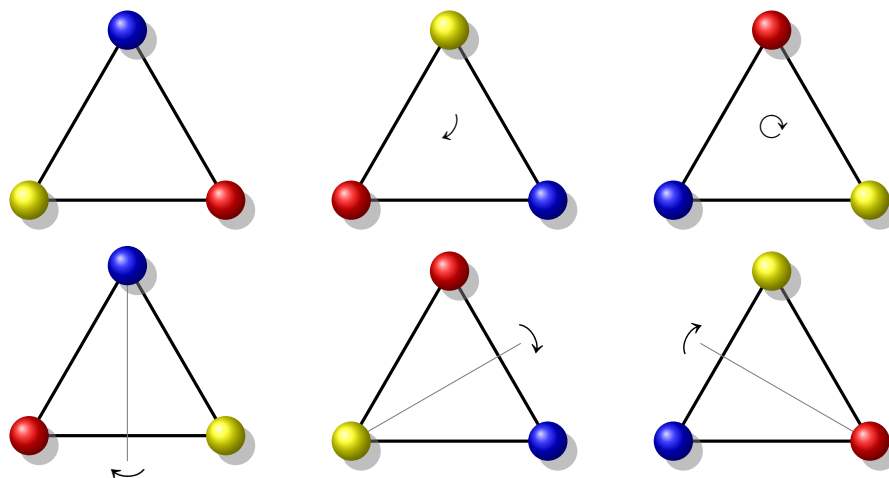


MAT 2250

Introduction à la théorie des groupes

Luc Bélair, François Bergeron et Christophe Hohlweg

22 octobre 2018



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	5
Avant-propos	6
1 Groupes	7
1.1 Lois de composition interne et monoïdes	8
1.2 Groupes	13
1.3 Sous-groupes	20
1.4 Sous-groupes engendrés par une partie d'un groupe	24
1.5 Le groupe symétrique, le groupe diédral et autres exemples	31
1.6 Une application : le système de cryptographie RSA	42
1.7 Exercices	45
2 Morphismes de groupes	57
2.1 Morphismes de groupes	57
2.2 Morphismes particuliers et théorème de Cayley	64
2.3 Sous-groupes normaux et produit semi-direct	68
2.4 Exercices	72
3 Groupes quotients et théorèmes d'isomorphisme	81
3.1 Groupes quotients	81
3.2 Théorèmes d'isomorphisme et applications	84
3.3 Présentations (finies) de groupes par générateurs et relations	87
3.4 Exercices	91
4 Actions de groupes	101
4.1 Groupe opérant sur un ensemble	102
4.2 Orbites et stabilisateurs	105

4.3	Actions transitives et classes modulo un sous-groupe	111
4.4	Formule de Burnside	113
4.5	Exercices	115
5	Les p-groupes et théorèmes de Sylow	121
5.1	Les p -groupes	121
5.2	Théorèmes de Sylow	122
5.3	Exercices	126
6	Groupes abéliens finis	129
6.1	Groupes abéliens primaires	129
6.2	Décomposition primaire	131
6.3	Théorème principal	133
6.4	Exercices	134
A	Rappels sur les ensembles et fonctions	137
A.1	Le langage ensembliste	137
A.2	Les fonctions	141
A.3	Relations d'équivalences	142
A.4	Exercices	145
B	Autres exemples d'actions de groupes	149
B.1	Actions linéaires	149
B.2	Le groupe des isométries du cube	152
B.3	A_5 comme groupe des rotations du dodécaèdre	156
B.4	Espaces homogènes	159
B.5	Le groupe $SL_2(\mathbb{Z})$	159
C	Théorie des groupes avec le calcul formel	163
	Bibliographie commentée	165
	Index	169

Table des figures

1.1	Table de multiplication	18
1.2	Deux graphes de Cayley pour S_3	31
1.3	Composition de permutations	33
1.4	Permutoèdre du groupe S_4	34
1.5	Un cycle.	35
1.6	Décomposition en cycles disjoints	37
1.7	Arrangement d'hyperplans dans \mathbb{R}_3 , correspondant à S_4	39
1.8	Réflexions et arrangement de droites	41
2.1	Isomorphisme entre les symétries du triangle et S_3	61
2.2	Graphe de Cayley de A_5	63
2.3	L'octaèdre.	71
3.1	Graphe de Cayley du groupe libre	88
4.1	Orbites dans \mathbb{C} pour les translations et rotations	109
4.2	Treillis des sous-groupes de S_4	112
4.3	Colorations du tétraèdre	114
B.1	Rotations du cube.	152
B.2	Les cinq cubes inscrits dans le dodécaèdre.	156
B.3	Rotation du dodécaèdre	156
B.4	Version réaliste d'un cube inscrit dans le dodécaèdre.	157
B.5	Permutation des 5 cubes d'un dodécaèdre	158
B.6	Pavage du plan hyperbolique	161

Avant-propos

Ce recueil est né en 2012 de la fusion de deux recueils de cours du Baccalauréat en mathématiques de l'UQAM : le premier, écrit par Luc Bélair, était conçu pour le cours MAT2000 - Algèbre 2 et le deuxième, écrit par Christophe Hohlweg en 2009, MAT1007-Algèbre 1.

Une version révisé et dynamique de ce recueil a été préparé en 2014 par François Bergeron : il y a ajouté de nombreuses illustrations, exemples, exercices avancés et des pistes d'explorations pour guider l'étudiant intéressé vers une théorie des groupes plus avancée. 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.

La présente version a été préparée par Christophe Hohlweg en 2018 ; elle constitue une réorganisation complète des notions et des exercices qui leurs sont reliés. On remercie d'avance ceux qui prendront la peine de signaler les erreurs de toute nature.

On suppose le lect.eur.rice familié.e avec les exemples classiques tels qu'entiers, réels, matrices, ainsi qu'avec la base du langage mathématique dont un rappel est fait brièvement à l'Annexe A. 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.

À la fin de chaque chapitre se trouve une liste d'exercices classés en trois catégories : les questions d'auto-évaluation, les exercices ainsi que les exercices exploratoires. Les questions d'auto-évaluation sont destinées à s'assurer de la bonne compréhension d'une méthode ou d'une définition de base vue dans le cours. **Il est donc important** de savoir faire ces exercices qui ne seront pas tout le temps corrigé durant le cours ; des solutions complètes ou partielles sont parfois fournies à titre d'auto-correction. Les exercices sont alors de niveau moyen a difficile. Les exercices exploratoires sont des exercices supplémentaires difficiles pour celles et ceux qui désirent explorer plus en avant la théorie des groupes.

C.H. tient à remercier chaleureusement Stéphanie Schanck pour la relecture de ces notes qu'elle a effectuée lors de l'automne 2016, relecture qui a grandement contribué à la qualité du document final. Il tient aussi à remercier Franco Saliola qui a eu la gentillesse de partager les exercices (et leurs solutions) pour le cours qu'il a donné en 2014.

Chapitre 1

Groupes

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

Afin de bien identifier ces différentes lois de calculs et ainsi pouvoir les définir, les exemples typiques suivants sont à garder en tête.

- (a) \mathbb{N} avec l'addition : l'addition de deux nombres entiers naturels est un nombre entier naturel ; 0 est un *élément neutre*, c'est-à-dire $0 + n = n = n + 0$ pour tout $n \in \mathbb{N}$; par contre l'équation $n + a = 0 = a + n$, où $a \in \mathbb{N}$ fixé, n'a de solution dans \mathbb{N} que si $a = 0$ car les nombres entiers négatifs ne sont pas des nombres entiers naturels.
- (b) \mathbb{Z} avec l'addition : l'addition deux deux entiers est bien entendu un entier ; 0 est encore un élément neutre et de plus l'équation $n + a = 0 = a + n$, où $a \in \mathbb{Z}$, a toujours une solution dans \mathbb{Z} qui est donnée par $n = -a$, *l'opposé* de a .
- (c) \mathbb{Z} avec la multiplication : la multiplication de deux nombres entiers est un nombre entier ; ici 1 est un élément neutre, c'est-à-dire dans ce cas que $1n = n = n1$ pour tout $n \in \mathbb{Z}$; par contre l'équation $an = 1 = na$, où $a \in \mathbb{Z}$, n'a de solution dans \mathbb{Z} que si $a \in \{\pm 1\}$ car 1 et -1 sont les seuls diviseurs de 1 dans \mathbb{Z} .
- (d) \mathbb{R}^* avec la multiplication : la multiplication de deux nombres réels non nuls est un nombre réel non nuls, le nombre 1 est un élément neutre car $1x = x = x1$ pour tout $x \in \mathbb{R}^*$ et l'équation $ax = 1 = xa$, où $a \in \mathbb{R}^*$, a toujours une solution dans \mathbb{R}^* qui est donnée par $x = a^{-1} = \frac{1}{a}$, *l'inverse* de a (cette dernière affirmation est fausse pour \mathbb{R} car on ne peut pas diviser par 0!).
- (e) $M_2(\mathbb{R})$, l'ensemble des matrices carrées 2×2 à coefficients réels, munit de la multiplication se comporte de façon similaire à \mathbb{Z} avec la multiplication : on peut multiplier deux matrices pour

obtenir une matrice ; la matrice identité I_2 est un élément neutre car $AI_2 = A = I_2A$ pour tout $A \in M_2(\mathbb{R})$ et l'équation $AX = I_2 = XA$ n'a de solution que si A est une matrice inversible et dans ce cas $X = A^{-1}$, la matrice inverse de A . On notera ici que la multiplication n'est pas commutative et donc la commutativité est une propriété supplémentaire à considérer.

On va introduire ici de nouveaux objets mathématiques qui vont illustrer les propriétés générales de ces opérations, en se détachant du particulier. Parmi les opérations, 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 quelles sont les propriétés qui donnent à une opération 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.

1.1 Lois de composition interne et monoïdes

Dans la suite du texte, on suppose que E est un ensemble non vide.

Lois de composition interne et magmas. On dit d'une fonction $* : E \times E \rightarrow E$ qu'elle est une **loi de composition interne sur E** . Le couple $(E, *)$ est alors appelé un **magma**. Si $(E, *)$ est un magma, on note $x * y$ l'image de (x, y) par la fonction $* : E \times E \rightarrow E$.

On dit d'une loi de composition de composition $*$ 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.** (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 identifié¹ à $\{0, 1, \dots, n\}$.
- (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

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

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

1. C'est un léger abus de langage qui sera rediscuté au Chapitre 3.1.

- (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 aussi l'exercice 1.10).
- (e) La paire $(\text{Fonct}(E), \circ)$ composée de l'ensemble des fonctions sur E et de la composition des fonctions forme un magma et la loi « \star » est associative.

Si il n'y a pas de risque de confusion quant à la loi de composition utilisée, on note par abus de notation E à la place de (E, \star) . Bien entendu, pour \mathbb{Z} par exemple il faut préciser $(\mathbb{Z}, +)$ (\mathbb{Z} munit de l'addition) ou (\mathbb{Z}, \cdot) (\mathbb{Z} munit de la multiplication).

Restriction des lois de composition interne aux sous-ensembles. Soit \star une loi de composition interne sur E et $A \subseteq E$ non vide. On dit que l'ensemble A est **stable sous \star** , si pour tout $x, y \in A$ on a $x \star y \in A$. La structure algébrique (A, \star) est appelée un *sous-magma*.

On dit alors que **\star restreinte² à A est une loi de composition interne sur A** . On dit aussi que **A hérite de la loi de E** .

Autrement dit, \star est aussi une loi de composition interne sur A par restriction de \star à A car la fonction

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

est bien définie.

Exemples. (a) Considéré comme sous-ensembles 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 $1 + (-1) = 0 \notin \mathbb{Z}^*$.

(b) La chaîne d'inclusion est suivante est formée de sous-ensemble stable à la fois pour la multiplication et l'addition sur chacun des ensembles dans lequel il est contenu : $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Il est agréable qu'un sous-ensemble soit stable par une loi de composition car comme l'illustre le résultat suivant.

Proposition 1.1. *Soit (E, \star) un magma et A est un sous-ensemble de E stable sous \star .*

1. *L'associativité est héréditaire : si \star est associative sur E alors \star restreinte à A est associative sur A .*
2. *La commutativité est héréditaire : si \star est commutative sur E alors \star restreinte à A est commutative sur A .*

2. Rigoureusement parlant, on devrait dénoter $\star|_{A \times A}$ et parler de la restriction de \star à $A \times A$, mais il n'y a pas risque de confusion.

Démonstration. (1) L'égalité $x * (y * z) = (x * y) * z$ est vraie pour tout $x, y, z \in E$, donc en particulier pour tout $x, y, z \in A$. (2) L'égalité $x * y = y * x$ est vraie pour tout $x, y \in E$, donc en particulier pour tout $x, y \in A$. ■

Éléments neutre et monoïdes. Tout comme c'est le cas de 1 pour la multiplication sur \mathbb{R} , ou de 0 pour l'addition sur \mathbb{R} , plusieurs opérations admettent des « éléments neutres ». Soit $(E, *)$ un magma. 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 $x \in E$; .

Définition. Un **monoïde** est un magma $(E, *)$ associatif et qui possède un élément neutre $e \in E$. Un monoïde est dit **commutatif** si l'opération est de plus commutative.

Exemples. (a) (\mathbb{N}^*, \cdot) est un monoïde dont l'élément neutre est 1, par contre le magma associatif $(\mathbb{N}^*, +)$ n'est pas un monoïde car l'élément neutre 0 de l'addition n'est pas un élément de \mathbb{N}^* .
 (b) L'ensemble des matrices $M_n(\mathbb{R})$ munit de la multiplication ou de l'addition est dans chaque cas un monoïde.

Proposition 1.2. *Si $(E, *)$ possède un élément neutre e , alors cet élément neutre est **unique**. De plus, si $A \subseteq E$ est stable sous $*$ et $e \in A$, alors e est élément neutre pour $(A, *)$. La paire $(A, *)$ est alors aussi un monoïde qui est appelé alors un **sous-monoïde** de $(E, *)$.*

Démonstration. Soit e et e' deux éléments neutre pour $*$, alors $e = e * e' = e' * e = e'$, et donc $e = e'$. Le deuxième énoncé est une conséquence directe de l'unicité et de la définition d'élément neutre. ■

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 dans un monoïde. Une question naturelle à se poser est : par quels éléments peut-on « diviser » dans le monoïde E ? Par exemple : dans le monoïde \mathbb{R} avec la multiplication, on peut diviser par tous les éléments sauf 0 ; dans le monoïde des fonctions sur un ensemble, on peut seulement « diviser » par les bijections, aussi appelées fonctions inversibles.

Définition. On dit que $x \in E$ est **inversible** dans le monoïde $(E, *)$ s'il existe $\tilde{x} \in E$ tel que $x * \tilde{x} = e = \tilde{x} * x$. On note par E^\times **l'ensemble des éléments inversibles** de E :

$$E^\times := \{x \in E \mid x \text{ est inversible}\}. \quad (1.1)$$

L'un des intérêts d'avoir un ou des éléments inversibles dans E est le suivant. Si $x \in E$ est inversible, alors on peut « diviser » une équation par x : pour $b \in E$, la solution de l'équation $x * y = b$ dans E

est :

$$y = e * y = (\tilde{x} * x) * y = \tilde{x} * (x * y) = \tilde{x} * b.$$

Un calcul similaire montre aussi que si x est inversible, l'élément \tilde{x} tel que $x * \tilde{x} = e = \tilde{x} * x$ est unique. On note $x^{-1} = \tilde{x}$ cet unique élément et on l'appelle **l'inverse de x dans E** .

Exemples. (a) Dans $(\mathbb{Z}, +)$, l'inverse de x est $-x$. Dans (\mathbb{Q}^*, \cdot) , l'inverse de x est $1/x$.

(b) On remarque facilement aussi que dans le monoïde $(\text{Fonct}(E), \circ)$, les éléments inversibles sont précisément les fonction inversibles sur E définie par l'Équation A.1 : $S_E = \text{Fonct}(E, E)^\times$.

(c) Dans un premier cours d'algèbre linéaire, on montre aussi que cette équation définit le fait d'être une matrice inversible pour la multiplication de matrices (ce qui est équivalent à montrer que son déterminant est non nul). On désigne habituellement par $\text{GL}_n(\mathbb{R})$ l'ensemble des matrices réelles de déterminant non nul et on $GL_n(\mathbb{R}) = M_n(\mathbb{R})^\times$.

Remarque. Une autre façon de concevoir la division de nombres x/y dans \mathbb{R}^* (resp. la soustraction $x - y$ dans \mathbb{Z}) et donc 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 $-y$).

On laisse le lecteur vérifier le résultat suivant.

Proposition 1.3. *On a $e^{-1} = e$ et, si $x, y \in E^\times$, alors $(x^{-1})^{-1} = x$ et $(x * y)^{-1} = y^{-1} * x^{-1}$. En particulier, $e, x^{-1} \in E^\times$ et E^\times est un sous-monoïde de E .*

Attention, comme le monoïde n'est pas forcément commutatif, on a en général

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

sinon $x * y = y * x$ car $(x^{-1})^{-1} = x$.

Conventions d'écriture et règles de calcul dans un monoïde. 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 E est un « monoïde » (sans mentionner la loi de composition interne), au lieu de $(E, *)$.

Sauf mention contraire, on note habituellement les opérations de monoïdes **multiplicativement** : $(x, y) \mapsto xy$ (au lieu de $(x, y) \mapsto x * y$), et on dit que ce sont des **produits**³ et l'élément neutre est noté 1_E , 1 ou e .

Dans le cas spécial où le monoïde $(E, *)$ est commutatif, on utilise souvent une **notation additive** afin de noter cette loi de composition interne : $(x, y) \mapsto x + y$ (au lieu de $(x, y) \mapsto x * y$), et on dit que ce sont des **sommes** ; l'élément neutre est noté 0_E ou 0 .

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

La plupart des habitudes de calcul que nous avons avec l'addition ou la multiplication sont transposables au calcul dans les monoïdes. Il faut toutefois bien faire attention dans les monoïdes non-commutatifs.

Soit $(E, *)$ un monoïde. Soit $x \in E$ et $n, m \in \mathbb{N}$ alors l'associativité de la loi $*$ permet de définir récursivement le produit x^n comme suit :

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

où e désigne l'élément neutre du monoïde. En **notation additive**, c'est-à-dire, si la loi est noté $+$, on a plutôt :

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

De plus, on montre facilement (par récurrence) que

$$x^n x^m = x^{n+m}, \quad (\text{ou encore } n \cdot x + m \cdot x = (n+m) \cdot x \text{ en notation additive}). \quad (1.2)$$

Attention, si le groupe G n'est pas commutatif, $(xy)^n \neq x^n y^n$. Comme x et y ne commutent pas nécessairement, on peut seulement affirmer que

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

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 $-(n \cdot x) = (-n) \cdot x$ (en particulier on note $-x$ l'inverse additif de x). On vérifie alors que, pour tout $m, n \in \mathbb{Z}$, on a encore la règle des exposants (1.2) (de même pour la version additive).

Proposition 1.4. (a) Soit $x \in E$ inversible et $n \in \mathbb{Z}$, alors $x^{-n} = (x^n)^{-1}$.

(b) Si $x_1, \dots, x_n \in E^\times$ alors $(x_1 * \cdots * x_n)^{-1} = x_n^{-1} * \cdots * x_1^{-1}$. En particulier, $x_1 * \cdots * x_n \in E^\times$.

Démonstration. Pour (1), on vérifie aisément que $x^{-n}x^n = e = x^n x^{-n}$, d'où le résultat. Pour (2) on procède par récurrence sur $n \in \mathbb{N}^*$. Le cas $n = 1$ est évident. Supposons maintenant que $(x_1 * \cdots * x_{n-1})^{-1} = x_{n-1}^{-1} * \cdots * x_1^{-1}$. En posant $x = x_1 * \cdots * x_{n-1}$ et $y = x_n$ dans l'énoncé de la proposition 1.3 on conclut que :

$$(x_1 * \cdots * x_{n-1} * x_n)^{-1} = (x * y)^{-1} = y^{-1} * x^{-1} = x_n^{-1} * x_{n-1}^{-1} * \cdots * x_1^{-1}.$$



1.2 Groupes

Un monoïde dans lequel « on peut diviser » par tous les éléments est appelé un groupe.

Définition. On dit que (G, \cdot) (ou tout simplement G) est **un groupe** si (G, \cdot) est un monoïde, et si tous les éléments de G sont inversibles. Un groupe G est dit **abélien**⁴, ou **commutatif**, si de plus la loi de composition interne sur G est commutative.

En d'autre terme, pour montrer qu'un magma G est une groupe, il faut montrer que :

- (i) sa loi de composition interne est associative ;
- (ii) que G admet un élément neutre pour cette loi ;
- (iii) que tous les éléments sont inversibles pour cette loi.

Par exemple, $(\mathbb{Z}, +)$ et (\mathbb{Q}^*, \cdot) sont des groupes abéliens, mais $(\text{GL}_n(\mathbb{R}), \cdot)$ ne l'est pas. Par exemple, dans $\text{GL}_2(\mathbb{R})$, 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

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

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

Proposition 1.5. *Soit E un monoïde⁵ dont l'élément neutre est e . Alors E^\times est un groupe dont l'élément neutre est e . En particulier, E est un groupe si et seulement si $E = E^\times$.*

Démonstration. Il faut montrer que

- (1) \cdot est une loi de composition interne sur E^\times ; en d'autres termes, que E^\times est stable pour \cdot ;
- (2) (E, \cdot) est un monoïde d'élément neutre e ;
- (3) Tout élément de E^\times est inversible.

Ces trois énoncés sont une reformulation directe de la proposition 1.3. ■

Définition. 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 .

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

5. On rappelle que l'on écrit E à la place de (E, \cdot) si le contexte est clair.

1.2.1 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. On invite le lecteur à vérifier toutes ces affirmations en exercice.

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. 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 $n = 1$.

Ensembles quotients $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. 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 fini d'ordre n .

- (b) (\mathbb{Z}_n, \cdot) est un monoïde commutatif, mais pas un groupe.
- (c) $(\mathbb{Z}_n^\times, \cdot)$ est un groupe abélien fini d'ordre $\varphi(n)$, l'indicatrice d'Euler de n (le nombre d'entier inférieur à n est premier avec n).

Algèbre linéaire. Les groupes apparaissent naturellement en algèbre linéaire. Par exemple, 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 matrices 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 1.5, $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ est un groupe. On l'appelle le **groupe linéaire**. Il est non abélien si $n > 1$. De plus, $(AB)^{-1} = B^{-1}A^{-1}$ (attention, ici l'ordre de multiplication est important, car la loi de composition interne n'est pas commutative).

Soit E un espace vectoriel en général. Alors E est un groupe abélien pour l'addition de vecteurs (voir Exercice 1.7). De plus, l'ensemble des applications linéaires bijectives sur E , noté $\mathrm{GL}(E)$, est un sous-ensemble de S_E . Comme la composée d'applications linéaires est linéaire, on 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 applications linéaires de \mathbb{R}^n vers \mathbb{R}^n , ayant déterminant 1. Ce sont des exemples de **Groupes de Lie**⁶.

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

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

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 les proportions sur une droite, etc. La géométrie affine correspond à étudier les théorèmes qui restent « invariants »⁷ par transformations affines. Ainsi, parce que les concepts intervenants dans son énoncé sont préservés par les transformations affines, on peut ramener

6. **Sophus Lie** (1842–1899).

7. Il y a une notion mathématique précise, que nous ne présentons pas ici.

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**.

1.2.2 Le groupe symétrique, première partie

En tant que groupes de fonctions inversibles, les groupes symétriques jouent un rôle fondamental en mathématiques. Nous allons discuter leur exemple un peu plus en détail.

Fonctions et bijections. On rappelle désigne par $\text{Fonct}(E, E)$ l'ensemble des fonctions de E vers E . Observons que cet ensemble est toujours non vide, même si E est vide⁸. 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 que

$$S_E = (\text{Fonct}(E, E))^\times. \quad (1.3)$$

On dit aussi de σ dans S_E que c'est une **permutation** de E . Puisque la composition est une loi de composition interne associative sur $\text{Fonct}(E, E)$ (voir Exercice 1.5), il s'ensuit que $(\text{Fonct}(E, E), \circ)$ est un monoïde (non commutatif en général). La fonction **identité** Id_E , telle que $\text{Id}_E(x) := x$, est l'élément neutre dans $(\text{Fonct}(E, E), \circ)$. C'est donc que $(\text{Fonct}(E, E), \circ)$ 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 $S_{\{1, \dots, n\}}$. Les éléments de S_n sont souvent appelés **permutations** et jouent un rôle important en mathématique.

