \end{aligned}$$

ce qui est trop dans un groupe d'ordre 96. Ainsi, on doit avoir $|H \cap K| = 16$. Alors

$$|HK| = \frac{32 \cdot 32}{16} = 64$$

Par ailleurs, $H \cap K$ est d'indice 2 dans H, et aussi dans K, d'où $H \cap K \lhd H$ et $H \cap K \lhd K$. Cela entraîne que $HK \subseteq N(H \cap K)$, le normalisateur de $H \cap K$. D'où $|N(H \cap K)| \geqslant 64$. Comme $|N(H \cap K)|$ doit aussi être un diviseur de 96, on doit avoir $|N(H \cap K)| = 96$, et donc $N(H \cap K) = G$, ce qui revient à dire que $H \cap K$ est un sous-groupe normal. ■

Solution 17. Pour un groupe G d'ordre $104 = 2^3 \cdot 13$, on suppose qu'aucun sous-groupe d'ordre 8 n'est normal. Les sous-groupes d'ordre 8 sont les 2-sous-groupes de Sylow. Leur nombre, N_2, est impair et divise 104. Les possibilités sont $N_2 = 1$ ou $N_2 = 13$. Si $N_2 = 1$, alors l'unique 2-sous-groupe de Sylow serait normal par le 2^e théorème de Sylow, mais cela ne peut être le cas par hypothèse. La seule possibilité qui reste est $N_2 = 13$, et il y a donc 13 sous-groupes d'ordre 8. ■

Solution 18. Pour G un groupe fini, soit p le plus petit diviseur premier de $|G|$, et $H \geqslant G$ tel que $[G : H] = p$. Dénotons par $E = \{H, x_1H, \ldots, x_{p-1}H\}$ l'ensemble des translatés à gauche de H. On considère le morphisme $\varphi : G \to S_E$ qui correspond à l'action de G sur E par translation à gauche, et on pose

$$K = \{f \in S_E \mid f(H) = H\}, \qquad \text{et} \qquad L = \{\varphi(h) \mid h \in H\}.$$

On veut montrer que H est un sous-groupe normal de G. Par définition, pour $g \in G$, $\varphi(g)$ est la permutation de E

$$\varphi(g)(x_iH) = gx_iH.$$

On a que $\ker(\varphi) \subseteq H$. En effet, supposons $g \in \ker(\varphi)$, on a alors en particulier, on a $gH = H$ et donc $g \cdot e = g \in H$, tel que voulu. On vérifie ensuite que K est un sous-groupe de S_E de cardinal

$|K| = (p-1)!$. En effet, K est le stabilisateur de H pour l'action naturelle de S_E sur E. En fixant H, il reste $(p-1)$ éléments de E à permuter et tous les cas se réalisent. On a donc $|K| = |S_{p-1}| = (p-1)!$.

Montrons maintenant que L est un sous-groupe de K, dont le cardinal divise donc $(p-1)!$. En effet, L est l'image de H par le morphisme φ. C'est donc un sous-groupe de S_E. D'autre part, pour $f \in L$, avec $f = \varphi(h)$ pour un certain $h \in H$, on a $f(H) = \varphi(h)(H) = hH = H$, puisque $h \in H$. Donc $L \subseteq K$ tel qu'annoncé. Montrons ensuite que $|L|$ divise $|H|$. À cette fin, considérons la restriction $\varphi|_H \colon H \to L$, xd φ à H. Par le théorème des isomorphismes, $\varphi|_H$ se factorise à travers un isomorphisme de $H/\ker(\varphi|_H)$ sur l'image de $\varphi|_H$ qui est L, d'où $|H| = |\ker(\varphi|_H)| \cdot |L|$.ce qui montre l'affirmation. résultat.