Ordre d'un groupe symétrique. Considérons plus en détail le groupe symétrique S_E , des permutations d'un ensemble E de cardinal n . Commençons par calculer son ordre.

Proposition 1.6. *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. Il est bien connu que le nombre de permutation de l'ensemble $[n]$, c'est-à-dire le cardinal de S_n , est $n!$ On montre l'énoncé plus général de la proposition par récurrence sur n . Si $n = 1$ il y a une et une seule fonction $E = \{x\} \rightarrow F = \{y\}$, qui est clairement bijective. Donc

8. Il y a une et une seule fonction de \emptyset vers \emptyset , et c'est une bijection.

$\mathcal{B}(E, F) = 1 = 1!$ dans ce cas. Supposons maintenant la propriété vraie pour $n - 1 \geq 1$: si E' et F' sont deux ensembles de cardinal $n - 1$, alors $|\mathcal{B}(E', F')| = (n - 1)!$. Soit $x \in E$. Alors, pour tout $y \in F$, on a $|E \setminus \{x\}| = |F \setminus \{y\}| = n - 1$. Donc par récurrence, $|\mathcal{B}(E \setminus \{x\}, F \setminus \{y\})| = (n - 1)!$ pour tout $y \in F$. Si $\alpha \in \mathcal{B}(E \setminus \{x\}, F \setminus \{y\})$ alors la fonction $f : E \rightarrow F$ telle que $f|_{E \setminus \{x\}} = \alpha$ et $f(x) = y$ est une bijection de E dans F (à vérifier). Donc pour tout $y \in F$, il y a $(n - 1)!$ bijection de E dans F tel que $f(x) = y$. C'est-à-dire que l'ensemble $A_y = \{f \in \mathcal{B}(E, F) \mid f(x) = y\}$ 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 la proposition s'ensuit pour tout $n \in \mathbb{N}^*$. ■

Écriture des permutations de S_n . La proposition ci-dessus suggère que l'on va pouvoir ramener l'étude du groupe symétrique sur un ensemble de cardinal n à celui du groupe S_n . Au lieu d'écrire les permutations de S_n comme des bijections, ce qu'elles sont, on simplifie l'écriture en les représentant par des matrices $2 \times n$. Ainsi, pour $\sigma \in S_n$, on note

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

Cette écriture se simplifie en écrivant sous forme de mots la deuxième ligne de la matrice : $\sigma = \sigma(1)\sigma(2)\dots\sigma(n)$. 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)

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} &= 123, & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} &= 213, & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} &= 132, \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} &= 321, & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} &= 231, & \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} &= 312. \end{aligned}$$

1.2.3 Table de multiplication

. 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 .

On peut donc facilement représenter la loi de composition interne sur S_3 par sa table de multiplication :

	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

Cette table nous permet d'observer plusieurs des propriétés du groupe S_3 . Par exemple, 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 : l'inverse de l'élément x est y si l'intersection de la ligne x avec la colonne y est e .

Remarque. On utilise généralement la table de multiplication pour décrire un (petit) groupe fini en donnant la liste de ces éléments, puis en donnant explicitement sa table de multiplication (en s'assurant qu'elle respecte l'associativité). Bien entendu, ce n'est pas pratique dès que le groupe est grand (essayer déjà S_4 de cardinal 24 pour vous en rendre compte). On développera dans la suite d'autres outils (tel les générateurs et relations) afin de pouvoir écrire facilement de « gros » groupes.

Ainsi, on peut parler du groupe G dont les éléments sont

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

avec la multiplication donnée par la table de la figure 1.1.

	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 1.1 – La table de multiplication du groupe G .

1.2.4 Produits directs de groupes

. On peut aussi construire de nouveaux exemples de groupes en utilisant le produit cartésien d'ensembles. Pour deux groupes G, H , on considère sur le produit cartésien

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

munit de la loi de composition interne suivante :

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

L'élément neutre est (e_G, e_H) , et l'inverse se calcule comme suit :

$$(g, h)^{-1} = (g^{-1}, h^{-1}).$$

En effet, on vérifie que :

$$\begin{aligned} (g, h) \cdot (e, e) &= (ge, he) = (g, h) \\ (e, e)(g, h) &= (eg, eh) = (g, h) \\ (g, h) \cdot (g^{-1}, h^{-1}) &= (gg^{-1}, hh^{-1}) = (e, e) \\ (g^{-1}, h^{-1}) \cdot (g, h) &= (g^{-1}g, h^{-1}h) = (e, e). \end{aligned}$$

L'associativité se vérifie aussi de même façon.

Définition. Le groupe $G \times H$ munit de celle loi de composition externe est appelé le **produit direct de G et H** (ou **produit direct externe**).

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 nk . On observe que la table de multiplication du **groupe de Klein** $\mathbb{Z}_2 \times \mathbb{Z}_2$ (d'ordre 4) n'est pas semblable à celle de \mathbb{Z}_4 . En effet, dans $\mathbb{Z}_2 \times \mathbb{Z}_2$ tous les éléments sont des involutions (c'est-à-dire qu'ils vérifient $g^2 = e$), ce qui n'est pas le cas dans \mathbb{Z}_4 .

La construction du produit direct se généralise aisément à plusieurs facteurs. Ainsi, pour n groupes G_1, \dots, G_n , on a le produit direct de groupes $G_1 \times \dots \times G_n$ avec l'opération

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) := (x_1 y_1, x_2 y_2, \dots, x_n y_n) \quad (1.4)$$

On écrit aussi parfois $\prod_{i=1}^n G_i$, pour ce produit.

Proposition 1.7. *Le produit cartésien $\prod_{i=1}^n G_i = G_1 \times G_2 \times \dots \times G_n$ des groupes G_1, \dots, G_n munit de la loi de composition de l'équation 1.4 est un groupe dont l'élément neutre est $(e_{G_1}, \dots, e_{G_n})$ et l'inverse de $(g_1, \dots, g_n) \in \prod_{i=1}^n G_i$ est $(g_1^{-1}, \dots, g_n^{-1})$. De plus, si les groupes G_1, \dots, G_n sont finis, alors $|\prod_{i=1}^n G_i| = \prod_{i=1}^n |G_i|$.*

Démonstration. La proposition se déduit aisément du cas de deux groupes traité ci-dessus avec l'aide d'une récurrence sur $n \in \mathbb{N}^*$. ■

1.3 Sous-groupes

On a vu jusqu'ici la définition de groupes, des premiers exemples ainsi que des règles de calculs classiques. Voyons maintenant la notion de sous-groupes qui nous sera très utile afin de construire des exemples plus nombreux de groupes, mais aussi afin de nous donner des outils d'étude pour les groupes.

Soit G un groupe d'élément neutre e . On a vu précédemment que pour montrer que (H, \cdot) est un groupe, pour H un sous-ensemble de G , il suffisait de montrer que H est stable pour la loi de composition interne de G , contient le neutre e de G , et que les inverses des éléments de H sont aussi dans H . Ceci suggère la définition suivante.

Définition. Un ensemble $H \subseteq G$ est un **sous-groupe** de G si il vérifie les conditions suivantes : (i) H est non vide ; (ii) H est un sous-ensemble stable de (G, \cdot) ; (iii) $x^{-1} \in H$ pour tout $x \in H$.

Si H est un sous-groupe de G , on écrit $H \leq G$. Un sous-groupe différent de G et de $\{e\}$ est dit **sous-groupe propre**.

Remarque. On voit facilement que $H = \{e\}$ et G sont des sous-groupes de G . Pour montrer que H est non vide, il suffit souvent de montrer qu'il contient l'élément neutre e de G .

Pour montrer qu'un ensemble est un groupe, il est souvent plus facile de montrer que c'est un sous-groupe d'un groupe déjà connu.

Proposition 1.8. Soit $H \leq G$, alors (H, \cdot) est un groupe d'élément neutre e .

Démonstration. L'ensemble H est non vide en vertu de la condition (i). Maintenant, en vertu de (ii) et (iii), si $x \in H$ alors $x^{-1} \in H$ et $e = xx^{-1} \in H$. Donc (H, \cdot) est un monoïde d'élément neutre e . Comme tous les éléments de H sont inversibles, $H^\times = H$ et on conclut grâce à la Proposition 1.5. ■

Bien entendu, tout le vocabulaire valide pour un groupe s'applique en vertu de la proposition ci-dessus aux sous-groupes. Par exemple, l'ordre d'un sous-groupe est son cardinal.

Exemple. (a) On a les (chaînes de) sous-groupes suivants :

$$\begin{aligned} (n\mathbb{Z}, +) &\leq (\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +); \\ (\mathbb{Q}^*, \cdot) &\leq (\mathbb{R}^*, \cdot) \leq (\mathbb{C}, \cdot). \end{aligned}$$

De plus, pour tout espace vectoriel E , $\text{GL}(E) \leq S_E$.

(b) Pour un groupe G , l'ensemble

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

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 $x, y \in Z(G)$ 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

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

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

On rappelle ici un résultat connu concernant le groupe additif \mathbb{Z} .

Proposition 1.9. *Les seuls sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$, pour $n \in \mathbb{N}$.*

Démonstration. Voir exercice 1.11. ■

Le premier énoncé ci-dessous donne un critère très utile et équivalent à celui donné dans la définition afin de montrer qu'un sous-ensemble est un sous-groupe.

Proposition 1.10. *Soit G un groupe.*

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

Démonstration. Voir exercice 1.12. ■

1.3.1 Classes modulo un sous-groupe

On va maintenant montrer qu'on peut se servir d'un sous-groupe de G afin de décomposer G en une union disjointe de sous-ensembles de même cardinal. Pour cela, on va s'inspirer de la relation de congruence modulo n dans \mathbb{Z} (c'est-à-dire modulo le sous-groupe $n\mathbb{Z}$ de \mathbb{Z}) :

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

Réinterprétant cette relation multiplicativement (elle est notée additivement ci-dessus), on considère la définition qui est donnée dans la proposition suivante.

Proposition 1.11. Soit H sous-groupe d'un groupe G , la **congruence à gauche modulo H sur G** , définie par

$$g_1 \equiv g_2 \pmod{H} \iff g_1^{-1}g_2 \in H \iff g_1H = g_2H. \quad (1.5)$$

est une relation d'équivalence. De plus :

1. les classes d'équivalence sont de la forme $xH := \{xh \mid h \in H\}$;
2. l'ensemble quotient de cette relation d'équivalence forme une partition de G .

Démonstration. Le fait que H soit un sous-groupe assure que la relation \equiv , définie en (1.5), est bien une relation d'équivalence. En effet la réflexivité découle du fait 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 $y \equiv x$. La transitivité est une conséquence 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

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

Il reste donc à montrer que la classe d'équivalence de x est bien $xH = \{xh \mid h \in H\}$. 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. ■

Définition. Soit G un groupe et H un sous-groupe de G . La classe d'équivalence

$$xH := \{xh \mid h \in H\}, \quad \text{pour } x \in G,$$

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

$$G/H := \{gH \mid g \in G\}. \quad (1.6)$$

Remarque. (a) $xH = H$ si et seulement si $x \in H$.

(b) xH n'est pas un sous-groupe de G en général. En fait $xH \leq G$ si et seulement si $x \in H$.

(c) 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 $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

(d) Observons 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

$$xH = yH \iff x^{-1}yH = H \iff y^{-1}xH = H \iff x^{-1}y \in H. \quad (1.7)$$

(e) 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 $Hx = \{hx \mid h \in H\}$. 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

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

(f) Pour G est abélien, les deux notions de classes à gauche et à droite coïncident, c.-à-d. que $xH = Hx$ pour tout $x \in G$.

Exemple. On considère $G = S_3$ et $H = \langle (12) \rangle$ alors :

$$G/H = \{H = (12)H; (23)H = (132)H; (13)H = (123)H\} \quad \text{et}$$

$$H \backslash G = \{H = H(12); H(23) = H(123); H(13) = H(132)\}.$$

Comme $(23)H = \{(23), (132)\} \neq \{(23), (123)\} = H(23)$, les classes à gauche et à droite ne sont pas égales. Observons que le cardinal de chaque classe (à droite ou à gauche) est égal $|H|$.

Une propriété importante des classes à gauche (ou à droite), observée dans l'exemple précédent, est soulignée par la proposition suivante.

Proposition 1.12. *Soit G un groupe et $H \leq G$, alors*

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

Démonstration. 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 $f : G/H \rightarrow H \backslash G$ 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 $f(x^{-1}H) = H(x^{-1})^{-1} = Hx$. ■

1.3.2 Théorème de Lagrange

On va démontrer dans cette section un résultat très important en théorie des groupes finis : le cardinal d'un sous-groupe divise toujours le cardinal du groupe.

Définition. Pour tout H sous-groupe d'un groupe G , le cardinal de l'ensemble quotient G/H (qui est égal au cardinal de $H \setminus G$) est appelé **l'indice** de H dans G . On le note

$$[G : H] := |G/H| \quad (1.8)$$

Lorsque G/H est un ensemble fini, on dit que H est **d'indice fini** dans G .

Par exemple, on a $[\mathbb{Z} : n\mathbb{Z}] = n$.

Théorème 1.13 (Théorème de Lagrange). *Soit G un groupe fini et $H \leq G$ alors*

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

En particulier, l'ordre de tout sous-groupe 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

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

car $|H| = |xH|$ pour tout $x \in G$ en vertu de la Proposition 1.12. ■

Exemples. (a) Les sous-groupes de S_3 peuvent être de cardinal 1, 2, 3, 6 qui sont les seuls diviseurs de $6 = |S_3|$. Il se pourrait qu'il n'existe pas de sous-groupe d'ordre un diviseur donnée d'un groupe, cette question sera la motivation pour les théorèmes de Sylow dans le Chapitre 5.

(b) Les seuls sous-groupes d'un groupe G d'ordre p un nombre premier sont de cardinal 1 (le sous-groupe réduit à l'élément neutre) et G tout entier.

(c) Il existe des groupes d'ordre n qui ne contiennent pas de sous-groupes de cardinal m pour un diviseur donné m de n ; voir l'exercice 2.30 dans le chapitre suivant.

1.4 Sous-groupes engendrés par une partie d'un groupe

Les espaces vectoriels peuvent être décrit de façon « minimale » en donnant une base de l'espace vectoriel et en disant que l'espace vectoriel est engendré par sa base. Nous allons présenter une notion analogue pour les groupes. Par exemple, si on considère le groupe \mathbb{Z} , avec l'addition, tout élément s'écrit sous la forme

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

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 1.9.

1.4.1 Partie génératrice d'un groupe

Définition. 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 . Ce sous-groupe de G (proposition 1.10) est appelé **sous-groupe de G 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 .

Proposition 1.14. Soit G un groupe et $S \subseteq G$. Dans $\mathcal{P}(G)$ ordonné par l'inclusion, $\langle S \rangle$ est le plus petit sous-groupe de G contenant S . En particulier, si $A \subseteq G$ tel que $A \subseteq \langle S \rangle$, alors $\langle A \rangle \subseteq \langle S \rangle$. En particulier si $G = \langle A \rangle$, alors $G = \langle S \rangle$.

Démonstration. Il faut montrer que $\langle S \rangle$ est le plus petit élément dans l'ensemble $\Lambda = \{H \in \mathcal{P}(G) \mid H \leq G, S \subseteq H\}$. Par définition

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

Si $K \in \Lambda$, alors K apparaît dans l'intersection de tous les sous-groupes de G qui contiennent S . En d'autres termes, $\langle S \rangle \subseteq K$. 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 . On laisse le soin au lecteur de vérifier le dernier énoncé en appliquant ce qui précède. ■

Exemples. (a) Le **sous-groupe trivial**, c'est-à-dire le sous-groupe $\{e\}$ réduit à l'élément neutre de G , est le plus petit sous-groupe contenant l'ensemble vide. Donc $\langle \emptyset \rangle = \{e\}$.

(b) On a aussi clairement $\langle G \rangle = G$.

Générateurs et mots. La définition ensembliste de partie génératrice que nous avons donné a beaucoup d'avantage car elle fait intervenir l'inclusion, la relation d'ordre sur l'ensemble des parties de G . Par contre, elle ne fait pas apparaître de système d'écriture des éléments du sous-groupe en fonction de ses générateurs. Ceci est l'objet du paragraphe suivant.

Soit S un ensemble et on considère alors une copie de S que l'on note $S^{-1} = \{s^{-1} \mid s \in S\}$. On appelle $A_S = S \sqcup S^{-1}$ un **alphabet**, et ses éléments des **lettres**, et on considère l'ensemble A_S^* des **mots sur l'alphabet A_S** , c'est-à-dire, l'ensemble des listes (a_1, \dots, a_k) où $a_i \in A_S$. On note un mot $a_1 \dots a_k$ au lieu de (a_1, \dots, a_k) . Si G est un groupe avec un loi \cdot et $S \subseteq G$, alors $S^{-1} \subseteq G$ et on associe au mot $a_1 \dots a_n$ le produit $a_1 \cdot \dots \cdot a_n$ des éléments a_i de G . Rappelons qu'un produit vide ($n = 0$) est égal à 1, et qu'une somme vide est égale à 0.

Définition. Soit G un groupe et $S \subseteq G$. On dit qu'un élément $g \in G$ est **représenté par le mot $a_1 \dots a_n$ sur l'alphabet A_S** si $g = a_1 \dots a_n$. Bien entendu e est le produit vide.

La proposition suivante produit une définition alternative et constructive d'un sous-groupe engendré.

Proposition 1.15. Soit G un groupe et $S \subseteq G$, alors $\langle S \rangle$ est l'ensemble des éléments de G représenté par les mots sur l'alphabet $S \sqcup S^{-1}$. Plus précisément :

$$\langle S \rangle = \{e, a_1 \dots a_n \mid n \in \mathbb{N}, a_i \in S \text{ ou } a_i^{-1} \in S, \text{ pour tout } 1 \leq i \leq n, n \in \mathbb{N}\}.$$

En notation additive, on a

$$\langle S \rangle = \{0, a_1 + \dots + a_n \mid n \in \mathbb{N}, a_i \in S \text{ ou } -a_i \in S, \text{ pour tout } 1 \leq i \leq n\}.$$

Démonstration. Soit $S \neq \emptyset$. Posons $H = \{e, a_1 \dots a_n \mid n \in \mathbb{N}^*, a_i \in S \text{ ou } a_i^{-1} \in S \text{ pour tout } 1 \leq i \leq n\}$. On remarque que $S \subseteq H$ et si $s \in S$ alors $e = ss^{-1} \in H$. Soit $y = y_1 \dots y_n$ et $z = z_1 \dots z_m$ des éléments de H , où $y_i, z_j \in S$ ou $z_i^{-1}, z_j^{-1} \in S$. Alors $yz^{-1} = y_1 \dots y_n z_m^{-1} \dots z_1^{-1}$.

Puisque $y_i z_j \in S$ ou $z_i^{-1}, z_j^{-1} \in S$, yz^{-1} est bien le produit d'élément de S ou de leurs inverses. Ainsi $yz^{-1} \in H$. On en déduit en vertu de la proposition 1.10 que $H \leq G$, d'où $H \in \Lambda$. En vertu de (1) on sait donc que $\langle S \rangle \subseteq H$. Montrons maintenant l'inclusion inverse. Soit $K \in \Lambda$ et $g = a_1 \dots a_n \in H$ avec $a_i \in S \subseteq K$ ou $a_i^{-1} \in S \subseteq K$. Donc, puisque K est un groupe, $a_i = (a_i^{-1})^{-1} \in K$ pour tout $1 \leq i \leq n$. D'où $g = a_1 \dots a_n \in K$. 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 la proposition 1.14. ■

Définition. Lorsque $S = \{s\}$, alors on dénote plus simplement⁹ par $\langle s \rangle$ le sous-groupe engendré par $s \in G$. Si $G = \langle s \rangle$ on dit que G est **monogène**.

Exemples.

- (a) $\mathbb{Z} = \langle 1 \rangle$ est un groupe monogène pour l'addition. En effet, si $n \in \mathbb{Z}$ est positif, alors $n = \underbrace{1 + 1 + \dots + 1}_{n \text{ fois}}$; et si $n \in \mathbb{Z}$ est négatif, on a $n = \underbrace{(-1) + (-1) + \dots + (-1)}_{|n| \text{ fois}}$.
- (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 $321 = \tau_1 \tau_2 \tau_1 = \tau_2 \tau_1 \tau_2$; $312 = \tau_2 \tau_1$ et $231 = \tau_1 \tau_2$. 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, $\tau_2 = \tau_1 \sigma$, $321 = \sigma \tau_1$ et $\sigma = \sigma^2 = \sigma^{-1}$.
- (f) On peut aussi vérifier, on va le montrer dans la section suivante, que $S_4 = \langle \tau_1, \tau_2, \tau_3 \rangle$ où $\tau_1 = 2134$, $\tau_2 = 1324$ et $\tau_3 = 1243$.

Remarque. 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**. Nous verrons dans le chapitre suivant comment identifier ces relations afin de s'en servir pour d'étudier les

9. Au lieu d'écrire $\langle \{s\} \rangle$.

groupes grâce à des générateurs bien choisis. 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).

Proposition 1.16. *Soit $G = \langle x \rangle$ un groupe monogène, $x \in G$, alors*

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

De plus G est abélien et la fonction $f : \mathbb{Z} \rightarrow \langle x \rangle$ définie en posant $f(k) := x^k$ est surjective, et vérifie : $f(k+l) = f(k)f(l)$ pour tout $k, l \in \mathbb{Z}$; et l'ensemble $\{k \in \mathbb{Z} \mid f(k) = e\}$ est un sous-groupe de \mathbb{Z} , donc est de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$.

Démonstration. Comme $xx^{-1} = xx^{-1} = e$, les produits dans G de lettres dans l'alphabet $A_x = \{x, x^{-1}\}$ sont soit des produits de la lettre x ou des produits de la seule lettre x^{-1} . Les éléments de $G = \langle x \rangle$ sont donc représentés par les mots x^n ou $(x^{-1})^n = x^{-n}$ avec $n \in \mathbb{N}$. Autrement dit, par les mots x^k avec $k \in \mathbb{Z}$. D'où

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

et la fonction f est surjective. Comme $x^k x^l = x^{k+l} = x^l x^k$ pour tout $k, l \in \mathbb{Z}$, on a bien que tous les éléments de G commutent entre eux. Donc G est un groupe abélien et $f(k+l) = f(k)f(l)$.

On note $H = \{k \in \mathbb{Z} \mid f(k) = x^k = e\}$. On voit que $0 \in H$ car $x^0 = e$. Maintenant, si $k, l \in H$, alors $f(k-l) = x^{k-l} = x^k (x^l)^{-1} = e$. Donc $k-l \in H$ et donc H est un sous-groupe de \mathbb{Z} en vertu de la proposition 1.10(a). On conclut grâce à la proposition 1.9 qu'il existe $n \in \mathbb{N}$ tel que $\{k \in \mathbb{Z} \mid f(k) = e\} = n\mathbb{Z}$. ■

Corollaire 1.17. *Si $\{k \in \mathbb{Z} \mid f(k) = e\} = 0\mathbb{Z} = \{0\}$, alors G est en bijection avec \mathbb{Z} et $x^k = 0$ si et seulement si $k = 0$.*

Démonstration. Il suffit de montrer que la fonction f est injective. Soit $k, l \in \mathbb{Z}$ tel que $f(k) = f(l)$, alors $x^k = x^l$. On en déduit que $e = x^k x^{-l} = x^{k-l}$. D'où $k-l \in \{k \in \mathbb{Z} \mid f(k) = e\} = 0\mathbb{Z} = \{0\}$; autrement dit $k-l = 0$ et $k = l$. On a bien f injective. ■

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

Nous allons maintenant nous intéresser à l'étude du cardinal d'un groupe et de ses sous-groupes. Nous savons déjà que l'ordre d'un sous-groupe divise l'ordre du groupe en vertu du théorème de Lagrange, nous allons maintenant étudier la notion d'ordre d'un élément dans un groupe.

Définition. L'**ordre d'un élément** $x \in G$ est l'ordre du sous-groupe (monogène) $\langle x \rangle$. On le note $\text{ord}_G(x)$, ou simplement $\text{ord}(x)$ si il n'y a pas de confusion possible.

Si le groupe $\langle x \rangle$ est infini, on dit que l'ordre de x est infini, et on écrit $\text{ord}(x) := \infty$. S'il est fini, on pose $\text{ord}(x) := |\langle x \rangle|$. Le groupe monogène fini $\langle x \rangle$ est alors appelé **groupe cyclique**.

Exemple. Observons que dans $(\mathbb{Z}, +)$, tous les éléments non nuls sont d'ordre infini et $\text{ord}(0) = 1!$ 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.

Remarque. (i) Pour un groupe G fini, on a $\text{ord}(x)$ divise $|G|$, pour chaque élément x de G , en vertu du théorème de Lagrange. En particulier si G est fini, alors $x^{|G|} = e$ pour tout $x \in G$.

(ii) 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 $\text{ord}(x) = 1 = |\langle x \rangle|$, alors $\langle x \rangle = \{x\}$. Comme tout sous-groupe de G contient e , on a $e \in \langle x \rangle$, et donc $x = e$.

(iii) Évidemment, G est infini s'il contient un élément d'ordre infini x , puisqu'il contient l'ensemble infini $\langle x \rangle$.

(iv) On a en général (exercice) $\text{ord}(x) = \text{ord}(x^{-1})$. Les éléments d'ordre 2 dans G sont donc des **involutions** car $x^{-1} = x$ implique $x^2 = e$.

(v) Parmi les groupes finis dits **exceptionnels** (voir Section 2.1.3), le plus grand est le groupe M , qu'on appelle le « Monstre ». Une des raisons est que son ordre est « assez » grand

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

$$= 808017424794512875886459904961710757005754368000000000.$$

Le résultat suivant est une caractérisation importante de l'ordre d'un élément et très utile à son calcul dans le cas fini.

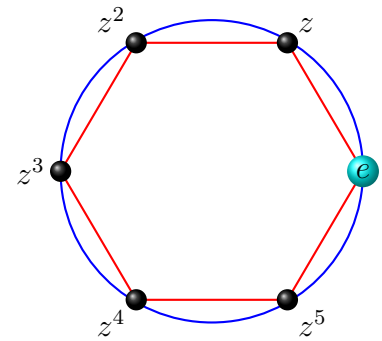
Proposition 1.18. Soit G un groupe et $x \in G$ d'ordre fini. Alors l'ordre d'un élément x est la plus petite puissance de x qui donne l'élément neutre, c.-à-d.

$$\text{ord}(x) = \min\{n \in \mathbb{N}^* \mid x^n = e\}. \tag{1.9}$$

En particulier, si $\text{ord}(x) = n$, alors :

(i) le groupe cyclique $\langle x \rangle$ s'écrit : $\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$.

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



Groupe cyclique, $z^6 = e$.

Démonstration. On sait que $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$. On pose $n = \min\{n \in \mathbb{N}^* \mid x^n = e\}$ et $H = \{e, x, \dots, x^{n-1}\}$. On a $H \subseteq \langle x \rangle$. Soit $x^m \in \langle x \rangle$, $m \in \mathbb{Z}$. On écrit $m = nq + r$ où $0 \leq r < n$ est le reste de la division euclidienne de m par n . Il s'ensuit $y = x^m = x^r \in \{e, x, x^2, \dots, x^{n-1}\} = H$. Ce qui montre (i).

Maintenant, si $x^l = x^k$ avec $0 \leq k \leq l \leq n - 1$, on a $x^{l-k} = e$ et $0 \leq l - k < n$. Par minimalité de $n \in \mathbb{N}^*$ pour la propriété $x^n = e$, on obtient $k - l = 0$ et donc $k = l$. Donc les éléments dans H sont deux à deux distincts, ce qui, en d'autres termes, signifie que $n = |H| = |\langle x \rangle| = \text{ord}(x)$. Pour (ii) il suffit pour conclure d'observer que $x^{n-1}x = x^n = e = x x^{n-1}$. ■

Corollaire 1.19. *Soit G un groupe et $x \in G$ d'ordre fini. Soit $n \in \mathbb{N}^*$ tel que $x^n = e$, alors $\text{ord}(x)$ divise n . Si de plus n divise tous les entiers $m \in \mathbb{N}^*$ tel que $x^m = e$, alors $n = \text{ord}(x)$.*

Démonstration. Posons $k = \text{ord}(x)$. On effectue la division euclidienne de n par k : $n = kq + r$ où $0 \leq r < k$. Donc $e = x^n = (x^k)^q x^r = x^r$. Par minimalité de k pour la propriété $x^k = e$ vu dans la proposition précédente et comme $0 \leq r < k$ on a $r = 0$. Donc k divise n . Si maintenant n divise tous les entiers m tel que $x^m = e$, il divise aussi k . Donc $k = n$ avec cette hypothèse supplémentaire. ■

Exemples. On constate que dans S_3 , on a $\text{ord}(e) = 1$, $\text{ord}(213) = \text{ord}(132) = \text{ord}(321) = 2$ (ce sont des involutions) et $\text{ord}(231) = \text{ord}(312) = 3$. Comme autre exemple, dans \mathbb{Z}_6 , on a $\text{ord}(0) = 1$, $\text{ord}(1) = \text{ord}(5) = 6$, $\text{ord}(2) = \text{ord}(4) = 3$, et $\text{ord}(3) = 2$ (donc 3 est une involution). Notez que, dans tous ces exemples, l'ordre d'un élément divise bien l'ordre du groupe comme le veut le théorème de Lagrange.

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 1.18 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 Rubik.

Corollaire 1.20. *Si G est un groupe fini engendré par S , alors tous les générateurs sont d'ordre fini et $s^{-1} = s^{d-1}$, avec $d = \text{ord}(s)$ pour $s \in S$. En particulier*

$$G = \langle S \rangle = \{e, s_1 \dots s_n \mid s_i \in S, n \in \mathbb{N}^*\}$$

(on n'a nul besoin de considérer les inverses des générateurs).

Démonstration. En vertu de la proposition 1.15, $x \in G$ s'écrit donc comme un produit de générateurs : $x = s_1 \dots s_m$ (avec $x_i \in S$ ou $x_i^{-1} \in S$), et on n'a nul besoin de considérer les inverses. Il suffit donc de remplacer chaque inverse s^{-1} (pour $s \in S$) par le mot s^{d-1} , où $d = \text{ord}(s)$. ■

Exemple. Noter que pour S_3 engendré par $S = \{\tau = (12), \sigma = (123)\}$, on a $(13) = \tau\sigma^{-1}$. Mais comme σ est d'ordre 3, et donc $\sigma^{-1} = \sigma^2$. On obtient donc $(13) = \tau\sigma\sigma$ qui est un mot dans l'alphabet S seulement (au lieu de $A_S = S \cup S^{-1}$).

Les groupes $(\mathbb{Z}_n, +)$. Nous discutons ici l'ordre des éléments de \mathbb{Z}_n .

Proposition 1.21. *Soit $\bar{x} \in \mathbb{Z}_n$ et $d = \text{pgcd}(x, n)$, alors $\text{ord}(\bar{x}) = n/d$.*

Démonstration. Considérons les deux entiers $k := n/d$ et $\ell := x/d$. On note tout d'abord que $\text{pgcd}(k, \ell) = 1$. En effet, si d' divise k et ℓ , alors $d'd$ divise x et n . Or $d = \text{pgcd}(x, n)$, donc $d' = 1$.

Soit $m \in \mathbb{N}^*$ tel que $m\bar{x} = \bar{0}$. Alors $mx = bn$ pour un certain $b \in \mathbb{N}$. En divisant n et x par leur $\text{pgcd } d$ on obtient $: m\ell = bk$. Comme $\text{pgcd}(k, \ell) = 1$, on a par le lemme de Gauss que k divise m . Pour conclure que $k = \text{ord}(\bar{x})$ il suffit maintenant de montrer que $k\bar{x} = \bar{0}$ en vertu du corollaire 1.19. Calculant dans \mathbb{Z}_n , on a (en notation additive) $: k \cdot \bar{x} = \overline{k(d\ell)} = \overline{n\ell} = \bar{n\ell} = \bar{0}$. ■

On a vu précédemment que les sous-groupes de \mathbb{Z} sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}^*$. La proposition suivante donne un analogue pour le groupe des entiers modulaires.

Proposition 1.22. *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. Voir exercice 1.35. ■

Exemple. Les sous-groupes de \mathbb{Z}_6 sont $\{\bar{0}\}$, $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$, $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$ et $\langle \bar{1} \rangle = \mathbb{Z}_6$, qui sont les images par la bijection de la proposition ci-dessus des sous-groupes $6\mathbb{Z}$, $2\mathbb{Z}$, $3\mathbb{Z}$ et \mathbb{Z} .

Corollaire 1.23. *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. Voir exercice 1.35. ■

1.4.3 Graphe de Cayley.

La notion de partie génératrice nous permet de développer un outil plus commode que la table de multiplication afin de représenter un groupe. Une façon de visualiser comment un couple (G, S) , où G est un groupe engendré par S , est de construire le **graphe de Cayley** pour (G, S) . Les sommets du graphe sont les éléments du groupe. Pour chaque générateur s , on a un arc de g à h :

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

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 appelle le graphe de Cayley du groupe S_4 , pour les générateurs $\tau_i = (i, i + 1)$, le **permutoèdre de S_4** . Les arêtes **bleues**, **rouges** et **vertes** correspondent respectivement à la multiplication par les transpositions (12) , (23) et (34) . Les hexagones viennent de ce que

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

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 1.2 ; tandis qu'avec les générateurs $\tau_1 = (12)$ et $\sigma = (123)$, on obtient le graphe de droite de cette même figure.

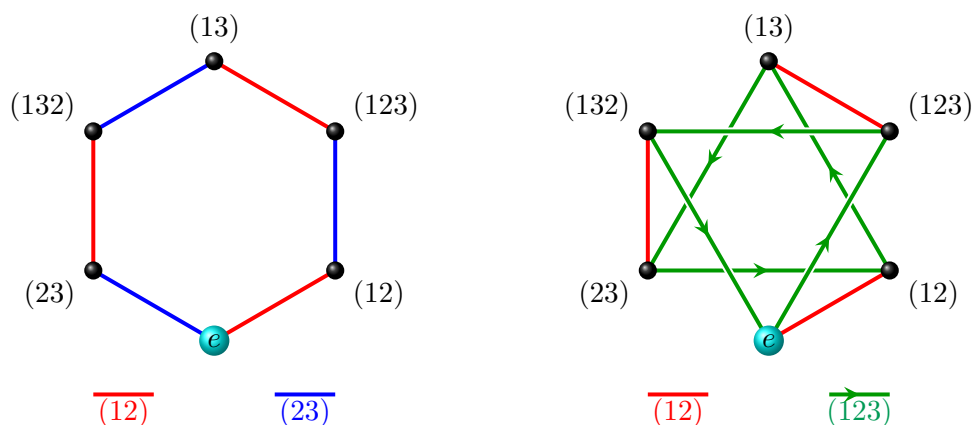


FIGURE 1.2 – Deux graphes de Cayley pour S_3 .

1.5 Le groupe symétrique, le groupe diédral et autres exemples

Nous clôturons ce chapitre avec deux exemples très classiques et importants : le groupe symétrique et le groupe diédral.

1.5.1 Le groupe symétrique, partie 2

On continue ici l'exemple général du groupe symétrique commencé au §1.2.2

Pour faciliter la présentation, on choisit de prendre $E = \{1, 2, \dots, n\}$, mais certaines de nos

observations s'appliquent au cas général¹⁰. 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 aussi). Comme nous allons le voir plus tard, tout groupe fini est une copie d'un sous-groupe d'un groupe symétrique (théorème de Cayley¹¹). La question de trouver tous les sous-groupes d'un groupe symétrique est donc étroitement liée à la classification de tous les groupes finis !

Générateurs distingués du groupe symétrique. Une **inversion**¹² d'une permutation $\sigma \in S_n$ est un couple (i, j) tel que :

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

On appelle le nombre d'inversions de la permutation $\sigma \in S_n$ la **longueur de σ** . Ce nombre est noté :

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

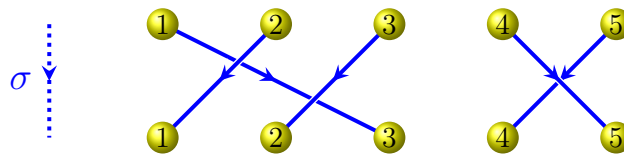
On établit facilement que $\ell(\sigma) = 0$ si et seulement si $\sigma = e$. En effet, il est clair que la longueur de e est 0, puisque e n'a pas d'inversion. Inversement, si $\ell(\sigma) = 0$ alors on doit avoir $\sigma(1) < \sigma(2) < \dots < \sigma(n)$, d'où $\sigma = 12 \dots n = e$. Par exemple,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



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, $1 \leq i < n$,

10. 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.

11. Arthur Cayley (1821-1895).

12. Observons que cette notion utilise l'ordre sous-jacent sur les entiers.

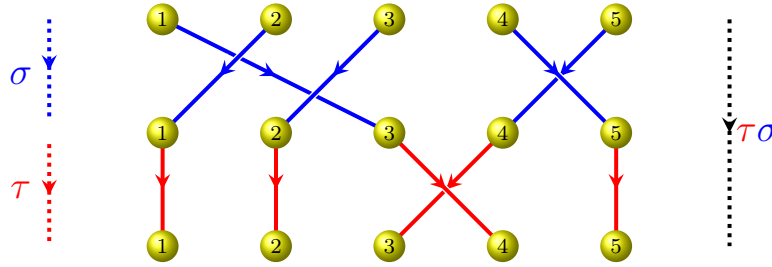


FIGURE 1.3 – Composition de permutations

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

$$\sigma \tau_i = \sigma(1)\sigma(2)\dots\sigma(i - 1) \underbrace{\sigma(i + 1)\sigma(i)}_{\curvearrowright} \sigma(i + 2)\dots\sigma(n).$$

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 1.24. Soit $\sigma \in S_n$ et $1 \leq i < n$, alors $\ell(\sigma\tau_i) = \ell(\sigma) \pm 1$. Plus précisément,

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

De plus, $\ell(\sigma) = 0$ si et seulement si $\sigma = e$ et, si $\sigma \neq e$, il existe $1 \leq i \leq n - 1$ tel que $\ell(\sigma\tau_i) = \ell(\sigma) - 1$.

Démonstration. Posons $\sigma = a_1a_2\dots a_n$ où $a_i = \sigma(i)$. Comme on l'a déjà observé, $\alpha = \sigma\tau_i = a_1\dots a_{i-1}a_{i+1}a_ia_{i+2}\dots a_n$ 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 : par exemple, si (i, k) est une inversion de α alors $(i + 1, k)$ est une inversion de α car $a_i = \sigma(i) = \sigma\tau_i(i + 1) = \alpha_{i+1}$ et $\sigma(k) = \alpha_k$; les autres cas sont laissés en exercices pour le lecteur. 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 $(i, i + 1)$.

Finalement, 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 .

Maintenant, si $\ell(\sigma) = 0$ on a vu après la définition de la longueur que $\sigma = e$. Le dernier énoncé en découle sans difficulté et est laissé en exercice au lecteur. ■

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 1.25. *Toute permutation $\sigma \in S_n$ est un produit de $\ell(\sigma)$ transpositions adjacentes. En d'autres termes : $S_n = \langle \tau_1, \dots, \tau_{n-1} \rangle$.*

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 $\sigma(i) > \sigma(i + 1)$ grâce au lemme 1.24. Ainsi, toujours en vertu du lemme 1.24, $\ell(\sigma\tau_i) = \ell(\sigma) - 1 < \ell(\sigma)$. Par hypothèse de récurrence, $\sigma\tau_i$ 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. ■

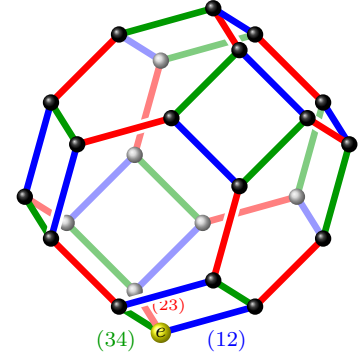


FIGURE 1.4 – Permutoèdre du groupe S_4 .

Signature d'une permutation. Une autre utilité de la longueur est de permettre la définition suivante. On considère la fonction

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

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

$$\det(a_{ij})_{1 \leq i, j \leq n} = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1, \sigma(1)} a_{2, \sigma(2)} \cdots a_{n, \sigma(n)}, \quad (1.10)$$

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

Corollaire 1.26. Pour tout σ , et τ dans S_n , on a

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

Démonstration. Il suffit de montrer que

$$\ell(\sigma\tau) \equiv \ell(\sigma) + \ell(\tau) \pmod{2}. \quad (1.11)$$

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 (1.11) est laissée en exercice. ■

Ordre et cycles d'une permutation. La notion de cycle¹³ est fondamentale dans le groupe symétrique. Elle rend possible une nouvelle décomposition des permutations. Cette décomposition permet entre autre de calculer très facilement l'ordre d'une permutation.

Pour $1 < p \leq n$, 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 $1 \leq a_1, a_2, \dots, a_p \leq n$ tels que

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

avec de plus $\gamma(b) = b$ pour tout $b \notin \{a_1, \dots, a_p\}$. On dit de ces derniers b , que ce sont des points fixes de γ . La figure 1.5 représente un cycle de façon plus imagée.

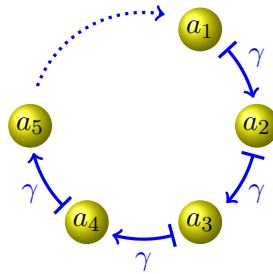


FIGURE 1.5 – Un cycle.

On désigne habituellement par (a_1, a_2, \dots, 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

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

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

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

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 1.27. *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) $\text{ord}(\gamma) = p$.
- (3) le signe de γ est $(-1)^{p-1}$.

Démonstration. Voir exercice 1.42. ■

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 $\{a_1 \dots, a_p\} \cap \{b_1 \dots, b_q\} = \emptyset$. 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 1.28. *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 1.6. Dans celle-ci, on joint les éléments de l'ensemble sous-jacent par une flèche $i \rightarrow j$, si $\sigma(i) = j$. On voit bien ainsi apparaître les cycles disjoints, pour le moins que le dessin soit fait correctement.

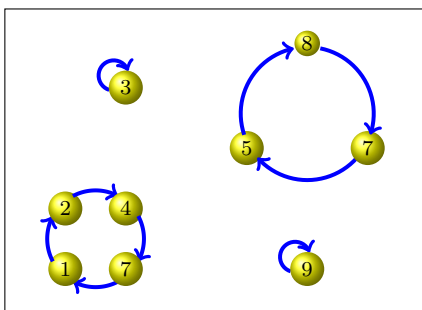


FIGURE 1.6 – La décomposition de la permutation 248736159 en cycles disjoints.

Corollaire 1.29. Soit $\sigma = \gamma_1 \dots \gamma_k \in S_n$ une permutation en cycle décomposée en cycles disjoints, alors $\text{ord}(\sigma) = \text{ppcm}(\text{ord}(\gamma_1), \text{ord}(\gamma_2), \text{ord}(\gamma_3), \dots, \text{ord}(\gamma_k))$. De plus : $\epsilon(\sigma) = (-1)^{n-c(\sigma)}$, où $c(\sigma)$ est le nombre de cycles de σ .

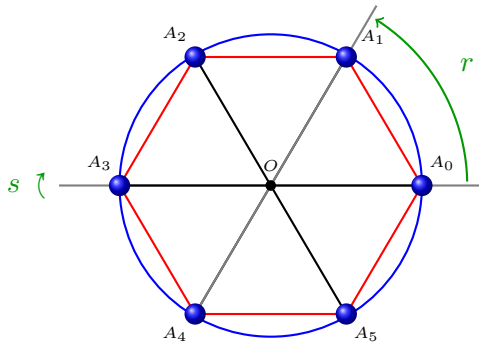
Démonstration. Exercice. ■

Par exemple, avec la permutation $\sigma = 729158436 \in S_9$ de l'exemple précédent, on trouve de cette manière que $\text{ord}(\sigma) = 12$, 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 .

1.5.2 Les isométries d'un polygone régulier : le groupe diédral

Pour un entier $m \geq 3$, on considère le polygone plan régulier convexe P_m à m sommets $A_0 \dots, A_{m-1}$ 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-dessous), 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 O qui envoie A_k sur A_{k+1} , la rotation r^2 de centre O qui envoie A_k sur A_{k+2} , la rotation r^3 de centre O qui envoie A_k sur A_{k+3} , etc.



Le groupe D_6 agit sur l'hexagone.

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

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

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

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

est d'ordre $2 \cdot 4 = 8$. Plus généralement, pour $m \geq 3$, 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

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

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

Proposition 1.30. *Soit $m \in \mathbb{N}$, $m \geq 3$, alors*

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

Démonstration.

- (1) La première partie de la proposition est une conséquence de ce qui précède. Pour ce qui est de la deuxième partie : par définition, une symétrie vérifie $s^2 = e$ et $s \neq e$ donc $\text{ord}(s) = 2$. De plus, puisque $r^m(A_i) = A_i$, r^m ($m \geq 3$) fixe au moins trois points du plan, donc $r^m = e$ et $r, r^2, \dots, r^{m-1} \neq e$ donc $\text{ord}(r) = m$ (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 $sr sr = e$.

- (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, ou réflexions, 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} .

En effet, si f est une isométrie qui préserve P_m , alors le sommet A_0 s'envoie par f sur un sommet A_k : $f(A_0) = A_k$, où $0 \leq k \leq m-1$. Si f fixe la médiatrice du segment $[A_0, A_k]$ alors f est la réflexion d'axe cette médiatrice. Sinon, f est la rotation d'angle $(\overrightarrow{OA_0}, \overrightarrow{OA_k})$ qui est précisément r^k . Donc f est bien l'une des isométries décrites ci-dessus. D'où le résultat. ■

Remarque. (a) 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** $s^2 = r^m = sr sr = e$. On démontrera ce fait dans le chapitre 3.1 et on le notera comme suit

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

- (b) On observe que le produit $t = sr$ est une réflexion préservant P_m (laquelle?). De plus, s et t engendrent D_m et des relations suffisantes pour construire D_m pour ces générateurs sont données ci-dessous :

$$D_m = \langle s, t \mid s^2 = (st)^m = t^2 = e \rangle.$$

On dit que D_m est engendré par réflexions.

1.5.3 Groupes engendrés par des réflexions

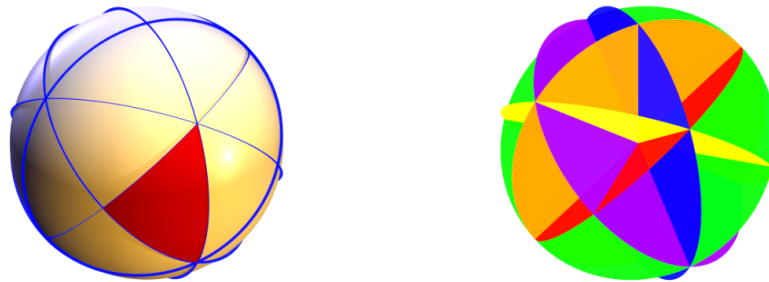


FIGURE 1.7 – Arrangement d'hyperplans dans \mathbb{R}_3 , correspondant à S_4

Les groupes symétriques et les groupes diédraux font partie (à isomorphisme¹⁴ près) d'une famille de groupes de grand intérêt en recherche mathématique contemporaine. Ce sont des sous-groupes de

14. Voir Section (2.1.1).

$GL_n(\mathbb{R})$ qui s'obtiennent en composant des **réflexions** par rapport à des hyperplans, c'est-à-dire, des sous espaces vectoriels de \mathbb{R}^n de dimension $n - 1$. On observe qu'une réflexion est un automorphisme de \mathbb{R}^n qui est son propre inverse. Dans \mathbb{R}^4 , les matrices suivantes sont des matrices de réflexions :

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

qui engendrent le groupe S_4 . 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 1.7. Dans la partie de droite de cette figure, les plans sont obtenus comme intersection¹⁵ avec les hyperplans de réflexion. Il y a un plan pour chaque réflexion¹⁶ 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 1.7, ainsi qu'à la figure 1.8. 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 permettent de déterminer quels sont tous les groupes finis de ce genre. Un autre exemple que nous verrons plus tard (Voir Section 4.1) est le groupe « diédral ». Plus généralement, parmi les groupes engendrés par les réflexions, on retrouve les **groupes de Coxeter**¹⁷ qui jouent un rôle fondamental dans plusieurs domaines des mathématiques, de la physique, et en cristallographie.