On a en fait $|L| = 1$ et $H = \ker(\varphi)$. En effet, par les arguments ci-haut, $|L| < p$ et $|L|$ est un diviseur de $|H|$, donc aussi un diviseur de $|G|$. Par l'hypothèse faite sur p, la seule possibilité est que $|L| = 1$. Mais alors φ envoie tous les éléments de H sur l'élément neutre de S_E, ou autrement dit $H \subseteq \ker(\varphi)$. On conclut que $H = \ker(\varphi)$ comme voulu. ■

Exercices exploratoires

Solution 19. Plus généralement, si « $\star$ » est une opération sur B, les propriétés de $\star$ sont en général vérifiées pour les fonctions $f : X \to B$ et $g : X \to B$, quelque soit X, muni de l'opération $f \star g$ définie en posant

$$(f \star g)(x) := f(x) \star g(x), \qquad \text{pour tout} \qquad x \in X.$$

Dans chaque cas, on se ramène en effet à vérifier que la propriété est satisfaite dans B. Par exemple, si $\star$ est une opération commutative dans B, alors on a une opération commutative correspondante dans B^X, l'ensemble des fonctions de X dans B. En effet, on calcule ainsi

$$(f \star g)(x) = f(x) \star g(x) = g(x) \star f(x) = (g \star f)(x),$$

en observant que l'étape du milieu correspond à la commutativité de $\star$ pour B. Il en est de même pour l'associativité, l'inverse, l'élément neutre (qui correspond à la fonction constante dont la valeur est le neutre pour $\star$ dans B), etc. Donc, si $(B, \star)$ forme un groupe (abélien), alors c'est le cas aussi pour $(B^X, \star)$.

(a) En utilisant le principe ci-dessus, on conclut que $(\mathbb{R}^X, +)$ et $(\mathbb{R}^X, \cdot)$ sont des groupes abéliens. La distributivité de la multiplication sur l'addition dans $\mathbb{R}$ entraîne qu'on a la même propriété dans $\mathbb{R}^X$, par le même principe.

(b) Pour montrer que l'ensemble $\mathcal{C}(\mathbb{R})$ des fonctions continues de $\mathbb{R}$ vers $\mathbb{R}$ est a bien un anneau, avec les opérations comme ci-dessus ; il suffit d'observer que $\mathcal{C}(\mathbb{R})$ est un sous-ensemble de $\mathbb{R}^{\mathbb{R}}$ fermé pour l'addition, l'inverse additif et le produit de $\mathbb{R}^{\mathbb{R}}$. En effet, la somme et le produit de deux fonctions continues donne une fonction continue, et l'inverse additif d'une fonction continue est une fonction continue.

(c) Pour voir qu'on a bien un anneau en considérant l'ensemble $M_n(A)$, des matrices carrées $n \times n$ à coefficients dans A, avec les opérations habituelles sur les matrices ; on part du fait déjà connu que $M_n(A)$ forme un anneau dans le cas où A est un corps. On remarque en effet que les seules propriétés des corps utilisées dans la démonstration classique sont celles d'anneau unitaire. Les calculs sont exactement les mêmes qu'on fait dans un cours d'algèbre linéaire, omis le calcul de l'inverse de matrices qui n'intervient pas ici.

(d) On sait déjà que $A[x_1, \ldots, x_n]$ forme un anneau dans le cas où A est un corps. Encore une fois, les seules propriétés des corps utilisées dans ce cas sont celles d'anneau unitaires commutatif, et on a donc le résultat par les arguments classiques.

■

Solution 20. Sur les entiers de Gauss

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\},$$

on a la **norme**

$$N(a + bi) := a^2 + b^2.$$

L'ensemble $\mathbb{Z}[i]$ forme un sous-anneau de $\mathbb{C}$, qui contient clairement les entiers $\mathbb{Z}$ (posant $b = 0$). En effet, pour $x = a + ib$ et $y = c + di$ dans $\mathbb{Z}[i]$, on constate que

$$\begin{aligned} x + y &= (a + c) + i(b + d), \\ x - y &= (a - c) + i(b - d), \\ xy = ac - bd + i(ad + bc) & \end{aligned}$$

qui sont bien tous de la forme $\alpha + \beta\, i$, avec α et β in $\mathbb{Z}$. De plus, $N(xy) = N(x)N(y)$ puisque