1.5.4 Un groupe à la Galois

On considère, sur le sous-ensemble de \mathbb{C} dont les éléments sont de la forme

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

avec a, b, c, d , et e des nombres réels, la restriction des « transformations » $f : \mathbb{C} \rightarrow \mathbb{C}$ vérifiant :

- (1) $f(x + y) = f(x) + f(y)$, pour tout $x, y \in \mathbb{C}$,
- (2) $f(xy) = f(x)f(y)$, 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. Les conditions ci-dessus entraînent aussi que

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

15. Pour plus de détails, voir **Swallowtail on the shore**, dans la série de textes *Snapshots of modern mathematics from Oberwolfach*, No7/2014.

16. Attention, le groupe contient aussi d'autres éléments.

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

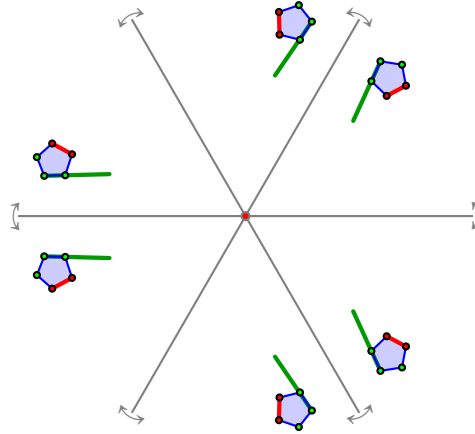


FIGURE 1.8 – Réflexions selon des droites d’angles $2k\pi/6$, avec $0 \leq k \leq 2$.

avec

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

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** différentes¹⁸ de 1 :

$$f_k(\zeta) = \zeta^k, \quad 1 \leq k \leq 4,$$

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 »¹⁹, 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 $p(z) = a + bz + cz^2 + dz^3 + ez^4$.

18. Ceci résulte de la condition (3).

19. À ce sujet, voir la notion d’isomorphisme, Section 2.1.1.

1.6 Une application : le système de cryptographie RSA

La généralisation suivante du petit théorème de Fermat²⁰ (due à Gauss²¹), 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 possible²² le système de cryptographie à clé publique « RSA ».

Théorème 1.31 (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'Euler²³.

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.

Les systèmes de cryptographie à clé publique sont de grand intérêt dans le contexte des transactions informatiques. L'algorithme RSA²⁴ 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 1.32. *Si $n = pq$ avec $p \neq q$ nombres premiers, alors $\varphi(n) = (p-1)(q-1)$.*

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

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 génère²⁵ 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 $n := pq$.

20. Pierre Fermat, 1601-1665.

21. Carl Friedrich Gauss (1777-1855).

22. Cela n'est qu'une de ses nombreuses applications.

23. Leonhard Euler, 1707-1783.

24. Rivest, Shamir et Adleman (1977).

25. Il existe des algorithmes "simples" et efficaces pour ce faire.

- (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 impossible²⁶ 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 \bar{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.

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 $ed \equiv 1 \pmod{\varphi(n)}$ ($\bar{e} = \bar{d}^{-1}$). 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

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

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 . ■

²⁶. 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.

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

$$\begin{aligned} p &= 632382913902128079995508264334209792839330997 \\ &\quad 050865499213108496836190519861047497803309801 \\ q &= 558218333272171098430334114939430707924967254 \\ &\quad 197312990249604572758081938867755300016964127. \end{aligned}$$

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

$$\begin{aligned} e &= 150650905007553408748182082815984929359632269 \\ &\quad 852681585809504709739738485231104248045693804 \\ &\quad 710098188302655538010818866476054310788175542 \\ &\quad 136407374106205605523687223946800025812242019. \end{aligned}$$

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 $(91, 23)$.

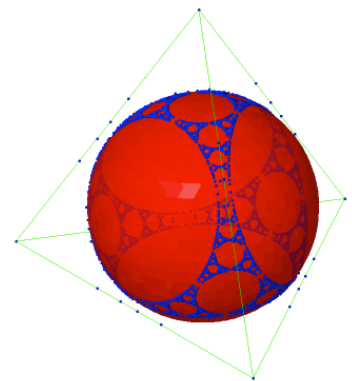
(b) Après calcul, on trouve la clef privée est $d = 47$. En effet $23 \cdot 47 = 1 + 15 \cdot 72 \equiv 1 \pmod{\varphi(n)}$.

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

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

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 classer 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,

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)!

1.7 Exercices

Questions d'auto-évaluation

Lois de composition, magmas et monoïdes

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

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

Question 1.3. 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 sous \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 $E = \text{GL}_n(\mathbb{R})$.

Question 1.4. Démontrer la Proposition 1.3, c'est-à-dire : montrer que l'inverse de l'élément neutre d'un groupe est égal à lui-même; montrer que l'inverse de l'inverse de x est égal à x et que l'inverse de $x * y$ est $y^{-1} * x^{-1}$.

Question 1.5. Soit E un ensemble. Vérifier que la composition de fonction munie l'ensemble $\text{Fonct}(E, E)$ d'une structure de monoïde.

Groupes

Question 1.6. On considère les ensembles $\mathbb{N}^*, \mathbb{Z}, \mathbb{Z}^*, \mathbb{Q}, \mathbb{Q}^*, \mathbb{Q}^+, \mathbb{Q}^{+*}, \mathbb{R}^*, \mathbb{R}^+, \mathbb{R}^{+*}, \mathbb{Z}^-, \mathbb{Q}^-$ et \mathbb{R}^- . 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.

Réponses partielles : (a) Les monoïdes sont $\mathbb{Z}, \mathbb{Q}, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{Z}^-, \mathbb{Q}^-$ et \mathbb{R}^- et seuls les deux premiers sont des groupes; (b) Les monoïdes sont $\mathbb{N}^*, \mathbb{Z}, \mathbb{Z}^*, \mathbb{Q}^+, \mathbb{Q}, \mathbb{R}^+, \mathbb{R}^*, \mathbb{R}^{+*}, \mathbb{Q}^*$ et \mathbb{Q}^{+*} et seuls les quatre derniers sont des groupes.

Question 1.7. Pour tout espace vectoriel V , déduire de la définition d'espace vectoriel que $(V, +)$ est un groupe. En conclure que $(\mathcal{M}_n(\mathbb{R}), +)$ est un groupe.

Question 1.8. Soit $n \in \mathbb{N}^*$.

- (a) Vérifier que $(\mathbb{Z}_n, +)$ est un groupe abélien de cardinal n .
- (b) Vérifier que (\mathbb{Z}_n, \cdot) est un monoïde commutatif. Est-ce un groupe ? (Justifier.)
- (c) Vérifier 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 ?

Question 1.9. Écrire la table de multiplication du groupe de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$ et la comparer à celle du groupe \mathbb{Z}_4 .

Question 1.10. Soit G un groupe et soit $a, b \in G$ tel que $a^5 = e$ et $a^3b = ba^3$.

- (a) Montrer que $a^6b = ba^6$;
- (b) en déduire que $ab = ba$.

Question 1.11. Déterminer lesquels des énoncés ci-dessous est vrai ou faux. Si il est vrai, en donner une démonstration ; si il est faux, en donner un contre-exemple.

- (a) Si $x^2 = e$, alors $x = e$.
- (b) Si $x^2 = a^2$, alors $x = a$.
- (c) Pour tout $a, b \in G$, on a $(ab)^2 = a^2b^2$.
- (d) Si $x^2 = x$, alors $x = e$.
- (e) Pour tout $x \in G$, il existe $y \in G$ tel que $x = y^2$.
- (f) Pour tout $x, y \in G$, il existe un élément $z \in G$ tel que $y = xz$.

Sous-groupes

Question 1.12. (voir Proposition 1.10) Soit G un groupe. Montrer que

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

Question 1.13. 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 .

Question 1.14. Est-ce que le sous-ensemble $\{1234, 4213, 4321, 3241, 3412\}$ est un sous-groupe de S_4 ?.

Réponse : penser au théorème de Lagrange.

Question 1.15. Déterminer les sous-groupes de $\mathbb{Z}_4 \times \mathbb{Z}_2$ et donner leur ordre.

Sous-groupes engendrés par une partie

Question 1.16. Soit G un groupe dont e désigne l'élément neutre. Vérifier que $\langle \emptyset \rangle = \{e\}$ et $\langle G \rangle = G$.

Question 1.17. On pose dans S_3 , $S = \{\tau_1, \tau_2\}$ où $\tau_1 = 213$ et $\tau_2 = 132$. Montrer que l'élément 321 est représenté par les mots $\tau_1\tau_2\tau_1$, $\tau_2\tau_1\tau_2$ et $\tau_1\tau_2\tau_1\tau_2\tau_2$.

Question 1.18. 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?

Question 1.19. Soit G un groupe d'ordre p premier, montrer que G est cyclique.

Question 1.20. Comment s'écrit un groupe monogène G si la loi est notée additivement?

Question 1.21. 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) $\text{ord}(g^{-1}) = \text{ord}(g)$.

Question 1.22. Soient p et q des nombres premiers distincts. Soit G un groupe fini qui possède un élément d'ordre p et un élément d'ordre q . Montrer que l'ordre de G est un multiple de pq .

Réponse : Si G possède un élément d'ordre p , alors par le théorème de Lagrange, p divise $|G|$. De même, q divise $|G|$. Comme $\text{pgcd}(p, q) = 1$, on a que pq divise $|G|$.

Question 1.23. 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 $\text{ord}(x) = n$ et $\text{ord}(y) = m$ sont premiers entre eux, alors $\text{ord}(xy) = nm$.

Qu'en est-il si $xy \neq yx$?

Groupes symétriques et diédraux

Question 1.24. 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.

Question 1.25. Décomposer en cycles disjoints les permutations dans S_3 et dans S_4 et calculer l'ordre de leurs éléments.

Question 1.26. Considérons les trois permutations suivantes de S_7 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 2 & 5 & 1 & 6 & 3 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 7 & 2 & 3 & 4 & 5 \end{pmatrix} \quad \gamma = (1, 3, 7, 4, 2, 6)$$

1. Calculer σ^{-1} , τ^{-1} , γ^{-1} .
2. Écrire σ , τ et γ comme produits de cycles disjoints.
3. Écrire σ , τ et γ comme produits de transpositions.
4. Écrire σ , τ et γ comme produits de transpositions adjacentes.
5. Déterminer si σ , τ et γ sont des permutations paires ou impaires.

Question 1.27. Établir la table de multiplication du groupe diédral D_3 . Comparer avec la table du groupe S_3 : que remarque-t-on ?

Exercices

Exercice 1.1. Montrer que l'ensemble

$$E = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{C} \right\}$$

muni de la multiplication des matrices est un groupe.

Exercice 1.2. Soit $H = \{2^k : k \in \mathbb{Z}\}$. Montrer que (H, \times) est un groupe.

Exercice 1.3. Soient X un ensemble, $f : X \rightarrow X$ une bijection et $G = \{f^k : k \in \mathbb{Z}\}$. Montrer que (G, \circ) est un groupe.

Exercice 1.4. 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

$$(A, B) \mapsto A \Delta B = (A \cup B) \setminus (A \cap B) \quad (\text{Différence symétrique}).$$

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

Exercice 1.5. 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 1.6. Soit G le produit cartésien d'ensembles $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ et \mathbb{Z} . On définit une loi de composition interne sur G par

$$(a, m) * (b, n) = (ab, m + n)$$

où $a, b \in \mathbb{R}^*$ et $m, n \in \mathbb{Z}$. Montrer que $(G, *)$ est un groupe.

Exercice 1.7. Soit G un groupe.

- (a) On suppose que pour tout $x \in G$ on a $x^2 = e$. Montrer que G est abélien.
- (b) On suppose que tout élément de G est égal à son inverse. Montrer que G est abélien.

Exercice 1.8. Montrer que le produit direct de groupes abéliens est un groupe abélien.

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

- (a) Montrer que l'ensemble $O(n) = \{M \in \mathcal{M}_n(\mathbb{R}) \mid {}^t M M = \text{Id}_n\}$ est un sous-groupe de $\text{GL}_n(\mathbb{R})$. C'est le **groupe orthogonal**. Rappelons que ${}^t M$ désigne la transposée de M .
- (b) Montrer que l'ensemble $SO(n) = \{M \in O(n) \mid \det(M) = 1\}$ 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 1.10. Montrer que G est un groupe abélien si et seulement si G est égal à son centre.

Exercice 1.11. (voir Proposition 1.9) Montrer que les seuls sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $(n\mathbb{Z}, +)$, pour $n \in \mathbb{N}$ (indication : si H est un sous-groupe de \mathbb{Z} , considérer n égal au plus petit entier positif non nul dans H).

Exercice 1.12. Soit G un groupe. Pour $x \in G$ on note

$$G_x = \{g \in G \mid gx = xg\}.$$

- (a) Montrer que, pour tout $x \in G$, G_x est un sous-groupe de G .
- (b) On pose $G = S_3$ le groupe symétrique à 6 éléments et on pose les éléments $e = 123$ et $\sigma = 231$. Montrer que $G_e = S_3$ et $G_\sigma = \langle \sigma \rangle$.

Exercice 1.13. 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 1.14. Soit G un groupe et H, K deux sous-groupes de G . On suppose qu'il existe $a, b \in G$ tel que :

$$aH = \{ah \mid h \in H\} \subseteq \{bk \mid k \in K\} = bK.$$

Montrer que $H \leq K$.

Exercice 1.15. Soit G un groupe et $A \subseteq G$. Pour $g \in G$ on note $gAg^{-1} = \{gxg^{-1} \mid x \in A\}$.

- (a) Montrer que $Z(A) = \{g \in G \mid gx = xg, \text{ pour tout } x \in A\}$ est un sous-groupe de G .
- (b) Montrer que gAg^{-1} et A sont en bijection.
- (c) Montrer que $N(A) = \{g \in G \mid gAg^{-1} = A\}$ est un sous-groupe de G .
- (d) Montrer que $Z(A) \leq N(A)$.

Exercice 1.16. Soit G un groupe. Soit H un sous-groupe de G tel que si H' est un sous-groupe non trivial de G , alors $H \subseteq H'$. Montrer que $H \subseteq Z(G)$, où $Z(G)$ est le centre de G .

Exercice 1.17. Montrer que le centre $Z(G \times H)$, du produit direct de groupes est égal au produit direct des centres : $Z(G) \times Z(H)$.

Exercice 1.18. 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 $x \sim y$.

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

Exercice 1.19. Soit G un groupe et $H \leq G$, montrer que

- si $x \in G$ alors les conditions suivantes sont équivalentes : (i) $xH = H$; (ii) $x \in H$; (iii) $xH \leq G$;
- si $x, y \in G$ alors $xH = yH \iff x^{-1}yH = H \iff y^{-1}xH = H \iff x^{-1}y \in H$;
- si G est abélien, alors $xH = Hx$ pour tout $x \in G$;
- si $x, y \in G$, alors $y \in xH \iff y^{-1} \in Hx^{-1}$;
- si $x \in H$, alors la fonction $h \mapsto xh$ est une bijection de H sur xH . En déduire que xH , H et Hx ont même cardinal.
- Montrer que pour tout $x, y, z \in G$ tel que $xyH = xzH$ on a $yH = zH$.

Exercice 1.20. (Formule de l'indice) Soit H un sous-groupe d'indice fini d'un groupe G et $K \leq H$. Le but de ce problème est de montrer que K est d'indice fini dans G si et seulement si il est d'indice fini dans H , ainsi que la formule suivante :

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

- 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
 - $\Lambda = IJ$ est un système de représentant des classes G/K ;
 - Λ est en bijection avec $I \times J$.
- Montrer que $[G : K] = [G : H][H : K]$.
- En déduire que K est d'indice fini dans G si et seulement si il est d'indice fini dans H .

Exercice 1.21. Soit G un groupe et H_1, \dots, 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 1.22. Soit G un groupe et H, K deux sous-groupes finis de G .

- Montrer que si $|H|$ et $|K|$ sont premiers entre eux, alors $H \cap K = \{e\}$.
- On pose $n = [H : H \cap K]$. Soit $\{x_i \mid 1 \leq i \leq n\}$ un système de représentants des classes de $H/H \cap K$.
 - Montrer que $\{x_i K \mid 1 \leq i \leq n\}$ est une partition de HK .

(ii) Montrer que

$$|HK| = |KH| = \frac{|H||K|}{|H \cap K|}.$$

Exercice 1.23. Soit G un groupe non abélien tel que tout sous-groupe propre de G est abélien. Montrer qu'il existe deux éléments a et b de G tels que $G = \langle a, b \rangle$.

Exercice 1.24. (a) Montrer que \mathbb{Q} , muni de l'addition, n'est pas un groupe monogène.

(b) Montrer que \mathbb{R} , muni de l'addition, n'est pas un groupe monogène.

(c) Montrer que \mathbb{R}^* , muni de la multiplication, n'est pas un groupe monogène.

Exercice 1.25. Soit G un groupe fini et $A \subseteq G$ non vide. On suppose que A est stable pour la multiplication de G , c'est-à-dire $xy \in A$ pour tout $x, y \in A$. Montrer que A est un sous-groupe de G .

Exercice 1.26. Soit G un groupe et H un sous-ensemble fini de G de cardinal $m \in \mathbb{N}^*$. On suppose que H est stable pour la loi de composition interne de G , c'est-à-dire, $xy \in H$ pour tout $x, y \in H$.

(a) Soit $x \in H$, montrer que $x^n \in H$ pour tout $n \in \mathbb{N}^*$.

(b) Soit $x \in H$, montrer qu'il existe un entier $1 \leq n \leq m$ tel que $x^n = e$.

(c) Montrer que H est un sous-groupe de G .

Exercice 1.27. Soient a et b les matrices suivantes de $\text{GL}_2(\mathbb{Z})$.

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

1. Montrer que $\text{ord}(a) = 4$ et $\text{ord}(b) = 3$.

2. Montrer que $\text{ord}(ab) = \infty$. En déduire que le sous-groupe $H = \langle \{a, b\} \rangle$ de $\text{GL}_2(\mathbb{Z})$ est d'ordre infini.

Exercice 1.28. Soit H l'ensemble des matrices de $\text{GL}_2(\mathbb{R})$ de la forme $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ et soit K l'ensemble des matrices de $\text{GL}_2(\mathbb{R})$ de la forme $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$.

(a) Montrer que H est un sous-groupe de $\text{GL}_2(\mathbb{R})$.

(b) Montrer que K est un sous-groupe H .

(c) Déterminer les éléments de H d'ordre 2.

(d) Trouver deux éléments A et B de H d'ordre 2 et tels que l'ordre de AB est infini.

Exercice 1.29. Soit p un nombre premier et G l'ensemble suivant de matrices à coefficients dans \mathbb{Z}_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 $\text{GL}_3(\mathbb{Z}_p)$, 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 1.30. Soit a un élément d'ordre 12 dans un groupe G .

1. Trouver le plus petit entier positif k tel que $a^{8k} = e$.
2. Déterminer l'ordre de a^8, a^9, a^{10}, a^5 .
3. Trouver tous les entiers j tels que $\text{ord}(a^j) = \text{ord}(a)$.
4. Généraliser les exercices précédents. C'est-à-dire, soit b un élément d'ordre m dans un groupe G' : déterminer l'ordre de b^k ; et trouver tous les entiers j tels que $\text{ord}(b^j) = m$.

Exercice 1.31. Soit p un nombre premier. Montrer que si H et K sont deux sous-groupes d'un groupe G tels que $|H| = |K| = p$, alors $H = K$ ou $H \cap K = \{e\}$.

Exercice 1.32. Soient G un groupe fini et p un nombre premier. Montrer que le nombre d'éléments d'ordre p dans G est un multiple de $p - 1$. (indication : utiliser l'exercice 1.31)

Exercice 1.33. Soit G un groupe et a un élément dans G d'ordre fini. Montrer que l'ordre de a^k , pour tout $k \in \mathbb{Z}$, divise l'ordre de a .

Exercice 1.34. Soient D un groupe d'ordre $2n$, où n est impair, et H un sous-groupe de G d'ordre n tel que $hxh^{-1} = h^{-1}$ pour tout $h \in H$ et tout $x \in D \setminus H$. Montrer que H est abélien et que tout élément de $D \setminus H$ est d'ordre 2.

Exercice 1.35. Soit $n \in \mathbb{N}^*$.

- (a) Soit H un sous-groupe de \mathbb{Z}_n , montrer que le sous-ensemble $K = \{x \in \mathbb{Z} \mid \bar{x} \in H\}$ est un sous-groupe de \mathbb{Z} .
- (b) Montrer que 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 .
- (c) Montrer que $\mathbb{Z}_n = \langle x \rangle$ si et seulement si $\text{pgcd}(x, n) = 1$.
- (d) On considère le monoïde multiplicatif \mathbb{Z}_n et on note $(\mathbb{Z}_n)^\times$ son ensemble d'éléments inversibles. Montrer que $(\mathbb{Z}_n)^\times$ est l'ensemble des générateurs de $(\mathbb{Z}_n, +)$.

Exercice 1.36. Soit X l'ensemble des nombres réels $x \neq 0, 1, 2$. Soit R_4 le groupe engendré par les applications $f(x) = 2 - x$ et $g(x) = 2/x$. Calculer l'ordre de R_4 ainsi que sa table de multiplication.

Exercice 1.37. Soit I et J les deux matrices suivantes de $\text{GL}_2(\mathbb{C})$.

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

1. Dresser la table du sous-groupe $Q = \langle \{I, J\} \rangle$ de $\text{GL}_2(\mathbb{C})$.

2. Calculer l'ordre de tout élément de Q .
3. Calculer les sous-groupes de Q .
4. Calculer le centre²⁷ de Q .
5. Existe-t-il un élément $a \in Q$ tel que $Q = \langle a \rangle$?

Exercice 1.38. On considère dans cet question le groupe symétrique S_4 . Avec nos conventions, on a les transpositions adjacentes

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

On considère les sous-groupes

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

- (a) Quels sont les ordres de H , K et L ?
- (b) Écrire la table de multiplication de ces sous-groupes. Sont-ils abéliens?
- (c) Que remarquez-vous?

Exercice 1.39. (Relations de tresse) Dans S_n , avec $\tau_i := (i, i+1)$, montrer que pour tout $1 \leq i, j \leq n$, on a

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

et

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

Exercice 1.40. On considère la fonction

$$\gamma : S_n \rightarrow \mathbb{Z}_2 \quad \text{avec} \quad \gamma(\sigma) := \ell(\sigma) \pmod{2}.$$

- (a) Montrer que $\gamma(e) = 0$, et que $\gamma(\tau_i) = 1$ pour tout $1 \leq i < n$.
- (b) Soit $\sigma\tau \in S_n$. Par récurrence sur $\ell(\tau)$, montrer que $\ell(\sigma\tau) = (\ell(\sigma) + \ell(\tau) \pmod{2})$.
- (c) Montrer que $\gamma(\sigma\tau) = \gamma(\sigma)\gamma(\tau)$, pour tout $\sigma, \tau \in S_n$.

Exercice 1.41. Soient A , B et C les parties suivantes du groupe symétrique S_4 :

$$\begin{aligned} A &= \{\sigma \in S_4 : \sigma(1) = 3\} \\ B &= \{\sigma \in S_4 : \sigma(2) = 2\} \\ C &= \{\sigma \in S_4 : \sigma(1) = 3 \text{ et } \sigma(2) = 2\}. \end{aligned}$$

Déterminer si A , B et C sont sous-groupes de S_4 .

²⁷ Le centre d'un groupe G est $Z(G) = \{g \in G : xg = gx \text{ pour tout } x \in G\}$. Il est un sous-groupe de G .

Exercice 1.42. [Démonstration de la Proposition 1.27] Soit $\gamma = (a_1, \dots, a_p) \in S_n$ un p -cycle, alors

- (a) $\gamma^{-1} = (a_1, a_p, a_{p-1}, \dots, a_2)$ est un p -cycle ;
- (b) $\text{ord}(\gamma) = p$.
- (c) le signe de γ est $(-1)^{p-1}$.

Exercice 1.43. (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 1.44. Soit σ une permutation dans S_n et $\sigma = \gamma_1 \dots \gamma_k$ sa décomposition de σ en cycles disjoints, alors on a

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

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

Exercice 1.45. Montrer qu'on peut exprimer les transpositions $\tau_i = (i, i+1)$ comme produit de transpositions de la forme $(1a)$, pour $2 \leq a \leq n$. En conclure que le groupe S_n est engendré par ces transpositions.

Exercice 1.46.

- (a) Quel est le centre du groupe S_n , pour $n \in \mathbb{N}^*$?
- (b) Calculer le centre de $\text{GL}_n(\mathbb{R})$. Dans quel cas $\text{GL}_n(\mathbb{R})$ est commutatif.

Exercice 1.47. 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 1.48 (Le théorème de Wilson²⁸). Cet exercice a pour but de proposer une preuve du théorème de Wilson qui exploite les notions de ce chapitre.

Théorème (Wilson) Soit $n \in \mathbb{N}$, $n \geq 2$, 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 $x = e$;

28. **John Wilson** (1741-1793).

- (ii) si $|G|$ est pair et G ne contient qu'une involution alors montrer que x est cette unique involution ;
- (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 1.49. On définit l'ensemble d'inversion d'une permutation $\sigma \in S_n$ par :

$$\text{inv}(\sigma) = \{(k, l) \mid 1 \leq k < l \leq n, \sigma(k) > \sigma(l)\}.$$

- (a) Soit $1 \leq i \leq n - 1$, montrer que :

$$\ell(\sigma\tau_i) = \{(i, i + 1)\} \sqcup \tau_i(\text{inv}(\sigma)) \iff \ell(\sigma\tau_i) > \ell(\sigma),$$

où $\tau_i(k, l) = (\tau_i(k), \tau_i(l))$ pour toute inversion $(k, l) \in \text{inv}(\sigma)$.

- (b) Soit $\sigma, \gamma \in S_n$, montrer $\text{inv}(\sigma) = \text{inv}(\gamma)$ si et seulement si $\sigma = \gamma$.

Exercice 1.50. 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

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

- (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.

Exercice 1.51. 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 une règle calculatoire simple pour déterminer quels sont les types des permutations dans A_n , pour n quelconque.

Exercice 1.52 (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) $\emptyset \in \mathcal{T}$, et $E \in \mathcal{T}$;
- (2) toute intersection finie d'éléments de \mathcal{T} est dans \mathcal{T} :

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

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

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

Une fonction **continue** entre deux espaces topologiques (E_1, \mathcal{T}_1) et (E_2, \mathcal{T}_2) est une fonction $f : E_1 \rightarrow E_2$ 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

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

avec la distance euclidienne habituelle $\text{dist}(x, y)$. 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 la loi de composition interne 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.

- Montrer que \mathbb{R}^n avec l'addition vectorielle est un groupe topologique.
- Montrer que GL_n , $O(n)$, $SO(n)$, et SL_n sont des groupes topologiques, avec la multiplication de matrices.
- Montrer que si (E, \mathcal{T}) est un espace topologique, alors l'ensemble

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

avec la composition de fonctions comme loi de composition interne, est un groupe.

Exercice 1.53. 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 $a_1 a_2 \cdots a_n$, 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 la loi de composition interne de **concaténation**, c.-à-d.

$$(a_1 a_2 \cdots a_n) \cdot (b_1 b_2 \cdots b_k) := a_1 a_2 \cdots a_n b_1 b_2 \cdots b_k,$$

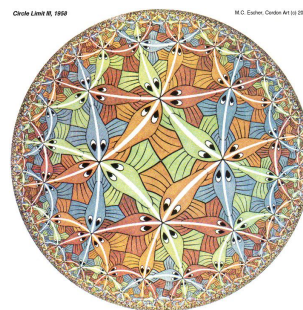
qui consiste simplement à coller ensemble les mots considérés.

- Montrer que la concaténation est associative, avec le mot vide comme élément neutre.
- Calculer le nombre de mots de longueur n sur un alphabet de longueur de k lettres.

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

Chapitre 2

Morphismes de groupes



Dans tout contexte mathématique, il importe de bien comprendre comment comparer les objets qui sont considérés, ceci afin de mieux comprendre leurs rôle et leurs propriétés. Lorsque ce contexte est algébrique, on parle de *morphismes d'objets*. Ce sont les fonctions entre structures algébriques de même nature qui « respectent » les opérations considérées ; par exemple pour les espaces vectoriels, ce sont les applications linéaires. Dans notre cas, ce sont les fonctions qui respectent les lois de composition de groupes que l'on appelle *morphismes de groupes*.

2.1 Morphismes de groupes

Soit (G, \cdot) et $(G', *)$ deux groupes. On notera $e := e_G$ l'élément neutre de G et $e' := e_{G'}$ l'élément neutre de G' .

Définition. Un **morphisme** (ou **homomorphisme**) de groupes de G vers G' est une application $\theta : G \rightarrow G'$ telle que

$$\theta(x \cdot y) = \theta(x) * \theta(y), \quad \text{pour tout } x, y \in G. \quad (2.1)$$

On dit d'un morphisme de G vers lui-même que c'est un **endomorphisme** de G . On note $\text{Hom}(G, G')$ l'ensemble des morphismes de G vers G' , et $\text{End}(G)$ l'ensemble des endomorphisme de G .

Remarque. (a) Il est clair que $\text{Hom}(G, G')$ et $\text{End}(G)$ sont non-vides, puisqu'on a toujours au moins le morphisme **trivial** $\theta : G \rightarrow G'$, qui envoie tous les éléments de G sur l'élément neutre de G' .

(b) 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' .

Exemples. Le signe $\varepsilon : S_n \rightarrow \{+1, -1\}$ est un morphisme de groupes¹ surjectif. Le déterminant $\det : \text{GL}_n \rightarrow \mathbb{R}^*$ (où \mathbb{R}^* est muni de la multiplication) ou bien encore l'application $f : \mathbb{Z} \rightarrow \langle x \rangle, k \mapsto x^k$, définie dans la Proposition 1.16, sont aussi des morphismes de groupes.

L'un des grands intérêts de la notion de morphisme de groupes entre G et G' est de permettre de comparer ou d'étudier tout ou en partie la structure de groupe sur G en parallèle à celle sur G' . Par exemple, la proposition suivante énonce que l'image de G par un morphisme de groupes de G vers G' est un sous-groupe de G' .

Proposition 2.1. *Si $\theta : G \rightarrow G'$ et $\psi : G' \rightarrow G''$ sont des morphismes de groupes, alors :*

- (1) $\theta(e) = e'$;
- (2) $\theta(x^{-1}) = \theta(x)^{-1}$ pour tout $x \in G$;
- (3) $H \leq G$ implique $\theta(H) \leq G'$;
- (4) $H' \leq G'$ implique $\theta^{-1}(H') \leq G$, où $\theta^{-1}(H') := \{x \in G \mid \theta(x) \in H'\}$;
- (5) $\psi \circ \theta : G \rightarrow G''$ est un morphisme de groupes ;
- (6) $\theta(\langle S \rangle) = \langle \theta(S) \rangle$, pour tout $S \subseteq G$;
- (7) $\text{ord}_{G'}(\theta(x))$ divise à la fois $\text{ord}_G(x)$ et $|\text{Im } \theta|$ pour tout $x \in G$.

Démonstration. Pour montrer (1), on observe que

$$\theta(e) e' = \theta(e) = \theta(ee) = \theta(e)\theta(e),$$

et donc $\theta(e)\theta(e) = \theta(e) e'$. Multipliant à gauche par l'inverse de $\theta(e)$, on trouve $\theta(e) = e'$.

Pour (2), considérons $x \in G$. On a :

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

ce qui implique $\theta(x^{-1}) = \theta(x)^{-1}$. Ensuite, prouvons (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 $x_1x_2^{-1} \in H$ on obtient, en vertu de (2), que

$$y_1y_2^{-1} = \theta(x_1)\theta(x_2)^{-1} = \theta(x_1)\theta(x_2^{-1}) = \theta(x_1x_2^{-1}) \in \theta(H).$$

Puisque $e' = \theta(e) \in \theta(H)$, on conclut que $\theta(H) \leq G'$. 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'énoncé. On laisse (6) et (7) en exercice au lecteur. ■

1. La structure de groupe sur $\{+1, -1\}$ correspond à l'opération de multiplication.

On en déduit immédiatement le résultat suivant :

Corollaire 2.2. $(\text{End}(G), \circ)$ est un monoïde. En particulier $\text{End}(G)^\times$ est un groupe.

2.1.1 Isomorphismes de groupes

À la vue du corollaire précédent, la question se pose donc quant à décrire l'ensemble des endomorphismes inversibles, c'est-à-dire, l'ensemble des endomorphismes bijectifs dont l'inverse est aussi un endomorphisme : on les appelle des **automorphismes** de G . L'ensemble des automorphismes est noté $\text{Aut}(G) = \text{End}(G)^\times$. En fait il se trouve que l'inverse d'un morphisme de groupes bijectif est lui-même un morphisme de groupes.

Proposition 2.3. Soit G et G' deux groupes.

1. Si $\theta : G \rightarrow G'$ est un morphisme de groupes bijectif, alors $\theta^{-1} : G' \rightarrow G$ est aussi un morphisme de groupes bijectif.
2. $\text{Aut}(G)$ est l'ensemble des endomorphismes de G bijectifs.
3. $\text{Aut}(G)$ 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 $\theta \circ \theta^{-1} = \text{Id} = \text{Id}_{G'}$, on a

$$x \cdot y = \text{Id}(x) \cdot \text{Id}(y) = \theta(\theta^{-1}(x)) \cdot \theta(\theta^{-1}(y)) = \theta(\theta^{-1}(x) \cdot \theta^{-1}(y)).$$

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. ■

Cette proposition justifie la définition suivante.

Définition. On dit qu'un morphisme bijectif $\theta : G \rightarrow G'$ est un **isomorphisme (de groupes²) de G sur G'** . On notera alors $\theta : G \xrightarrow{\sim} G'$. On note $\text{Isom}(G, G')$ l'ensemble des isomorphismes de G dans G' . S'il existe un isomorphisme entre deux groupes, on dit qu'ils sont **isomorphes**³. On dit alors aussi que G et G' sont dans la même **classe d'isomorphisme** et on note ce fait par $G \simeq G'$.

Deux groupes isomorphes ont les mêmes propriétés algébriques du point de vue de la théorie des groupes.

2. Quand plusieurs structures algébriques différentes sont utilisées, il faut faire bien attention à spécifier de quel objet le morphisme est : de groupes, d'espaces vectoriels, d'anneaux, etc.

3. Du grec « ισος » (isos) pour « même », et « μορφη » (morphè) pour « forme ».

Proposition 2.4. *La relation \simeq est une relation d'équivalence⁴. De plus, si G et G' sont deux groupes et θ est un isomorphisme de G sur G' , alors :*

1. G est abélien si et seulement si G' est abélien ;
2. pour tout $x \in G$ on a $\text{ord}(\theta(x)) = \text{ord}(x)$;
3. 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.

Démonstration. Voir les questions d'auto-évaluation 2.1 et 2.2. ■

La notion de classe d'isomorphisme simplifie de ce fait beaucoup l'étude des groupes, car maintenant il suffit donc de connaître un groupe dans chaque classe d'isomorphisme afin de comprendre tous les groupes de cette classe.

Remarque. On remarquera aussi que $\text{Isom}(G, G')$ peut être vide et donc deux groupes ne sont pas isomorphes en général. En effet, si $\text{Isom}(G, G')$ n'est pas vide, alors les deux groupes doivent avoir le même cardinal car un isomorphisme est en particulier une bijection.

Exemples. (a) L'application $\theta : \mathbb{Z}_2 \rightarrow \{+1, -1\}$ définie en posant $\theta(0) := 1$ et $\theta(1) := -1$ est un isomorphisme de groupes. En effet, on a

$$\begin{aligned} \theta(0 + 1) &= \theta(1) = -1 = 1 \cdot (-1) = \theta(0)\theta(1), \\ \theta(0 + 0) &= \theta(0) = 1 = 1 \cdot 1 = \theta(0)\theta(0), \\ \theta(1 + 1) &= \theta(0) = 1 = (-1) \cdot (-1) = \theta(1)\theta(1). \end{aligned}$$

Autrement dit, « additionner » dans \mathbb{Z}_2 revient au même que de « multiplier » dans $\{+1, -1\}$.

- (b) Les groupes 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.
- (c) De manière plus imagée, la Figure 2.1 illustre comment le groupe des symétries du triangle équilatéral, le groupe diédral D_3 , est isomorphe au groupe S_3 (voir l'exercice 2.13).

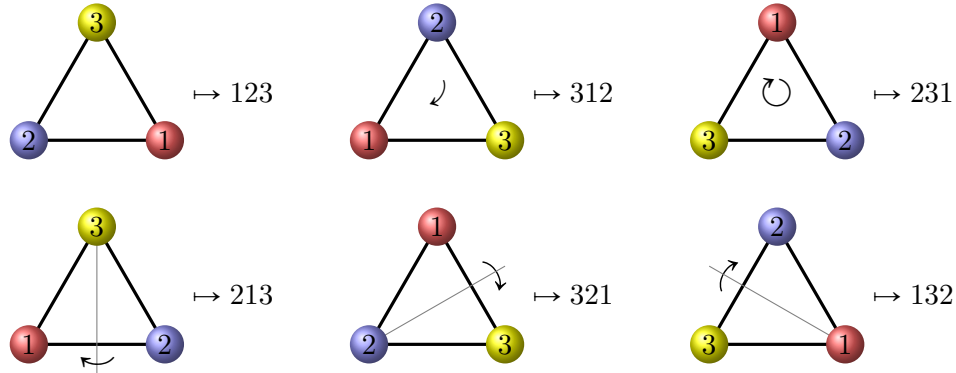
Proposition 2.5. *Soit E un ensemble non vide.*

- (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 $f : E \rightarrow F$. Il suffit de montrer que la fonction

$$\alpha : S_E \rightarrow S_F, \quad \text{avec} \quad \alpha(g) := f \circ g \circ f^{-1},$$

4. sur l'ensemble des groupes contenus dans un « univers » donné

FIGURE 2.1 – Isomorphisme entre les symétries du triangle et S_3 .

est un isomorphisme de groupes. On vérifie facilement que l'inverse de α est $\alpha^{-1} := S_F \rightarrow S_E$, 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

$$\begin{aligned}
 \alpha(g \circ g') &= f \circ g \circ g' \circ f^{-1} \\
 &= f \circ g \circ \text{Id}_E \circ g' \circ f^{-1} \\
 &= f \circ g \circ \text{Id}_E \circ g' \circ f^{-1} \\
 &= (f \circ g \circ f^{-1}) \circ (f \circ g' \circ f^{-1}) \\
 &= \alpha(g) \circ \alpha(g').
 \end{aligned}$$

La proposition est donc démontrée. ■

2.1.2 Noyau et image d'un morphisme de groupes

La notion d'isomorphisme est des plus importantes car elle permet de réduire l'étude des groupes à l'étude d'un représentant de sa classe d'isomorphisme. Nous allons discuter plus précisément la structure de bijection en rapport avec celle de groupes.

On rappelle qu'une application est bijective si et seulement si elle est surjective et injective. Un morphisme de groupes surjectif est appelé un **épimorphisme**, et on utilise la notation ⁵

$$\theta : G \twoheadrightarrow G' .$$

On dit d'un morphisme injectif, que c'est un **monomorphisme**, et on écrit

$$\theta : G \hookrightarrow G' .$$

5. Avec une flèche spéciale qui indique la surjectivité

- Exemples.** (a) Pour tout $n \in \mathbb{N}^*$, la fonction $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ définie par $\pi(k) = (k \bmod n)$ est un épimorphisme. Comme on le verra plus tard, c'est un cas spécial de « surjection canonique ».
- (b) Si H est un sous-groupe de G , alors l'inclusion $\iota : H \rightarrow G$, telle que $\iota(g) = g$, est un morphisme de groupes injectif appelé « injection canonique ».
- (c) Si $\theta : G \rightarrow G'$ un monomorphisme alors les groupes G et $\text{Im}(\theta)$ sont isomorphes.

Définition. Le **noyau**, noté $\ker(\theta)$, est le sous-groupe de G formé de l'image inverse de e' par θ , c.-à-d.

$$\ker(\theta) := \theta^{-1}(e') = \{g \in G \mid \theta(g) = e'\}.$$

La terminologie vient du terme allemand « kern », qui signifie noyau. C'est une notion naturelle qui apparaît dans de nombreux contextes algébriques (voir Exercice ??). D'autre part, on considère aussi **l'image d'un morphisme θ**

$$\text{Im}(\theta) := \theta(G) = \{\theta(x) \mid x \in G\}.$$

Il découle de la Proposition 2.1, que $\text{Im}(\theta)$ 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 2.6. *Si $\theta : G \rightarrow G'$ est un morphisme de groupes, alors*

- (1) *le noyau $\ker(\theta)$ est un sous-groupe de G ;*
- (2) *θ est injectif si et seulement si $\ker(\theta) = \{e\}$; et*
- (3) *θ est surjectif si et seulement si $\text{Im}(\theta) = G'$.*

En particulier, θ est un isomorphisme si et seulement si $\text{Im}(\theta) = G'$ et $\ker(\theta) = \{e\}$.

Démonstration. 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 $x_1 = x_2$. ■

Exemple (Le groupe alterné). 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, $\varepsilon : S_n \rightarrow \{+1, -1\}$. 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 2.2. 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 1.51, que les éléments de A_5 sont d'ordre 1, 2, 3, ou 5.

2.1.3 Classifier les groupes finis ?

Le problème de trouver une classification des groupes finis peut maintenant prendre un sens précis. **Problème** (Classification des groupes finis). Donner, à isomorphisme près, la liste de tous les groupes d'un ordre donné.

Pour $n \leq 16$, 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 Encyclopedia of Integer Sequences](#) ». Les premiers termes sont :

$$0, 1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, 5, 1, 2, 1, 14, 1, 5, 1, 5, 2, 2, 1, 15, 2, 2, 5, 4, 1, 4, 1, 51, 1, \dots$$

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

$$1, 1, 2, 5, 14, 51, 267, 2328, 56092, 10494213, 49487365422, \dots$$

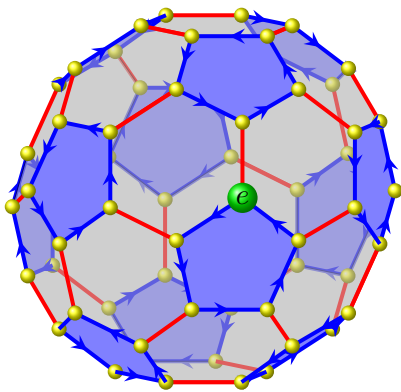


FIGURE 2.2 – Graphe de Cayley de A_5 , pour les générateurs (12345) et $(12)(34)$.

Nous verrons au Chapitre 6 comment on peut construire tous les groupes abéliens finis.

Le problème de la classification des groupes finis n'est pas, à date, résolu. Ce problème se décompose en fait en deux problèmes distincts.

Le premier est de donner une classification des groupes finis simples ⁶. On a depuis les années 1980 une classification complète des groupes simples finis, que l'on peut trouver ici : [Liste des groupe finis simples](#). Parmi ceux-ci, on a des familles infinies :

- La famille des groupes \mathbb{Z}_p pour p premier, qui n'ont aucun sous-groupe non trivial.
- La famille des groupes alternés A_n , avec $n \geq 5$. 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.

6. On en donnera la définition un peu plus loin dans ce chapitre.

– Seize familles de groupes de Lie.

On a de plus 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 1.4.2). Bien entendu, du fait de 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 $n \geq 5$. Pour les autres entiers k , il est 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, **7920**, 9828, 12180, 14880, 25308, ...

Le second est le problème de l'extension des groupes finis, qui est toujours un problème ouvert à l'heure actuelle.

Problème. Soit H, K deux groupes, donner, à isomorphisme près, la liste de tous les groupes G qui sont solution de la suite exacte courte suivante :

$$e \hookrightarrow H \hookrightarrow G \twoheadrightarrow K \twoheadrightarrow e$$

(voir Exercice 3.22 pour plus de détails sur les suites exactes courtes).

2.2 Morphismes particuliers et théorème de Cayley

2.2.1 Morphismes et produit direct de groupes

Au chapitre 1, nous avons montré que le produit cartésien $G_1 \times \cdots \times G_n$ de groupes G_1, \dots, G_n est naturellement muni d'une structure de groupes avec la loi de composition interne :

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) := (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

La proposition suivante est très utile afin d'obtenir facilement des morphismes de groupes dans le cas d'un groupe qui est produit cartésien de groupes.

Proposition 2.7. Si $\theta_i : G_i \rightarrow G'_i$, pour $1 \leq i \leq n$, sont des morphismes de groupes, alors on a un morphisme produit

$$\theta_1 \times \cdots \times \theta_n : G_1 \times \cdots \times G_n \rightarrow G'_1 \times \cdots \times G'_n$$

définie en posant

$$(\theta_1 \times \cdots \times \theta_n)(x_1, \dots, x_n) = (\theta_1(x_1), \dots, \theta_n(x_n)),$$

pour (x_1, \dots, x_n) dans $G_1 \times \dots \times G_n$. Si les θ_i sont des monomorphismes (resp. épimorphisme, ou isomorphisme), alors $\theta_1 \times \dots \times \theta_n$ est un monomorphisme (resp. épimorphisme, ou isomorphisme). Dans le cas où les θ_i sont des isomorphismes, l'inverse de $(\theta_1 \times \dots \times \theta_n)$ est $(\theta_1^{-1} \times \dots \times \theta_n^{-1})$, et c'est donc un isomorphisme.

Démonstration. Exercice. ■

Injection et projection canonique, propriété universelle. Pour chaque k , entre 1 et n , on a un monomorphisme de groupes $\iota_k : G_k \rightarrow G_1 \times \dots \times G_n$, défini en posant

$$\iota_k(x) := (\underbrace{e, \dots, e}_{k-1}, x, e, \dots, e),$$

et un épimorphisme de groupes $\pi_k : G_1 \times \dots \times G_n \rightarrow G_k$, simplement définis en posant

$$\pi_k(x_1, \dots, x_n) := x_k.$$

On dit de ι_k que c'est l'**inclusion canonique** de G_k dans le produit, et de π_k que c'est la k^e **projection canonique** sur la composante G_k . On vérifie aisément que $\pi_k \circ \iota_k = \text{Id}$, ou formulé en terme diagramme commutatif :

$$\begin{array}{ccc} G_k & \xrightarrow{\iota_k} & G_1 \times \dots \times G_n \\ & \searrow \text{Id} & \downarrow \pi_k \\ & & G_k \end{array}$$

La **propriété universelle** qui caractérise le produit direct de groupes fait l'objet de la proposition suivante. Elle permet en particulier d'étendre facilement des morphismes de groupes au produit directe des groupes images.

Proposition 2.8. *Pour tout groupe H , et des morphismes $\theta_1 : H \rightarrow G_1$ et $\theta_2 : H \rightarrow G_2$, il existe un unique morphisme $\theta : H \rightarrow G_1 \times G_2$, tel que*

$$\pi_1 \circ \theta = \theta_1, \quad \text{et} \quad \pi_2 \circ \theta = \theta_2.$$

On a alors $\theta(h) = (\theta_1(h), \theta_2(h))$, pour tout $h \in H$ et on écrit $\theta = (\theta_1, \theta_2)$. Formulé en terme de diagramme commutatif, ceci prend la forme

$$\begin{array}{ccccc} & & & G_1 & \\ & & & \uparrow \pi_1 & \\ & & & G_1 \times G_2 & \\ & & & \downarrow \pi_2 & \\ & & & G_2 & \\ H & \xrightarrow{\theta_1} & & & \\ & \dashrightarrow \exists! \theta & \rightarrow & & \\ & \xrightarrow{\theta_2} & & & \end{array}$$

Démonstration. Exercice. ■

2.2.2 Le produit direct interne

Nous allons donner ici un critère qui, si vérifié, permet de montrer qu'un groupe est isomorphe à un produit direct de groupes : c'est la notion de produit direct interne, dont la définition passe par la proposition suivante.

Proposition 2.9. *Soit G un groupe et H et K deux sous-groupes de G tels que*

$$xy = yx, \forall (x, y) \in H \times K \text{ et } H \cap K = \{e\}.$$

Alors l'ensemble $HK := \{hk \mid h \in H, k \in K\}$ est un sous-groupe de G , on a l'égalité $HK = KH$ et $HK \simeq H \times K$. En particulier, si plus $G = HK$, alors $G \simeq H \times K$.