$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2)$$

Pour tout x et y dans $\mathbb{Z}[i]$, avec $y \neq 0$, il existe q et r dans $\mathbb{Z}[i]$ tels que

$$x = qy + r, \qquad \text{et} \qquad N(r) < N(y).$$

Pour le voir, on commence par calculer $q = e + fi$, où

$$e := \left[\frac{ac + bd}{c^2 + d^2}\right] \qquad \text{et} \qquad f := \left[\frac{abc - ad}{c^2 + d^2}\right],$$

avec $[\alpha]$ désignant l'entier le plus près de $\alpha \in \mathbb{R}$. Ensuite, on pose simplement $r := x - q\, y$. Il est facile de vérifier que $N(r) < N(y)$ par calcul. ■

Solution 21. Pour K un corps fini de caractéristique p et ξ un générateur de K^*, on cherche à montrer que ξ^p est aussi un générateur de K^*. La fonction $\varphi_p : K \to K$, défini par $\varphi_p(x) := x^p$ est un automorphisme de corps de K. En particulier, il induit un automorphisme du groupe multiplicatif $\varphi_p : K^* \to K^*$ qui envoie le générateur ξ sur un autre générateur $\varphi_p(\xi) = \xi^p$, puisqu'un automorphisme de groupe préserve l'ordre des éléments, et donc $\varphi(x^n) = \varphi(x)^n = 1$ si et seulement si $x^n = 1$. ■

Bibliographie

[1] F. Bergeron, P. Leroux, et G. Labelle, *Combinatorial Species and Tree-like Structures*, Encyclopedia of Mathematics, Cambridge University Press, 1998. 497 pages.
Une rééddition des premiers chapitres est disponible sur le web. C'est la théorie développée à l'UQAM, présentée pour le niveau des études avancées. Une introduction plus accessible est donnée au chapitre 6 des notes Introduction à la combinatoire algébrique. Cependant, pour l'aspect théorie de Pôlya, il faut voir la version papier complète du livre.

[2] F. Bergeron et C. Hohlweg, *Arithmétique et géométrie classique*, disponible sur le web, 2014. 262 pages.

[3] J. Calais, *Eléments de théorie des groupes*, Presses Universitaires de France, 1984. (QA174.2C25)

[4] E. Cartan, *La théorie des groupes et les recherches récentes en géométrie différentielles*, Congrès international de Mathématiques, Toronto, août 1924. Voir sur le web cette référence historique, expliquant entre autres certains liens avec la théorie de la relativité.

[5] N. Carter, *Visual Group Theory*, MAA's Classroom Ressource Material series, 2009. Disponible en version papier et électronique. Il s'accompagne d'un logiciel libre qui permet d'explorer des propriétés des groupes est disponible à l'adresse `http://groupexplorer.sourceforge.net`.

[6] C.A. Daul, *Applications de la théorie des groupes à la chimie*, disponible sur le web, pour voir en quoi la théorie des groupes intervient en chimie.

[7] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker et R. A. Wilson, *Atlas of finite groups*, Clarendon Press Oxford, 1985. (QA171A86)
C'est la compilation des résultats de la classification des groupes finis.

[8] F.M. Goodman, *Algebra : Abstract and Concrete*, Disponible sur le web. En anglais, mais très bien présenté avec un point de vue original soulignant le rôle des symétries en mathématiques.

[9] A. Kostrikin, *Introduction à l'algèbre*, Éditions MIR, 1986. (QA154.2K6714)

[10] S. Lang, *Structures algébriques*, InterEditions, 1976. (QA251L2514)

[11] F. Liret et D. Martinais, *Algèbre* 1re *année*, 2e édition, Dunod, 2003. (QA155L47.2003)

[12] J.S. Milne, *Group Theory*, 135 pages. Disponible sur le web. Un bon livre en anglais, qui porte sur la matière de cours, mais qui va plus loin sur certains sujets. Aussi avec une bonne bibliographie classique, citant les meilleures sources. Son site personnel contient aussi d'autres notes de cours sur une vaste gamme de sujets.

[13] G. Polya, *Comment poser et résoudre un problème*. Dunod, 1962. (QA11P614)
Un classique pour apprendre à réfléchir aux mathématiques, ou au moins à y penser autrement.

[14] S. Sternberg, *Group Theory and Physics*, Cambridge University Press, 1995.
Un très bon livre pour aller plus loin. C'est du niveau des études avancées.

Alphabet grec

A,	α :	alpha	N,	ν :	nu
B,	β :	bêta	Ξ,	ξ :	xi
Γ,	γ :	gamma	O,	o :	omicron
Δ,	δ :	delta	Π,	π :	pi
E,	ε :	epsilon	P,	ρ :	rhô
Z,	ζ :	dzéta	Σ,	σ, ς :	sigma
H,	η :	êta	T,	τ :	tau
Θ,	θ :	thêta	Υ,	υ :	upsilon
I,	ι :	iota	Φ,	φ :	phi
K,	κ :	êta	X,	χ :	khi
Λ,	λ :	lambda	Ψ,	ψ :	psi
M,	μ :	mu	Ω,	ω :	omega

Index

Abel, Niels H., 16
action, 50
  à gauche, 50
  ensemble d'orbites, E/G, 50
  fonctions
    composition à droite, 55
    composition à gauche, 55
    conjugaison, 55
  isomorphisme, 63
  linéaire, 75
    isomorphisme, 75
    somme, 75
  morphisme, 63
  orbite, 50
  par conjugaison, 54
  sous-ensemble invariant, 51
  sous-ensemble stable, 51
  sur un ensemble, 50
  transitive, 50
  triviale, 50, 117
action de groupe
  continue, 82
agit, 50
alphabet, 46
alterné, groupe A_n, 86
anneau, 46
  commutatif, 46
automorphisme
  intérieur, 88

bijection, 140
Burnside, William, 61

Cantor, Georg, 137
Cartan, Elie, 72
Cauchy, Augustin Louis, 61
Cayley, Arthur, 31, 89
centralisateur, 54
centralisateur, $C(H)$, 54
centre, $Z(G)$, 24
commutateur, 102
composante primaire, 122
concatenation, 46
congruence
  à droite, 56
  à gauche, 56
  classe à gauche, 56
conjugaison
  action par, 54
  classe de, 54
conjugué, 54
Coxeter, H.S.M., 38
cryptographie RSA, 66

Dedekind, Julius Wilhelm Richard, 75
dense, 47
diédral, D_m, 52
Dirichlet, Johann, 140

ensemble
  $\varnothing$, 138
  $\mathbb{C}$, 138
  $\subseteq$, 138
  de relations, 55
  différence, 138

élément, 137
ensemble vide, 138
intersection, 140
$\mathbb{N}$, 138
$\mathcal{P}(E)$, 138
paire, 138
produit cartésien, 139
$\mathbb{Q}$, 138
$\mathbb{R}$, 138
réunion, 139
singleton, 138
sous-ensemble, 138
union, 139
union disjointe, 140
$\mathbb{Z}$, 138
ensemble d'orbites, E/G, 50
ensemble quotient, G/H, 56
entiers de Gauss
norme, 155
$\mathbb{Z}[i]$, 155
espace homogène, 72
Euler, Leonhard, 66

Fermat, Pierre, 66
fixe, 51
fonction, 140
action à droite, 55
action à gauche, 55
bijection, 20
composition, 20
continue, 48
ensemble de, 20
identité, 20
inverse, 140
permutation, 20
surjective, 140
fonction d'Euler, $\varphi(x)$, 41
Frobenius, Ferdinand Georg, 61

générateur, 54

Galileo, Galilei, 49
Galois, Évariste, 11
Gauss, Carl Friedrich, 66
groupe, 16
monstre, 28
p-groupe, 123
abélien, 16
somme directe, 121
action, 50
alterné, A_n, 86
centre, $Z(G)$, 24
commutatif, 16
cyclique, 27, 103
indécomposable, 128
de Coxeter, 110
des automorphismes intérieur, $\mathrm{Int}(G)$, 88
diédral, D_m, 52
endomorphisme, 83
fini, 27
formule de l'indice, 80
général linéaire, $\mathrm{GL}(V)$, 21
général linéaire, $\mathrm{GL}_n(\mathbb{R})$, 16
générateurs, 25
groupe quotient, G/N, 98
hyperoctaédral, B_n, 118
indice d'un sous-groupe, 58
isomorphe, 84
libre, 101
monogène, 25, 103
morphisme de groupes, 83
notation additive, 18
notation multiplicative, 18
ordre, 27
ordre d'un élément, 27
orthogonal, $O(n)$, 41
primaire, 123
résoluble, 108
règles de calcul, 22
simple, 57
sous-groupe, 24