Démonstration. Montrons d'abord que $HK = KH$ est un sous-groupe de G . On a $e = e.e \in HK$. De plus, si $h_1k_1, h_2k_2 \in HK$ alors par hypothèse on a :

$$h_1k_1(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1} = h_1h_2^{-1}(k_1k_2^{-1}) \in HK.$$

Maintenant, comme $hk = kh$ pour tout $h \in H$ et $k \in K$, on a par définition : $HK = KH$.

Considérons maintenant la fonction $\varphi : H \times K \rightarrow HK$, avec $\varphi(x, y) := xy$. Cette fonction est par définition surjective. En fait φ est un épimorphisme de groupes puisqu'on a les deux égalités :

$$\begin{aligned} \varphi((x_1, y_1) \cdot (x_2, y_2)) &= \varphi(x_1x_2, y_1y_2) = x_1x_2y_1y_2 \\ \varphi(x_1, y_1) \cdot \varphi(x_2, y_2) &= (x_1y_1) \cdot (x_2y_2) = x_1y_1x_2y_2, \end{aligned}$$

et ces deux expressions sont égales car les éléments de H et K commutent. De plus 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 $(x, y) = (e, e)$ et $\ker \varphi = \{(e, e)\}$. On en conclut que φ est un isomorphisme. ■

Définition. On dit que G est **produit direct interne** des sous-groupes H et K si H et K satisfont les conditions de la proposition 2.9. 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.

Exemple. Le groupe $G = \mathbb{Z}_6$ est produit direct interne de ses sous-groupes $H = \langle 3 \rangle$ et $K = \langle 2 \rangle$. En effet $H = \{0, 3\}$, $K = \{0, 2, 4\}$ et G est abélien donc les hypothèses de la Proposition 2.9 sont vérifiées aisément.

Remarque. Supposons que, dans la proposition 2.9, G est un groupe fini et que H et K satisfont aux hypothèses. Alors $HK \simeq H \times K$ est un groupe fini de cardinal $|HK| = |H||K| \leq |G|$. De plus $G = HK$ si et seulement si $|G| = |H||K|$ dans ce cas.

2.2.3 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 groupe symétrique S_n , pour un certain $n \in \mathbb{N}^*$. Autrement dit, bien connaître S_n peut permettre d'aider à comprendre tous les groupes finis. Le théorème qui suit est d'une grande importance et est dû au mathématicien anglais **Arthur Cayley** (1821-1895), un des pionniers de la théorie des groupes.

Théorème 2.10 (Théorème de Cayley). *Tout groupe G est isomorphe à un sous-groupe de S_G , le groupe de ses permutations. En particulier, si G est un groupe fini de cardinal $n \in \mathbb{N}^*$, alors G est isomorphe à un sous-groupe de S_n .*

Démonstration. Il suffit de construire un morphisme de groupes injectif $\Phi : G \rightarrow S_G$. Pour chaque $g \in G$, on considère la fonction $\Phi_g : G \rightarrow G$, 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 $\Phi : G \rightarrow S_G$, 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)

$$\begin{aligned} \Phi(g) \circ \Phi(h) &= \Phi_g \circ \Phi_h \\ &= \Phi_{gh} \\ &= \Phi(gh). \end{aligned}$$

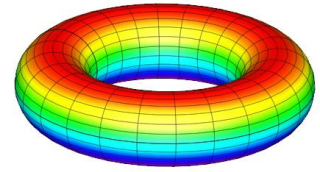
D'autres parts, Φ est injectif. En effet, si $g \in \ker(\Phi)$ alors $\Phi_g = \text{Id}$. Donc $\Phi_g(x) = gx = x$ pour tout $x \in G$, et donc $g = e$. On conclut donc que Φ est un monomorphisme de groupe, de G vers S_G . Le dernier énoncé du théorème est alors une conséquence de la proposition 2.5. ■

Exemple. Comme $|\mathbb{Z}_3| = 3$, on a par le Théorème de Cayley 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 .

Remarque. Le théorème de Cayley est d'une grande importance théorique, car il montre que l'on peut utiliser les technologies développées pour les groupes symétriques afin d'étudier tous les groupes. Par contre, en ce qui concerne la pratique, il est parfois très difficile d'utiliser ce théorème pour étudier des groupes finis à très grands cardinaux, car le groupe symétrique sera lui encore bien plus grand. Par exemple, \mathbb{Z}_9 est, à isomorphisme près, un sous-groupe de S_9 de cardinal 9!

Afin de pallier à ce problème pratique, nous allons développer dans le Chapitre 4 la notion d'action de groupes qui nous permettra de réduire l'ordre du groupe symétrique considéré pour étudier un groupe donné.

2.3 Sous-groupes normaux et produit semi-direct



Nous avons vu dans la section précédente une condition selon laquelle un groupe peut être décomposé en produit direct de groupes. Malheureusement ces conditions ne sont pas toujours vérifiées. Il est alors naturel d'affaiblir les conditions de la proposition 2.9. Pour cela, on va considérer une classe de sous-groupes H d'un groupe G : ceux dont l'ensemble des classes à gauche et égal à l'ensemble des classes à droites.

2.3.1 Sous-groupes normaux

Définition. Un sous-groupe H d'un groupe G est dit **normal** (ou **distingué**) si $xH = Hx$ pour tout $x \in G$. On écrit alors $H \triangleleft G$.

Un groupe est dit **groupe simple**⁷ si ses seuls sous-groupes normaux sont lui-même ou $\{e_G\}$.

Exemple. (a) 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 $xZ(G) = Z(G)x$.

(b) Tout sous-groupe d'indice 2 est normal (exercice).

Proposition 2.11. *Le noyau $\ker(\theta)$ d'un morphisme de groupes $\theta : G \rightarrow G'$ est un sous-groupe normal de G . En particulier, si G est un groupe simple, alors les morphismes de groupes non-triviaux $\theta : G \rightarrow H$ sont forcément des isomorphismes.*

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 G simple, alors si θ n'est pas trivial, 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 isomorphisme. ■

Proposition 2.12. 1. *Tout sous-groupe d'un groupe abélien G est normal.*

2. *L'intersection de sous-groupes normaux est un sous-groupe normal.*

3. *Si $G = \langle S \rangle$ est un groupe et $H = \langle T \rangle$ est un sous-groupe de G , avec $S, T \subseteq G$, alors $H \triangleleft G$ si et seulement si $sts^{-1} \in H$ pour tout $s \in S$ et $t \in T$.*

Démonstration. Voir la question d'auto-évaluation 2.10. ■

7. Cette notion est fondamentale dans l'étude du problème de classification des groupes finis, voir §2.1.3

- Remarque.** (a) La condition $H, K \leq G$ tel que $H \cap K = \{e\}$. Alors $hk = kh$ pour tout $(h, k) \in H \times K$ si et seulement si $H, K \triangleleft G$. Ceci est une condition utile afin d'appliquer la proposition 2.9 (exercice).
- (b) Attention, la relation « \triangleleft » n'est pas transitive. Autrement dit, on peut avoir $K \triangleleft H$ et $H \triangleleft G$, sans que $K \triangleleft G$. On trouve un exemple de cette non-transitivité dans S_4 (voir exercice 2.12). Par contre, si K est sous-groupe de H , lui-même sous-groupe de G , alors

$$K \triangleleft G \implies K \triangleleft H.$$

En effet, on a $xK = Kx$ pour tout $x \in G$ donc aussi pour tout $x \in H$.

2.3.2 Produit semi-direct interne

Définition. Soit G un groupe, $H \leq G$ un sous-groupe de G et $N \triangleleft G$ un sous-groupe normal de G . On munit l'ensemble $N \times H$ de la loi de composition suivante interne suivante :

$$(x, h)(y, g) = (xhyh^{-1}, hg).$$

On appelle alors l'ensemble $N \times H$ munit de cette loi de composition, noté⁸ $N \rtimes H$, le **produit semi-direct interne de N par H dans G** .

Proposition 2.13. Soit G un groupe, $H \leq G$ et $N \triangleleft G$.

1. Le produit semi-direct interne $N \rtimes H$ de N par H est un groupe.
2. Supposons que $N \cap H = \{e\}$ et $G = NH$, alors $G \simeq N \rtimes H$.

Démonstration. Exercice. ■

Exemple. Le lecteur vérifiera en exercice que le groupe diedral S_3 est isomorphe au produit semi-direct $\langle(123)\rangle \rtimes \langle(12)\rangle$.

2.3.3 Automorphismes intérieurs

Avant de définir le produit-semi-direct en toute généralité, nous allons discuter d'un sous-ensemble de $\text{Aut}(G)$ qui est lié à la conjugaison dans les groupes. La question, pour un groupe G de fixé, de calculer le groupe $\text{Aut}(G)$ des automorphismes de G est une question difficile.

Pour tout groupe G , et $g \in G$, la fonction de **conjugaison par g** est :

$$\varphi_g : G \rightarrow G \quad \text{définie par} \quad \varphi_g(x) := gxg^{-1}.$$

8. L'ordre de N et H est important, puisqu'il indique quel est le sous-groupe (le premier) qui est forcément normal.

On dit souvent, au lieu d'écrire $\varphi_g(x)$, que l'on **conjugue x par g** . La conjugaison par un élément d'un groupe est en fait un automorphisme de G qu'on appelle un **automorphisme intérieur**. On observe facilement qu'un sous-groupe H de G est normal si et seulement si $\text{Int}(G) \subseteq \text{Aut}(H)$.

Afin de montrer que φ_g est un automorphisme de G , on montre d'abord que cette fonction est un endomorphisme de G : pour $x, y \in G$ on a

$$\begin{aligned} \varphi_g(x)\varphi_g(y) &= (gxg^{-1})(gyg^{-1}) \\ &= gx(g^{-1}g)yg^{-1} \\ &= gxe yg^{-1} \\ &= gxyg^{-1} \\ &= \varphi_g(xy). \end{aligned}$$

De plus, φ_g admet comme fonction inverse $\varphi_{g^{-1}}$, c'est donc une bijection. 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 $\varphi_{g^{-1}} \circ \varphi_g = \text{Id}_G$. De même, on vérifie que $\varphi_{g^{-1}}$ est inverse à droite de φ_g .

On note $\text{Int}(G)$ l'ensemble des automorphismes intérieurs de G . On observe que $\text{Int}(G)$ peut être bien plus petit que G . Par exemple, si G est abélien, alors $\text{Int}(G) = \{e\}$. En fait, $\text{Int}(G)$ est un groupe comme le montre la proposition suivante.

Proposition 2.14. *Soit G un groupe, alors $\text{Int}(G)$ est un sous-groupe normal de $\text{Aut}(G)$. En particulier, $\varphi_{gh} = \varphi_g \circ \varphi_h$ et $\varphi_g^{-1} = \varphi_{g^{-1}}$ pour tout $g, h \in G$.*

Démonstration. Voir l'exercice 2.10. ■

2.3.4 Produits semi-directs

Proposition 2.15. *Soient G et F deux groupes et soit $\varphi \in \text{Hom}(G, \text{Aut}(F))$ un morphisme de groupes de G dans le groupe des automorphismes sur F . On notera ψ_g l'image de $g \in G$ par φ . On munit l'ensemble $F \times G$ de la loi de composition interne :*

$$(h, g)(h', g') = (h\psi_g(h'), gg').$$

Alors $F \times G$ munit de cette loi est un groupe que l'on note $F \rtimes_{\psi} G$ et l'on appelle **produit semi-direct**⁹ de F par G (relativement à ψ).

En particulier :

1. si ψ est l'application trivial (qui envoie G sur $\{\text{Id}_F\}$), alors $F \rtimes_{\psi} G = F \times G$.
2. si H, K sont deux sous-groupes d'un groupe G , $H \triangleleft G$, $H \cap K = \{e\}$ alors $H \rtimes K = H \rtimes_{\varphi} K$ où $\varphi \in \text{Hom}(K, \text{Aut}(H))$ est l'application définie en associant à $k \in K$ son automorphisme intérieur φ_k associé.

Démonstration. Voir l'exercice 2.29. ■

Exemple. Le groupe diédral D_n est isomorphe au produit semidirect $\mathbb{Z}_n \rtimes_{\varphi} C_2$, avec $\varphi : C_2 \rightarrow \text{Aut}(\mathbb{Z}_n)$ le morphisme $\varphi_i(k) := ik$; considérant que $C_2 = \{\pm 1\}$ est muni de 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 :

$$\begin{aligned} (k, 1) \cdot (\ell, 1) &= ((k + \ell \bmod n), 1), \\ (k, 1) \cdot (\ell, -1) &= ((k - \ell \bmod n), -1), \\ (k, -1) \cdot (\ell, 1) &= ((k + \ell \bmod n), -1), \\ (k, -1) \cdot (\ell, -1) &= ((k - \ell \bmod n), 1). \end{aligned}$$

Voir l'exercice 2.29 pour plus de détails.

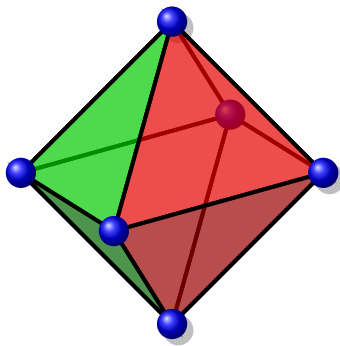


FIGURE 2.3 – L'octaèdre.

Exemple. (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 l'automorphisme $\varphi \in \text{Hom}(S_n, \text{Aut}((\mathbb{Z}_2)^n))$ est défini par :

$$\varphi_{\sigma}(k_1, k_2, \dots, k_n) := (k_{\sigma^{-1}(1)}, k_{\sigma^{-1}(2)}, \dots, k_{\sigma^{-1}(n)}).$$

9. La version « externe » du produit semi-direct mène à plusieurs domaines de recherche contemporains (algèbre homologique, topologie combinatoire, cohomologie de groupes, extensions de groupes, etc.) qui dépassent tous le niveau d'un premier cours sur la théorie des groupes.

Ici, on considère que \mathbb{Z}_2 est isomorphe à $C_2 = \{+1, -1\}$ 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}, σ) la matrice $(a_{ij})_{1 \leq i, j \leq n}$, 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 $2n$ points de la forme $(0, \dots, 0, \pm 1, 0, \dots, 0)$, 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

$$A = (1, 0, 0), \quad A^- = (-1, 0, 0), \quad B = (0, 1, 0), \quad B^- = (0, -1, 0), \quad C = (0, 0, 1), \quad \text{et } C^- = (0, 0, -1).$$

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

$$g \cdot A = B, \quad g \cdot A^- = B^-, \quad g \cdot B = A^-, \quad g \cdot B^- = A, \quad g \cdot C = C, \quad \text{et } g \cdot C^- = C^-.$$

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 .

2.4 Exercices

Questions d'auto-évaluation

Morphismes de groupes

Question 2.1. Vérifier que la relation d'isomorphisme est une relation d'équivalence. C'est-à-dire, 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 $G \simeq G''$.

Question 2.2. Soit $\theta : G \rightarrow G'$ un morphisme de groupes injectif.

- (a) Montrer que $G \simeq \theta(G) = \text{Im}(\theta)$.
- (b) Montrer que $\text{ord}(\theta(x)) = \text{ord}(x)$, 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.

Question 2.3. (a) Existe-t-il un morphisme de groupes surjectif $f : \mathbb{Z}_{24} \rightarrow \mathbb{Z}_5$? (Justifier)

(b) Existe-t-il un morphisme de groupes injectif $f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_{24}$? (Justifier)

Réponse : (a) non, le seul morphisme entre ces deux groupes est le morphisme trivial qui n'est pas surjectif dans ce cas ; (b) non car l'ordre de $\theta(\bar{1})$, $\bar{1} \in \mathbb{Z}_5$, serait 5 qui ne divise pas 24.

Question 2.4. Montrer que les applications suivantes sont des morphismes de groupes dont on déterminera le noyau, l'image et on spécifiera, en le justifiant, lesquelles sont injectives, surjectives ou bijectives :

(a) $f : \mathbb{R}^* \rightarrow \mathbb{R}^*$ définie par $f(x) = x^n$, où $n \in \mathbb{N}^*$.

(b) $f : \mathbb{R}^* \rightarrow \mathbb{R}^*$ définie par $f(x) = \frac{1}{x}$;

(c) $f : \mathbb{C}^* \rightarrow \mathbb{C}^*$ définie par $f(x) = |z|$;

(d) $f : (\mathbb{R}, +) \rightarrow (\mathbb{C}^*, \cdot)$ définie par $f(x) = \cos(x) + i \sin(x)$;

(e) $f : (\mathbb{C}, +) \rightarrow (\mathbb{C}^*, \cdot)$ définie par $f(z) = e^z$.

Question 2.5. 1. Montrer que les groupes \mathbb{R}^* et \mathbb{C}^* ne sont pas isomorphes.

Réponse : \mathbb{C} contient des éléments d'ordre 2 : i et $-i$

2. Montrer que les groupes \mathbb{R} et \mathbb{Q} ne sont pas isomorphes.

Réponse : ils n'ont pas la même cardinalité

3. Montrer que les groupes \mathbb{Z} et \mathbb{Q} ne sont pas isomorphes.

Réponse : \mathbb{Z} est cyclique, mais \mathbb{Q} ne l'est pas : si $\mathbb{Q} = \langle a/b \rangle$, alors chaque élément de \mathbb{Q} est de la forme na/b avec $n \in \mathbb{Z}$, ce qui n'est pas possible pour $1/2b$.

Morphismes de groupes particuliers et théorème de Cayley

Question 2.6. (Translation à gauche) Soit G un groupe. Pour chaque $g \in G$, on considère la fonction $\Phi_g : G \rightarrow G$, définie en posant $\Phi_g(x) := gx$.

(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?

Réponse : Non, car $\Phi_g(xy) = gxy \neq gxy = \Phi_g(x)\Phi_g(y)$.

(c) Montrer que $\Phi_g \circ \Phi_h = \Phi_{gh}$ pour tout $g, h \in G$.

Question 2.7. Soient G, H des groupes. Selon l'ordre choisi pour faire le produit cartésien, on obtient deux groupes, $G \times H$ et $H \times G$. Vérifier que l'application $\theta : G \times H \rightarrow H \times G$ définie par $\theta(g, h) = (h, g)$ est un isomorphisme.

Question 2.8. Montrer que le sous-groupe de S_n , $n \geq 4$, engendré par les transpositions simples $\tau_1 = (12)$ et $\tau_3 = (34)$ est isomorphe au groupe de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Sous-groupes normaux et produits semi-directs

Question 2.9. Pour chaque énoncé, indiquer s'il est vrai ou faux. Justifier la réponse.

1. Tout groupe non trivial possède au moins deux sous-groupes normaux distincts.

Réponse : **Vrai** : $\{e\}$ et G

2. Si H est un sous-groupe normal de G et $a \in G$, alors $ah = ha$ pour tout $h \in H$.

Réponse : **Faux**. $ah = h'a$ pour un $h' \in H$ avec $h' \neq h$ en général.

3. Si $H \triangleleft G$ et $f : G \rightarrow G'$ est un homomorphisme de groupes, alors $f(H) \triangleleft G'$.

Réponse : **Faux**. (**Vrai** si f est surjectif.) Contre-exemple : Soient

$$V = \{(), (12)(34), (13)(24), (14)(23)\}$$

$$H = \{(), (13)(24)\}$$

On a que $H \triangleleft V$ et $V \triangleleft S_4$, mais que H n'est pas un sous-groupe normal de S_4 . Alors, si $f : V \rightarrow S_4$ est l'application identité, alors $f(H)$, ce qui est H , n'est pas un sous-groupe normal de S_4 .

Question 2.10. Soit G un groupe et $H \leq G$.

- (1) Montrer que les énoncés suivants sont équivalents.

- (a) $H \triangleleft G$;
- (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 $h \in H$.

- (2) Démontrer la proposition 2.12.

- (3) Si $H = \langle T \rangle$, montrer que $H \triangleleft G$ si et seulement si $gtg^{-1} \in T$ pour tout $g \in G$.

Réponse : Il suffit de voir que $G = \langle G \rangle$ et d'appliquer la proposition 2.12.

- (4) Si $G = \langle S \rangle$, montrer que $H \triangleleft G$ si et seulement si $shs^{-1} \in H$ pour tout $s \in S$.

Question 2.11. Soit G un groupe et $H, K \leq G$, montrer que

- (a) si $H \triangleleft G$ et $K \leq G$ contenant H alors $H \triangleleft K$;
- (b) $H \triangleleft G \implies H \cap K \triangleleft G$;

Question 2.12. 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 $H \triangleleft K$ et $K \triangleleft S_4$, mais que H n'est pas normal dans S_4 .

Question 2.13. Trouver tous les sous-groupes normaux de S_3 .

Exercices

Exercice 2.1. Soit $\theta \in \text{Hom}(G, G')$.

- Montrer que si $H' \leq G'$ alors $\theta^{-1}(H') \leq G$.
- Montrer que si $S \subseteq G$, alors $\theta(\langle S \rangle) = \langle \theta(S) \rangle$.
- Montrer que si $x \in G$ alors $\text{ord}_{G'}(\theta(x))$ divise à la fois $\text{ord}_G(x)$ et $|\text{Im } \theta|$.
- Montrer que si θ est bijectif et G est abélien, alors G' est abélien. Est-ce que la surjectivité est suffisante ?
- Montrer que si θ est injectif et G' est abélien, alors G est abélien.

Exercice 2.2. Soient α et β les deux permutations suivantes.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

- Calculer les sous-groupes $\langle \alpha \rangle$, $\langle \beta \rangle$, et $\langle \alpha, \beta \rangle$ de S_4 .
- Montrer que $\langle \alpha, \beta \rangle$ et $(\mathbb{Z}_8)^\times$ sont isomorphes.
- Déterminer tous les morphismes de $\langle \alpha, \beta \rangle$ dans \mathbb{Z}_4 . Pour chaque morphisme, déterminer son noyau et son image.

Exercice 2.3. Soit

$$G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R}, (a, b) \neq (0, 0) \right\}.$$

- Montrer que G muni de la multiplication matricielle est un sous-groupe de $\text{GL}_2(\mathbb{R})$.
- Montrer que G est isomorphe au groupe \mathbb{C}^* .

Exercice 2.4. Soient $f : G \rightarrow H$ et $g : H \rightarrow K$ des homomorphismes de groupes. Montrer que $g \circ f$ est trivial si et seulement si $\text{Im}(f) \subseteq \ker(g)$.

Exercice 2.5. 1. Soient G' un groupe et $f : \mathbb{Z}/31\mathbb{Z} \rightarrow G'$ un homomorphisme non trivial. Montrer que f est injectif.

- Soient G un groupe et $g : G \rightarrow \mathbb{Z}/23\mathbb{Z}$ un homomorphisme non trivial. Montrer que g est surjectif.

Exercice 2.6. 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

$$\theta : (\mathbb{Z}_6, +) \rightarrow (\mathbb{Z}_3, +) , \quad \text{définie en posant} \quad \theta([k]_6) := [k]_3.$$

- Montrer que θ est bien définie, à savoir qu'on a toujours que si $[k]_6 = [m]_6$ alors $[k]_3 = [m]_3$.
- 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 2.7. Soient G un groupe abélien fini d'ordre n et soit $m \in \mathbb{N}$ tel que $\text{pgcd}(m, n) = 1$. Montrer que l'application $f(x) = x^m$ est un automorphisme de G .

Exercice 2.8. Soit $a \in \mathbb{Q}^*$, on pose $f_a : \mathbb{Q} \rightarrow \mathbb{Q}$ l'application définie par

$$f_a(x) = ax.$$

(a) Montrer que f_a est un automorphisme du groupe additif \mathbb{Q} .

(b) Montrer que si φ est un endomorphisme du groupe additif \mathbb{Q} , alors pour tout $n \in \mathbb{Z}$ et $m \in \mathbb{N}^*$, on a :

$$\varphi(n) = n\varphi(1) \quad \text{et} \quad \varphi\left(\frac{n}{m}\right) = \frac{n}{m}\varphi(1).$$

(c) Montrer que l'application suivante est un isomorphisme de groupes :

$$\begin{aligned} \varphi : \mathbb{Q}^* &\longrightarrow \text{Aut}(\mathbb{Q}) \\ a &\longmapsto f_a \end{aligned}$$

(d) Trouver tous les automorphismes du groupe $(\mathbb{Z}, +)$.