normal, 57
sous-groupe engendré, 25
sous-groupe propre, 24
spécial linéaire,SL_n, 21
spécial orthogonal, $SO(n)$, 41
symétrique, 31
symétrique, S_E et S_n, 20
table de multiplication, 21
topologique, 48

hériditaire, 16
Hamilton, William Rowan, 47
homéomorphisme, 48
homothéties, 52
hyperoctaédral
groupe, 118
hyperoctaèdre, HO_n, 118

idéal, 95
inclusion, 138
indécidable, 102
indice
d'un sous-groupe, $[G : H]$, 58
fini, 58
invariant, 51
involutions, 28
isomorphisme, 63
premier théorème d', 99

jeu de taquin, 44
Jordan, Camille, 14

Klein, Felix, 21

Lagrange, Joseph Louis, 49
langage reconnaissable, 119
lettre, 46
libre, groupe, 101
Lie, Sophus, 21
loi de composition, 15
élément inversible, 16
élément neutre, 16
associative, 15
commutative, 15
sous-ensemble stable, 16
Lorentz, Hendrik, 14

Mobius, August Ferdinand, 74
monoïde, 16
libre, 46
monstre, 28
morphisme, 63
epimorphisme, 84
automorphisme, 87
intérieur, 88
isomorphisme, 84, 87
monomorphisme, 84
noyau, $\ker(\theta)$, 85
trivial, 83
mot, 46
longueur, 46
vide, 46

Newton, Sir Issac, 77
nombre
addition, 18
complexe
racines de l'unité, 104
multiplication, 19
normal, 57
sous-groupe, 57
normalisateur, $N(H)$, 54
Novikov, Petr, 102

opération
élément inversible, 16
binaire, 15
inverse, 17
stable, 16
opère
à gauche, 50
opposé d'un élément, 18

orbite
  disjointes, 51
  partition, 51
orbite, Orb(x), 50

partage
  notation $\mu \vdash n$, 78
  part, 78
partition
  orbites disjointes, 51
permutation
  circulaire, 34
  cycle, 34
    longueur, 34
  paire, 86
  signe, $\varepsilon(\sigma)$, 33
  transposition, 34
point fixe, $\mathrm{fix}_g(E)$, 61
Polya, George, 63
polynôme
  invariant, 77
présentation, 54
présentation de groupe, 102
  générateurs, 101
  relations, 102
problème du mot, 102
produit cartésien, 139
produit direct
  externe, $G \times H$, 114
  inclusion, 114
  interne, 116
    decomposition, 116
    facteurs, 116
  projection, 114
  propriété universelle, 115
produit direct, $G \times H$, 114
produit semi-direct
  externe, 117
  interne, 117
  $K \rtimes_\varphi H$, 117

quotient de groupes
  propriété universelle, 99

réflexion, 37
Redfield, John Howard, 63
relation, 54
représentation
  dimension, 90
représentation linéaire, 75
rotation, 52
Russell, Bertrand, 138

Schutzenberger, Marcel Paul, 45
simple, groupe, 57
sous-action, 51
sous-groupe
  de Sylow, 130
  normal
    trivial, 57
  normal, $H \lhd G$, 97
sous-groupes de S_n
  nombre de, 65
  nombre de classes de conjugaison, 65
stabilisateur, Stab(x), 51
stable, 51
Sylow, Ludwig, 129

théorème
  d'isomorphisme, 99
  de Cayley, 89
  de Lagrange, 58
  de Sylow, 130
  de Wilson, 81
topologie, 48
transformation de Möbius, 74
transitive, action, 50
translation
  du plan, 52

Wilson, John, 81

Young, Alfred, 46