(e) Trouver tous les automorphismes du groupe $(\mathbb{Q}, +)$.

Exercice 2.9. Soit G un groupe fini dont l'élément neutre est noté e . Soit $\varphi : G \rightarrow G$ un isomorphisme tel que si $\varphi(g) = g$, alors $g = e$.

(a) Montrer que tout élément de G s'exprime sous la forme $g^{-1}\varphi(g)$.

(b) Si φ est d'ordre 2, montrer que $\varphi(g) = g^{-1}$ pour tout $g \in G$ et que G est un groupe abélien d'ordre impair.

Exercice 2.10. Soit G un groupe. On utilise ici les notations de la section 2.3.3.

(a) Montrer que l'ensemble $\text{Int}(G)$ des morphismes intérieurs du groupe G est un sous-groupe normal de $\text{Aut}(G)$.

(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 $|\text{Int}(G)| \leq |G|$.

(d) Calculer $\text{Int}(S_3)$ et $\text{Int}(\mathbb{Z}_n)$.

Exercice 2.11 (Version forte du théorème de Cayley). Soit H un sous-groupe d'un groupe G tel que $[G : H] = m \in \mathbb{N}$. On définit

$$\begin{aligned} \Phi : G &\rightarrow S_{G/H} \\ \Phi(g)(xH) &= (gx)H \end{aligned}$$

où $S_{G/H}$ est le groupe de permutations de l'ensemble G/H . (Donc, $S_{G/H} \cong S_m$.)

- (a) Montrer que Φ est un homomorphisme de groupes.
- (b) Montrer que si H est un sous-groupe normal de G , alors H est le noyau de Φ . Sinon, $\ker(\Phi)$ est le plus grand sous-groupe normal de G contenu dans H .
- (c) Montrer que $g^{m!} \in H$ pour tout élément $g \in G$.
(Remarquer que H n'est pas forcément normal.)

Exercice 2.12. Soient n and m des entiers positifs. Montrer à l'aide de la théorie des groupes que $n!m!$ divise $(n+m)!$. (Indice : trouver un sous-groupe approprié de S_{n+m} et appliquer le théorème de Lagrange.)

Exercice 2.13. Montrer que :

- (a) le groupe diédral D_m est isomorphe à un sous-groupe de S_m pour tout entier $m \geq 3$. En déduire que $D_3 \simeq S_3$.
- (b) \mathbb{Z}_n est isomorphe à un sous-groupe de S_n pour tout entier $n \in \mathbb{N}$.

Exercice 2.14. Soit $\theta : G \rightarrow G'$ un morphisme de groupes, montrer que

- (a) si $H \triangleleft G$ alors $\theta(H) \leq \theta(G)$, et que si θ est surjectif alors $\theta(H) \triangleleft G'$. Est-ce vrai dans le cas où θ n'est pas surjectif?
- (b) Si $H' \triangleleft G'$ alors $\theta^{-1}(H') \triangleleft G$.

Exercice 2.15. Soit G un groupe et $H \leq G$ d'indice 2, montrer que H est normal dans G .

Exercice 2.16. Soit H un sous-groupe normal de G . Montrer que si H est monogène, alors tout sous-groupe de H est un sous-groupe normal de G .

Exercice 2.17. 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 2.18. Soit G un groupe et $H, K \leq G$.

- (a) Montrer que $HK \leq G \iff HK = KH$.
- (b) Montrer que si $HK \leq G$ alors $HK = \langle H \cup K \rangle$. Est-ce que dans ce cas HK est abélien?
- (c) Montrer que si $H \triangleleft G$ alors $HK \leq G$ et $H \triangleleft HK$.

Exercice 2.19. Soit G un groupe. Soit H, K des sous-groupes de G tel que $H \cap K = \{e\}$ et $G = HK$. Montrer que H et K sont des sous-groupes normaux de G si et seulement si $hk = kh$, pour tout $(h, k) \in H \times K$. En déduire que si H, K sont des sous-groupes normaux de G , $H \cap K = \{e\}$ et $G = HK$, alors $G \simeq H \times K$.

Exercice 2.20. Démontrer la Proposition 2.7.

Exercice 2.21. Démontrer la Proposition 2.8.

Exercice 2.22. Soit G_1, \dots, G_n des groupes Pour σ une permutation dans S_n . Vérifier que l'application

$$\varphi_\sigma : G_1 \times \dots \times G_n \rightarrow G_{\sigma(1)} \times \dots \times G_{\sigma(n)}$$

définie par

$$\varphi_\sigma(g_1, \dots, g_n) = (g_{\sigma(1)}, \dots, g_{\sigma(n)})$$

est un isomorphisme.

Exercice 2.23. Soit A un groupe abélien, B un sous-groupe de A , et $\theta : A \rightarrow B$ un morphisme de groupes 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 .

Exercice 2.24. Démontrer la Proposition 2.13.

Exercice 2.25. Soit $\varphi : G \rightarrow G'$ et $\psi : G' \rightarrow G$ deux morphismes de groupes tel que $\psi \circ \varphi = \text{Id}_G$.

- (a) Montrer que ψ est surjective.
- (b) Montrer que φ est injective.
- (c) Montrer que $\ker(\psi) = \ker(\varphi \circ \psi)$.
- (d) Montrer que $G' \simeq \ker \psi \rtimes \varphi(G)$.

Exercice 2.26. (a) Le groupe diédral \mathcal{D}_6 est engendré par la rotation r d'ordre 6 et la réflexion s d'ordre 2. Soit $H = \langle r^2, s \rangle$ et $K = \langle r^3 \rangle$.

- (i) Montrer que H et K sont des sous-groupes normaux de \mathcal{D}_6 .
- (ii) Montrer que $H = \mathcal{D}_3$ et $K \simeq \mathbb{Z}/2\mathbb{Z}$.
- (iii) Montrer que $\mathcal{D}_6 \simeq \mathcal{D}_3 \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 2.27 (Produit direct interne de plusieurs sous-groupes). Soit G un groupe et soit H_1, \dots, H_n des sous-groupes normaux de G .

- (a) 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 $g = h_1 h_2 \dots h_n, h_i \in H_i$.

- (b) On suppose que

$$H_i \cap \langle H_1 \cup \dots \cup \widehat{H_i} \cup \dots \cup H_n \rangle = \{e\},$$

pour tout $1 \leq i \leq n$, et

$$G = H_1 H_2 \dots H_n.$$

Montrer que

$$G \simeq H_1 \times H_2 \times \dots \times H_n.$$

On dit alors que G est le **produit direct interne** de ses sous-groupes normaux H_1, \dots, H_n .

- (c) Montrer que \mathbb{Z}_{30} est produit direct interne de ses sous-groupes $\langle 15 \rangle$, $\langle 10 \rangle$ et $\langle 6 \rangle$.

Exercice 2.28. Soit G un groupe, $N \triangleleft G$ un sous-groupe normal de G et $H \leq G$ un sous-groupe de G tel que $G = N \rtimes H$ est un produit semi-direct interne. Si $K \leq G$ tel que $N \subseteq K$, montrer que $K \simeq N \rtimes (K \cap H)$.

Exercices exploratoires

Exercice 2.29 (Produit semidirect externe). Soient G et H deux groupes et soit $\varphi \in \text{Hom}(G, \text{Aut}(H))$ un morphisme de groupes de G dans le groupe des automorphismes sur H . On notera φ_g l'image de $g \in G$ par φ . On munit l'ensemble $H \times G$ de la loi de composition interne : $(h, g)(h', g') = (h\varphi_g(h'), gg')$.

- (a) Montrer que $H \times G$ munit de cette loi est un groupe. Déterminer φ pour que cette structure soit le produit direct.

Ce groupe sera noté $H \rtimes_{\varphi} G$ (ou plus simplement $H \rtimes G$) et est appelé *produit semi-direct de H par G (relativement à φ)*.

- (b) Soit H, K deux sous-groupes de G .

(a) Montrer que si $HK = KH$ alors HK est un sous-groupe de G .

(b) Supposons que $G = HK$, H est normal dans G et $K \cap H = \{e\}$. Montrer que $G \simeq H \rtimes K$ pour un automorphisme de H que l'on précisera.

(c) Avec les mêmes hypothèses que ci-dessus, montrer que $G \simeq H \times K$ si et seulement si $kh = hk$, pour tout $k \in K$ et $h \in H$.

- (c) Soit $m \geq 3$. Montrer que $\mathcal{D}_m \simeq \mathbb{Z}/m\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$ où $\varphi_{1+2\mathbb{Z}}(1 + m\mathbb{Z}) = m - 1 + m\mathbb{Z}$.

Exercice 2.30 (Le groupe alterné A_4). On considère le groupe alterné A_4 .

- (a) Écrire les éléments de A_4 en produit de cycles disjoints et donner leurs ordre.

(b) Montrer que $H = \langle (12)(34), (14)(23) \rangle$ est un sous-groupe normal de A_4 isomorphe au groupe de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) Soit σ un 3-cycle dans A_4 . On pose $K = \langle \sigma \rangle$. Montrer que $A_4 \simeq H \rtimes K \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\psi} \mathbb{Z}_3$ pour un morphisme ψ que l'on précisera.

(d) Montrer que $A_4 = \langle (123), (12)(34) \rangle$.

(e) Montrer que le groupe alterné 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 2.31. Définir la notion de morphisme, de monomorphisme, d'épimorphisme, et d'isomorphisme de monoïdes. Pour toute bijection $f : E \rightarrow F$, on considère la fonction

$$\Phi_f : \text{Fonct}(E, E) \rightarrow \text{Fonct}(F, F),$$

qui envoie $g \in \text{Fonct}(E, E)$ 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 $\text{Im}(\theta)$, le noyau et l'image d'un morphisme de monoïde $\theta : M \rightarrow M'$, avec les définitions évidentes. Montrer qu'on a

- (a) Le noyau $\ker(\theta)$ est un sous-monoïde de M .

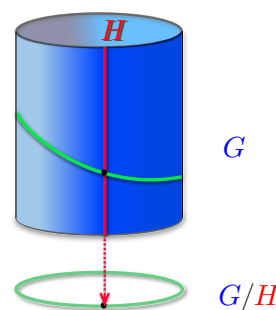
- (a) L'image $\text{Im}(\theta)$ est un sous-monoïde de M' .
- (b) θ est injectif si et seulement si $\ker(\theta) = \{e\}$;
- (c) θ est surjectif si et seulement si $\text{Im}(\theta) = M'$.

Exercice 2.32. Rappelons (voir Exercice 1.53) 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 concaténation. On considère ici le cas où A est un ensemble fini.

- (a) Soit $f : \mathcal{A}^* \rightarrow M$ 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 $\varphi : M \rightarrow \text{Fonct}(M, M)$, 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 $M \times E \rightarrow E$ est équivalente à la donnée d'un morphisme de monoïde $M \rightarrow \text{Fonct}(E, E)$.
- (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) $A \times E \rightarrow E$. Voir la notion de **monoïde syntaxique** en théorie des automates.

Chapitre 3

Groupes quotients, et théorèmes d'isomorphisme



Dans ce chapitre, nous allons développer d'autres outils importants pour la construction et l'étude de groupes, la notion de groupes quotients, qui mènera aux très utiles théorèmes d'isomorphisme. Nous généraliserons ainsi la construction de la structure de groupe sur l'ensemble quotient \mathbb{Z}_n provenant du groupe $(\mathbb{Z}, +)$ avec la relation modulo n associé au 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 $(\mathbb{Z}_n, +)$.

Enfin, dans une dernière partie, nous allons montrer que nous pouvons associer à tout ensemble de générateurs un ensemble de relations qui nous permettra de *présenter un groupe par générateurs et relations*. Dans le cas des espaces vectoriels et des leurs morphismes, les applications linéaires, nous savons que toute application linéaire est définie de façon unique en donnant l'image d'une base ce qui est très utile dans la pratique. Dans les cas des groupes et de leurs morphismes, nous verrons à la fin de ce chapitre que ce phénomène se généralise en considérant, à la place des bases, les générateurs **et** les relations.

3.1 Groupes quotients

En plus de son rôle dans la décomposition d'un groupe en produit semi-direct, le rôle principal de la notion de sous-groupe normal réside dans le rôle fondamental que ces sous-groupes jouent dans la construction de « groupes quotients ».

Pour que l'ensemble quotient (des classes à gauche) G/N admette une structure de groupe héritée

de celle G , comme c'est le cas pour \mathbb{Z}_n qui hérite la sienne de celle de \mathbb{Z} , il faut imposer à N certaines conditions : la notion de sous-groupe normal apparaît alors naturellement. Rappelons qu'un sous-groupe N d'un groupe G est dit normal si $xNx^{-1} = N$ pour tout $x \in G$ que l'on note alors $H \triangleleft G$.

Théorème 3.1. *Soit G un groupe et N un sous-groupe normal de G .*

1. *La loi de composition interne*

$$G/N \times G/N \longrightarrow G/N \quad \text{telle que} \quad (xN) \cdot (yN) := xyN \quad (3.1)$$

*munit G/N d'une structure de groupe appelée **groupe quotient de G par N** . L'élément neutre est la classe N et l'inverse de xN est $(xN)^{-1} = x^{-1}N$.*

Si G est fini, alors G/N est fini et $|G/N| = |G|/|N|$.

2. *La surjection naturelle*

$$\begin{aligned} \pi : G &\longrightarrow G/N \\ x &\longmapsto \pi(x) = xN \end{aligned}$$

*est un épimorphisme de groupes appelé **projection 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 **une application bien définie**, c.-à-d. que pour $xN, x'N, y'N$ tel que $xN = x'N$ et $yN = y'N$, il faut montrer que $xyN = x'y'N$. Puisque $N \triangleleft G$, 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

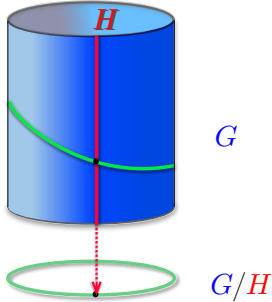
$$xN \cdot x^{-1}N = xx^{-1}N = N = x^{-1}N \cdot xN.$$

Si G est fini, le théorème de Lagrange nous donne immédiatement que $|G/N| = |G|/|N|$. Calculant que $\pi(xy) = xyN = xN \cdot yN = \pi(x) \cdot \pi(y)$, on constate que π est un morphisme de groupes, surjectif car $\pi(x) = xN$, pour tout $xN \in G/N$. De plus, on a déjà vérifié l'égalité suivante :

$$\{x \in G \mid xN = N\} = N = \ker(\pi).$$

Ce qui conclut la preuve. ■

Remarque. Comme $G/\{e\} \simeq G$, on écrit parfois $G/\{e\} = G$ par abus de notation.



Le corollaire suivant souligne le fait que les sous-groupes normaux coïncident avec les noyaux des morphismes de groupes.

Corollaire 3.2. Soit G un groupe et $H \leq G$, alors $H \triangleleft G$ si et seulement si il existe un morphisme de groupes $\theta : G \rightarrow G'$ tel que $H = \ker(\theta)$. En particulier, $\ker(\theta) \triangleleft G$, pour tout morphisme de groupes $\theta : G \rightarrow G'$.

Démonstration. Si $H \triangleleft G$, il suffit de prendre $\theta = \pi : G \rightarrow G/H$. Réciproquement, on sait que le noyau de tout morphisme de groupes est normal dans G . ■

Exemple. 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 .

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.

On montre cet énoncé par récurrence sur le cardinal de G . Soit G tel que $\text{ord}(g)$ est une puissance de 3, pour tout $g \in G$. Choisissons un élément $h \in G$, autre que e , ayant l'ordre $\text{ord}(h) = 3^k$. Puisque $g \neq 0$, on a $k \neq 0$. Posons $H = \{e, h, \dots, h^{3^k-1}\}$. Si $G = H$ alors on a fini, puisque $|G| = |H| = 3^k$. Autrement, on a $H \subset G$, avec $2 \leq |H| < |G|$. 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 $|H| \geq 2$. 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 $\pi : G \rightarrow G/H$, défini par $g \mapsto gH$. 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 $\text{ord}(gH)$, et donc $\text{ord}(gH)$ est une puissance de 3. L'hypothèse de récurrence s'applique donc à G/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.

Sous-groupes d'un groupe quotient. Afin de mieux comprendre la structure du groupe quotient G/N , en particulier en ce qui concerne ses sous-groupes, la proposition suivante est fondamentale.

Proposition 3.3. *Soit G un groupe, $N \triangleleft G$ et $\pi : G \rightarrow G/N$ 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 . De plus si K est un tel sous-groupe de G contenant N , alors $\pi(K) = K/N$. En particulier si G est fini, alors $|\pi(K)| = |K|/|N|$.*

Remarque. (a) On a $L \leq G/N$ si et seulement si il existe $N \leq K \leq G$ tel que $\pi(K) = L$. De plus dans ce cas, on a $N \triangleleft K$, le groupe K/N est bien défini et $L = K/N$.

(b) Si $K = \langle S \rangle$, on a $\pi(K) = \langle \pi(S) \rangle$.

Exemple. Les sous-groupes de \mathbb{Z}_6 sont donc les $\pi(\mathbb{Z}_k)$ où $6\mathbb{Z} \subseteq k\mathbb{Z}$. Donc, les seuls sous-groupes de \mathbb{Z}_6 sont donc : $\pi(\mathbb{Z}) = \langle \bar{1} \rangle = \mathbb{Z}_6$, $\pi(6\mathbb{Z}) = \{\bar{0}\}$, $\pi(3\mathbb{Z}) = 3\mathbb{Z}/6\mathbb{Z} = \langle \bar{3} \rangle \simeq \mathbb{Z}_2$ et $\pi(2\mathbb{Z}) = 2\mathbb{Z}/6\mathbb{Z} = \langle \bar{2} \rangle \simeq \mathbb{Z}_3$.

Démonstration. Soit $K \leq G$ 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 $xN, yN \in \pi(K)$ on a $x, y \in K$, et donc $xN(yN)^{-1} = xy^{-1}N = \pi(xy^{-1}) \in \pi(K)$. Il s'ensuit que $\pi(K) \leq G/N$. Autrement dit, la fonction $K \rightarrow \pi(K)$ est bien définie. Reste à montrer qu'elle est bijective.

Surjectivité : Soit $L \leq G/N$, posons $K = \pi^*(L) = \{g \in G \mid \pi(g) \in L\}$. 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 $L \leq G/N$, donc $xy^{-1} \in K$. Donc $K \leq G$. 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 $K' \leq G$, on obtient que $x \in K'$.

Maintenant, on sait que $\pi(K) \leq G/N$. 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

$$|G/N| = |G/K| \cdot |K/N|.$$



3.2 Théorèmes d'isomorphisme et applications

Les « théorèmes d'isomorphisme » ont pour but de décrire la structure et les propriétés générales des morphismes de groupes. Ils en donnent des décompositions canoniques.

3.2.1 Factorisation des morphismes de groupes

Dans une terminologie moderne, on dit de l'énoncé suivant qui est la **propriété universelle du quotient de groupes**.

Théorème 3.4 (Factorisation des morphismes). *Soit G un groupe, $N \triangleleft G$ et $\pi : G \rightarrow G/N$ la surjection canonique. Si $\theta : G \rightarrow G'$ est un morphisme de groupes tel que $N \subseteq \ker(\theta)$, alors il existe un unique morphisme $\varphi : G/N \rightarrow G'$ 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 :

$$\begin{array}{ccc} G & \xrightarrow{\theta} & G' \\ \pi \downarrow & \searrow \exists! \varphi & \\ G/N & & \end{array}$$

On déduit immédiatement le résultat suivant.

Corollaire 3.5 (Premier théorème d'isomorphisme). *Si $\theta : G \rightarrow G'$ est un morphisme de groupes, alors $G/\ker(\theta) \simeq \text{Im}(\theta)$. En particulier, si G est fini on a $|G| = |\ker(\theta)| \cdot |\text{Im}(\theta)|$.*

Démonstration. On applique le théorème de factorisations des morphismes avec $N = \ker \theta$: on obtient de fait un morphisme injectif $\varphi : G/\ker(\theta) \rightarrow G'$. Comme $\text{Im}(\theta) = \text{Im}(\varphi)$ on a bien que φ est un isomorphisme de $G/\ker(\theta)$ sur $\text{Im}(\theta)$. Si G est fini on a en vertu du théorème 3.1 :

$$|\text{Im}(\theta)| = |G/\ker(\theta)| = \frac{|G|}{|\ker(\theta)|}.$$

■

Exemple. On sait que le groupe alterné $A_n = \ker(\epsilon)$ est normal dans S_n et que l'application signature ϵ est surjective. Donc, en vertu du théorème d'isomorphisme, il existe un unique isomorphisme $\bar{\epsilon} : S_n/A_n \rightarrow \{\pm 1\}$ tel que $\epsilon = \bar{\epsilon} \circ \pi$. En particulier on obtient l'isomorphisme $S_n/A_n \simeq \mathbb{Z}_2$. On rappelle qu'en vertu du théorème de Lagrange, A_n 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 $\mathbb{R} \triangleleft \mathbb{C}$, car $(\mathbb{C}, +)$ est abélien. De plus, on a un épimorphisme de groupes $\theta : \mathbb{C} \rightarrow \mathbb{R}$, défini par $\theta(a + ib) = b$. Son noyau est $\ker(\theta) = \mathbb{R}$. En vertu du théorème d'isomorphisme, il existe donc un unique isomorphisme $\varphi : \mathbb{C}/\mathbb{R} \rightarrow \mathbb{R}$ tel que $\theta = \varphi \circ \pi$, comme annoncé.

Démonstration du théorème 3.4. 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 $\varphi : G/N \rightarrow G'$, 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. ■

3.2.2 Groupes monogènes et cycliques

Un autre des résultats fondamentaux de la théorie des groupes que l'on verra dans le dernier chapitre 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 $n \in \mathbb{Z}$.

Proposition 3.6. 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 $\theta : \mathbb{Z} \rightarrow G$ définie par $\theta(n) = x^n$. Alors θ est un morphisme de groupes et $\ker(\theta) = n\mathbb{Z}$ pour $n \in \mathbb{N}$, en vertu de la Proposition 1.16. Donc en vertu du théorème d'isomorphisme, $G \simeq \mathbb{Z}_n$. Puisque $n = |G| = |\mathbb{Z}_n| = n$, on en déduit le résultat. ■

Exemples.

- (a) Soit $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$. On a $\mathbb{U} \leq (\mathbb{C}^*, \cdot)$ et $\mathbb{U} \simeq (\mathbb{R}, +)/2\pi\mathbb{Z}$.
- (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 $e^{2i\pi/n}$.

Corollaire 3.7. *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. ■

3.2.3 Deuxièmes et troisièmes théorèmes d'isomorphisme

Le résultat suivant, en particulier le second énoncé, illustre bien le terme « quotient » qui est un synonyme de division.

Théorème 3.8. *Soit G un groupe et $H \triangleleft G$ et $K \leq G$.*

1. *On a $H \cap K \triangleleft G$ et $K/(K \cap H) \simeq HK/H$ (deuxième théorème d'isomorphisme).*
2. *Si $K \triangleleft G$ et $K \subseteq H$, alors $H/K \triangleleft G/K$ et $(G/K)/(H/K) \simeq G/H$ (troisième théorème d'isomorphisme).*

Démonstration. Exercice. ■

Exemple. On a $6\mathbb{Z} = 2\mathbb{Z}3\mathbb{Z}$ et $2\mathbb{Z} \cap 3\mathbb{Z} = \{0\}$ donc $6\mathbb{Z}/3\mathbb{Z} \simeq 2\mathbb{Z}/\{0\} \simeq 2\mathbb{Z}$.

3.3 Présentations (finies) de groupes par générateurs et relations

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**.

3.3.1 Groupes libres

Soit S un ensemble. On rappelle un peu de terminologie introduite au §1.4.

On considère $S^{-1} = \{s^{-1} \mid s \in S\}$ un ensemble en bijection avec S . On considère l'ensemble A_S^* des mots sur l'alphabet $A_S = S \sqcup S^{-1}$; on rappelle qu'un mot est une liste $a_1 \dots a_k$ avec $a_i \in A_S$. Alors A_S^* est un monoïde engendré par A_S pour la concaténation des mots dont l'élément neutre est le mot vide δ (voir l'exercice 1.53).

Exemple. Si $S = \{s\}$, alors par exemple $ssss^{-1}s \in A_S^*$ est un mot qui est la concaténation de sss et de $s^{-1}s$. Si $S = \{a, b\}$ alors $ab^2a^{-3}b = abba^{-1}a^{-1}a^{-1}b$ est un mot qui est la concaténation de ab et $ba^{-3}b$.

On considère maintenant la plus petite relation d'équivalence \sim sur A_S^* tel que

$$uaa^{-1}v \sim uv \sim ua^{-1}av,$$

pour tout $a \in A_S$ et $u, v \in A_S^*$. On note $[w]$ la classe d'équivalence de $w \in A_S^*$.

Théorème 3.9. *Soit S un ensemble fini non vide. L'ensemble quotient $F_S := A_S^*/\sim$ est un groupe infini engendré par S pour la loi suivante héritée de la concaténation sur A_S^* :*

$$\begin{aligned} F_S \times F_S &\longrightarrow F_S \\ ([a_1 \dots a_k], [b_1 \dots b_l]) &\longmapsto [a_1 \dots a_k b_1 \dots b_l]. \end{aligned}$$

L'élément neutre est $e = [\delta]$ et l'inverse de $[a_1 \dots a_k]$ est $[a_k^{-1} \dots a_1^{-1}]$.

Démonstration. Exercice 3.25 (difficile). ■

Définition. Le groupe $F_S := A_S^*/\sim$ est appelé le **groupe libre sur S** .

Exemple. (a) Si $S = \{s\}$, alors $F_S = \langle s \rangle$ est monogène infini et donc $F_S \simeq \mathbb{Z}$. On a par exemple $ssss^{-1}s = s^3$ dans F_S .

(b) Si $S = \{a, b\}$ alors

$$F_S = \langle a, b \rangle = \{e, a, a^{-1}, b, b^{-1}, ab, ba, ab^{-1}, b^{-1}a, a^{-1}b, ba^{-1}, a^{-1}b^{-1}, b^{-1}a^{-1}, aba, \dots\}.$$

Le mot $ba^2a^{-3}b = ba^{-1}b$ est la concaténation de ba et $a^{-2}b$.

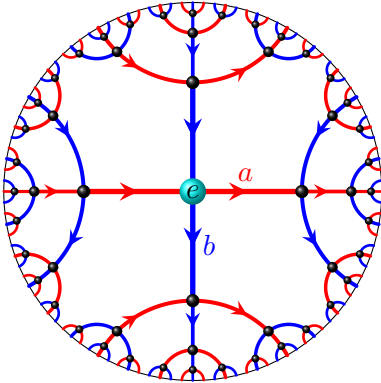


FIGURE 3.1 – Une portion du graphe de Cayley du groupe libre $F_{\{a,b\}}$.

Pour abus de notation, on notera une classe $[w]$ d'un mot w par un mot qui la représente, ce qui pourrait être w lui-même. La démonstration du théorème repose sur le fait que chaque classe d'équivalence de mot contient un unique **mot réduit** : $x_1x_2 \dots x_n$ est réduit si $x_i \neq x_{i+1}^{-1}$. Autrement dit, deux lettres consécutives dans le « mot » $x_1x_2 \dots x_n$ ne sont pas l'inverse l'une de l'autre.

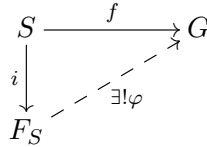
Les éléments de F_S sont donc les mots $x_1x_2 \dots x_n$, de lettres où $x_i = s$ ou $x_i = s^{-1}$ pour $s \in S$; avec la condition que deux lettres consécutives dans le mot $x_1x_2 \dots x_n$ ne sont pas l'inverse l'une de l'autre. Le produit de deux suites $\alpha = x_1x_2 \dots x_n$ et $\beta = y_1y_2 \dots y_k$ s'obtient simplement par concaténation de celles-ci : $\alpha \cdot \beta := x_1x_2 \dots x_n y_1y_2 \dots y_k$, modulo les simplifications nécessaires, dues au fait que les dernières lettres de α et les premières de β sont telles qu'on doit simplifier. Ces simplifications s'effectuent

en effaçant (récursivement) deux lettres consécutives, si elles sont l'inverse l'une de l'autre. Ainsi, on a

$$\begin{aligned}
 (ababb^{-1}a^{-1}b) \cdot (b^{-1}ababaa^{-1}b) &= ababb^{-1}a^{-1}bb^{-1}ababaa^{-1}b \\
 &= ababb^{-1}a^{-1}ababaa^{-1}b \\
 &= abab^{-1}b abaa^{-1}b \\
 &= abababaa^{-1}b.
 \end{aligned}$$

3.3.2 Propriété universelle des groupes libres et présentation par générateur et relation

Théorème 3.10 (Propriété universelle des groupes libres). *Soit S un ensemble fini non vide, G un groupe et $f : S \rightarrow G$ une application. Alors il existe un unique morphisme de groupes φ tel que le diagramme suivant soit commutatif :*



où i est l'injection canonique de S dans F_S . De plus, si $G = \langle f(S) \rangle$ alors φ est surjective.

Démonstration. Exercice 3.25. ■

En particulier, ce théorème signifie que $\varphi(x_1 \dots x_k) = f(x_1) \dots f(x_k)$, pour tout $x_i \in A_S$.

Exemple. On considère $G = \mathcal{D}_m$ le groupe diédral engendré par une réflexion s et la rotation r d'ordre m , où $m \geq 2$. On pose $S = \{a, b\}$. Alors on a une application $f : S \rightarrow G$ définie par $f(a) = s$ et $f(b) = r$. Donc $G = \langle f(S) \rangle$. Par la propriété universelle des groupes libres, il existe un unique morphisme de groupes surjectif $\varphi : F_S \rightarrow G = \mathcal{D}_m$.

Corollaire 3.11. *Tout groupe G engendré par une partie finie S est le groupe quotient d'un groupe libre.*

Démonstration. Il suffit de considérer f comme l'injection canonique de S dans F_S . ■

Corollaire 3.12. *Soit S un ensemble fini non vide et G un groupe.*

1. *Soit $\varphi : F_S \rightarrow G$ un morphisme de groupes, $R \subseteq F_S$ et $N(R)$ le plus petit sous-groupe normal contenant R (c'est-à-dire l'intersection de tous les sous-groupes normaux dans F_S qui contiennent*

S). Si $R \subseteq \ker \varphi$. Alors il existe un unique morphisme de groupes $\bar{\varphi}$ tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} F_S & \xrightarrow{\varphi} & G \\ \pi \downarrow & \nearrow \exists! \bar{\varphi} & \\ F_S/N(R) & & \end{array}$$

De plus, $\bar{\varphi}$ est surjective si φ est surjective et $\bar{\varphi}$ est injective si $N(R) = \ker(\varphi)$.

2. Si $G = \langle S \rangle$ alors il existe un unique morphisme surjectif de groupes $\varphi : F_S \rightarrow G$ tel que $\varphi(s) = s$ pour tout $s \in S$. De plus :

- (i) si $R \subseteq \ker \varphi$, alors il existe un unique morphisme de groupes $\bar{\varphi} : F_S/N(R)$ tel que $\bar{\varphi}(sN(R)) = s$;
- (ii) si $\ker \varphi = N(R)$ alors $\bar{\varphi}$ est un isomorphisme.

Démonstration. L'énoncé est un corollaire du théorème ci-dessus, ainsi que du premier théorème d'isomorphisme (car si $R \subseteq \ker \varphi$, le plus petit sous-groupe normal contenant R est forcément contenu dans le sous-groupe normal $\ker \varphi$). ■

Le deuxième énoncé du corollaire précédent motive la définition de présentation par générateurs et relations.

Définition. Une **présentation** d'un groupe G est la donnée d'un ensemble de générateur S de G est d'un ensemble dit de **relations** $R \subseteq F_S$ de G tel que $G \simeq F_S/N(R)$. Dans ce cas on note $G = \langle S \mid R \rangle$.

Exemples. (a) En poursuivant l'exemple précédent de $G = \mathcal{D}_m$, on voit que $R = \{a^2, b^m, abab\} \subseteq \ker \varphi$.

On peut en fait montrer que $R = \{a^2, b^m, abab\} \subseteq \ker \varphi$ (exercice 3.18). Donc le groupe diédral \mathcal{D}_m admet la présentation $\mathcal{D}_m := \langle r, s \mid r^m, s^2, (rs)^2 \rangle$.

(b) On a aussi les présentations suivantes (exercices) :

$$\begin{aligned} \mathcal{D}_m &= \langle s, t \mid s^2, t^2, (st)^m \rangle \\ \mathbb{Z}_n &= \langle z \mid z^n \rangle, \\ \mathrm{SL}_2(\mathbb{Z}) &= \langle s, r \mid s^4, r^6 \rangle, \\ S_n &= \langle s_1, \dots, s_{n-1} \mid s_i^2, (s_i s_{i+1})^3, (s_i s_j)^2 \text{ pour } |i-j| > 1 \rangle, \\ A_n &= \langle c_1, \dots, c_{n-2} \mid c_i^3, (c_i c_j)^2 \text{ pour } i \neq j \rangle. \end{aligned}$$

(c) Un même groupe peut avoir plusieurs présentations. Par exemple, on a

$$A_5 = \langle a, b \mid a^2, b^3, (ab)^5 \rangle = \langle c, d \mid c^2, d^4, (cd)^5, (c^{-1}d^{-1}cd)^3 \rangle.$$

- Remarque.** (a) Bien qu'on écrive les relations comme un ensemble constitué de mots α dans F_S , il faut les interpréter comme des identités $\alpha = e$ pour α vu dans G via φ . Techniquement donc, on se donne R un sous-ensemble fini de F_S , en comprenant que $\alpha \in R$ correspond à l'identité $\alpha = e$.
- (b) 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 .
- (c) On a souvent des relations qui font intervenir le **commutateur**, $[a, b] := a^{-1}b^{-1}ab$, de deux éléments. On observe que

$$[a, b] = e \quad \text{ssi} \quad a^{-1}b^{-1}ab = e \quad \text{ssi} \quad ab = ba,$$

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 Novikov¹. Cependant, on peut déterminer certaines classes de présentations de groupes pour lesquelles le **problème du mot** est décidable.

3.4 Exercices

Questions d'auto-évaluation

Groupes quotients

Question 3.1. L'énoncé suivant est-il vrai (justifier la réponse) : Si $H \triangleleft G$ et si $[G : H] = 2014$, alors $x^{2014} \in H$ pour tout $x \in G$?

Réponse : Vrai.

- $H \triangleleft G$, donc G/H est un groupe.
- Par le théorème de Lagrange, $(xH)^{2014} = eH$ pour tout $xH \in G/H$.
- Comme $(xH)^{2014} = x^{2014}H = H$, on a que $x^{2014} \in H$, car $gH = H$ ssi $g \in H$ (résultat du cours).

Question 3.2. Soit G un groupe et H un sous-groupe normal de G d'indice n . Montrer que pour tout $a \in G$, $a^n \in H$. Donner un exemple de sous-groupe H non normal d'un groupe G pour lequel l'énoncé précédent est faux.

Question 3.3. Soit G un groupe et $N \triangleleft G$. Vérifier les énoncés suivants.

- (a) On a $L \leq G/N$ si et seulement si il existe $N \leq K \leq G$ tel que $\pi(K) = L$. De plus dans ce cas, on a $N \triangleleft K$, le groupe K/N est bien défini et $L = K/N$.

1. Voir **Petr Novikov** (1901-1975)

(b) Si $K = \langle S \rangle$, on a $\pi(K) = \langle \pi(S) \rangle$.

Question 3.4. Donner tous les sous-groupes de $(\mathbb{Z}_{20}, +)$.

Question 3.5. Soit G un groupe et $H \leq G$ vérifiant : si $xH = x'H$, $yH = y'H$, alors $xyH = x'y'H$, pour tout $x, x', y, y' \in G$. Montrer que $H \triangleleft G$. En déduire que l'ensemble quotient G/H est un groupe pour la loi $xH \cdot yH = xyH$ si et seulement si $H \triangleleft G$.

Réponse : Comme $gH = ghH$ pour tout $g \in G$ et $h \in H$, l'hypothèse donne $ghg^{-1}H = gg^{-1}H = H$ et donc $ghg^{-1} \in H$ pour tout $g \in G$ et $h \in H$. Il s'en suit que H est normal dans G . Le deuxième énoncé est une conséquence directe de ce qui précède et de la preuve du théorème 3.1.

Théorèmes d'isomorphismes

Question 3.6. Justifier les isomorphismes suivants en utilisant le théorème de factorisation ou le premier théorème d'isomorphisme :

(a) $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$;

Réponse : Considérer la fonction **partie réelle des nombres complexes** et montrer que c'est un morphisme de groupes additifs.

(b) $(\mathbb{C}^*/\mathbb{U}, \cdot) \simeq (\mathbb{R}^{+*}, \cdot)$;

Réponse : Considérer la fonction **module des nombres complexes** et montrer que c'est un morphisme de groupes multiplicatif.

Question 3.7. Soit G un groupe et $f : G \rightarrow \mathbb{Z}/2\mathbb{Z}$ un morphisme de groupes surjectif. Montrer que $[G : \ker(f)] = 2$.

Question 3.8. Soit $n \in \mathbb{N}$ et d qui divise n .

(a) Montrer qu'il existe un morphisme de groupes injectif $\iota : (\mathbb{Z}_d, +) \rightarrow (\mathbb{Z}_n, +)$.

(b) Montrer qu'il existe un morphisme de groupes surjectif $\varphi : (\mathbb{Z}_n, +) \rightarrow (\mathbb{Z}_d, +)$.

Question 3.9. Soit H, K des groupes et $G = H \times K$, $A = \{e_H\} \times K$ et $B = H \times \{e_K\}$. Vérifiez que $A \triangleleft G$, $B \triangleleft G$, et que $G/A \simeq H$ et $G/B \simeq K$.

Question 3.10. Soient $G = \mathbb{Z}/24\mathbb{Z}$, $H = \langle 4 + 24\mathbb{Z} \rangle$ le sous-groupe de G engendré par $4 + 24\mathbb{Z}$, et $N = \langle 6 + 24\mathbb{Z} \rangle$ le sous-groupe de G engendré par $6 + 24\mathbb{Z}$.

(a) Créer une liste de tous les éléments de $(H + N)/N$.

(b) Créer une liste de tous les éléments de $H/(H \cap N)$

(c) Indiquer explicitement la correspondance entre $H/(H \cap N)$ et $(H + N)/N$ du deuxième théorème d'isomorphisme.

Réponse :

— On a $H = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}\}$ et $N = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}\}$. D'où :

$$H + N = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}\} \text{ et}$$

$$(H + N)/N = \{0 + N, 2 + N, 4 + N\};$$

— On a $H \cap N = \{\overline{0}, \overline{12}\}$, d'où $0 + H \cap N = \{0, 12\}$, $4 + H \cap N = \{4, 16\}$ et $8 + H \cap N = \{8, 20\}$.

— L'isomorphisme $H/(H \cap N) \rightarrow (H + N)/N$ est donné par $h + H \cap N \mapsto h + N$, donc :

$$0 + H \cap N \mapsto 0 + N; 4 + H \cap N \mapsto 4 + N; 8 + H \cap N \mapsto 8 + N = 2 + N.$$

Présentation par générateurs et relations

Question 3.11. Montrer que $\mathbb{Z}_n = \langle a \mid a^n \rangle$, où $n \in \mathbb{N}$.

Question 3.12. Ecrire une preuve du corollaire 3.12.

Question 3.13. Soit A et B deux ensemble en bijection, montrer que $F_A \simeq F_B$.

Exercices

Exercice 3.1. Soit G un groupe abélien fini dont tous les éléments sont une puissance de p premier. Montrer que $|G|$ est une puissance de p .

Exercice 3.2. Soit G un groupe fini et H un sous-groupe normal de G .

1. Si K un sous-groupe de G tel que $[G : H]$ et $|K|$ sont premiers entre eux, montrer que $K \subseteq H$.
2. On suppose que $[G : H]$ et $k = |H|$ sont premiers entre eux. Montrer que H est l'unique sous-groupe de G d'ordre k .

Exercice 3.3. Soit G un groupe abélien et p un nombre premier. Soit H le sous-groupe de G constitué par les éléments d'ordre une puissance de p .

1. Montrer que H est un sous-groupe de G .
2. Montrer que G/H ne possède pas d'éléments dont l'ordre est une puissance non nulle de p .

Exercice 3.4. Soit G un groupe et $Z(G)$ son centre.

- (a) Soit $H \leq Z(G)$, montrer que G/H est un groupe pour la loi $(xH, yH) \mapsto xyH$.
- (b) On suppose que le groupe $G/Z(G)$ est monogène, montrer que G est abélien.

Exercice 3.5. Soient G un groupe d'ordre $2q$, où q est un nombre premier *impair*, et H un sous-groupe normal de G d'ordre 2.

- (a) Montrer que G est un groupe abélien.
- (b) Montrer que G est monogène.

Exercice 3.6. Soit G un sous-groupe d'indice fini dans (\mathbb{C}^*, \cdot) , montrer que $G \simeq (\mathbb{C}^*, \cdot)$ (on pourra utiliser l'exercice 3.2).

Exercice 3.7. Soit G le groupe

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R} \text{ tels que } ad \neq 0 \right\}$$

où l'opération de G est la multiplication de matrices.

(a) Montrer que

$$N = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\}$$

est un sous-groupe normal de G .

(b) Montrer que les matrices

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

appartiennent à la même classe à gauche modulo N .

(c) En déduire que G/N est un groupe abélien.

Exercice 3.8. Soit G un groupe dont l'élément neutre est noté e . On note $Z(G)$ le centre de G . Le commutateur de $x, y \in G$, noté $[x, y]$ est l'élément de G défini par $[x, y] = x^{-1}y^{-1}xy$. Le groupe dérivé de G est le sous-groupe $[G, G]$ de G engendré par les commutateurs de G :

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle.$$

- (a) Montrer que G est abélien si et seulement si $[G, G] = \{e\}$.
- (b) Montrer que $[G, G] \triangleleft G$.
- (c) Soit $H \triangleleft G$ tel que $H \cap [G, G] = \{e\}$, montrer que $H \subseteq Z(G)$.
- (d) Soit $H \triangleleft G$, montrer que G/H est abélien si et seulement si $[G, G] \subseteq H$.
- (e) Soit H et K deux sous-groupes normaux de G tel que $H \leq K$. Montrer que si G/H est abélien, alors G/K et K/H sont abéliens.
- (f) Sachant que le groupe alterné A_n (le sous-groupe du groupe symétrique S_n des permutations paires) est engendré par les cycles de longueur 3, montrer que $[S_n, S_n] = A_n$.
- (g) En déduire qu'il y a exactement deux homomorphismes de S_n dans \mathbb{C}^* , pour $n \geq 2$.

Exercice 3.9. On dit qu'un sous-groupe normal H de G est un sous-groupe normal maximal de G si $H \neq G$ et si $H \leq K \leq G$ entraîne $K = H$ ou $K = G$.

Montrer que $H \triangleleft G$ est un sous-groupe normal maximal de G ssi G/H ne possède pas de sous-groupe normal à part que G/H et $\{H\}$.

Exercice 3.10. Justifier les isomorphismes suivants :

- (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 3.11. Soit G, G' deux groupes finis. On note $\delta : G \rightarrow G'$ le morphisme trivial, c'est-à-dire, $\delta(g) = e_{G'}$ pour tout $g \in G$.

- (a) Montrer que si $|G|$ et $|G'|$ sont premiers entre eux, alors $\text{Hom}(G, G') = \{\delta\}$.
- (b) Montrer que tout morphisme de groupes de $G = S_3$ dans $G' = \mathbb{Z}/3\mathbb{Z}$ est trivial.

Exercice 3.12. Soit $n = pq$ où p, q sont deux nombres premiers distincts. Soit $H = \langle p \rangle \leq \mathbb{Z}_n$ et $K = \langle q \rangle \leq \mathbb{Z}_n$. Montrer que $\mathbb{Z}_n \simeq H \times K \simeq \mathbb{Z}_p \times \mathbb{Z}_q$.

Exercice 3.13. Soit $m \geq 3$. On pose, dans le groupe diédral \mathcal{D}_m engendré par la rotation r d'ordre m et la réflexion s d'ordre 2, $H = \langle r \rangle$ et $K = \langle s \rangle$. Montrer que $\mathcal{D}_m \simeq H \rtimes K \simeq \mathbb{Z}_m \rtimes_{\varphi} \mathbb{Z}_2$, où φ sera à déterminer.

Exercice 3.14. Soit G_1, \dots, G_n des groupes. Pour $1 \leq i \leq n$ on considère H_i un sous-groupe de G_i .

- (a) Montrer que le produit direct $H_1 \times \dots \times H_n$ est un sous-groupe de $G_1 \times \dots \times G_n$, qui est normal si chacun des H_i l'est.
- (b) Montrer que $(G_1 \times G_2)/(H_1 \times H_2) \simeq (G_1/H_1) \times (G_2/H_2)$.

Exercice 3.15. On considère le groupe diédral \mathcal{D}_{2m} , $m \geq 2$ d'ordre $4m$. On considère une rotation $r \in \mathcal{D}_{2m}$ d'ordre m et $H = \langle r \rangle$. Montrer que $H \triangleleft \mathcal{D}_m$ et donner tous les sous-groupes de \mathcal{D}_m/H .

Exercice 3.16. (Deuxième et troisième théorèmes d'isomorphisme) Soit G un groupe et $H \triangleleft G$ et $K \leq G$.

- (a) Montrer que $H \cap K \triangleleft G$ et $K/(K \cap H) \simeq HK/H$.
- (b) Si de plus $K \triangleleft G$ et $K \subseteq H$, montrer que $H/K \triangleleft G/K$ et $(G/K)/(H/K) \simeq G/H$.

Exercice 3.17. On pose, dans le groupe diédral \mathcal{D}_6 engendré par la rotation r d'ordre 6 et la réflexion s d'ordre 2, $H = \langle r^2, s \rangle$, $K = \langle r^3 \rangle$ et $L = \langle s \rangle$.

- (a) Montrer que $H = \mathcal{D}_3 \simeq S_3$.
- (b) Montrer que $\mathcal{D}_6 \simeq H \times K$.
- (c) En déduire que $\mathcal{D}_6 \simeq S_3 \times \mathbb{Z}_2$.
- (d) Montrer que $\mathcal{D}_6 \simeq H \times L$.

Exercice 3.18. Montrer que $\mathcal{D}_m = \langle s, r \mid s^2, r^m, srsr \rangle$, où $m \geq 2$.

Exercice 3.19. Soit $m \geq 2$.

- (a) Montrer que $\mathcal{D}_m = \langle s, t \mid s^2, t^2, (st)^m \rangle$.
- (b) Soit G un groupe fini engendré par deux involutions distinctes. Montrer que 2 divise $|G|$ et que $|G| = 2m$. Montrer que $G \simeq \mathcal{D}_m$, le groupe diédral d'ordre $2m$. Qu'en est-il si G est infini ?

Exercice 3.20. Montrer que S_4 est isomorphe à $G = \langle a, b \mid a^4, b^2, (ab)^3 \rangle$, où $n \in \mathbb{N}$.

Exercice 3.21. (*Lemme de Zassenhaus*) Soient H et K deux groupes, $H' \triangleleft H$ et $K' \triangleleft K$.

1. Montrer que $H'(H \cap K')$ est un sous-groupe normal de $H'(H \cap K)$.
2. Montrer que $K'(K \cap H')$ est un sous-groupe normal de $K'(K \cap H)$.
3. Montrer que l'on a un isomorphisme de groupes quotients :

$$H'(H \cap K) / H'(H \cap K') \cong K'(H \cap K) / K'(H' \cap K)$$

Exercices exploratoires

Exercice 3.22. Soit H, K et G trois groupes, on considère

$$e \xrightarrow{i} H \xrightarrow{\varphi} G \xrightarrow{\psi} K \xrightarrow{p} e$$

une **suite exacte courte de groupes**, c'est-à-dire, i, φ sont des morphismes de groupes injectifs, ψ, p sont des morphismes de groupes surjectifs et $\ker \psi = \varphi(H)$.

- (a) Soit H' un groupe et

$$e \xrightarrow{i'} H' \xrightarrow{\varphi'} G \xrightarrow{\psi} K \xrightarrow{p} e$$

une suite exacte courte de groupe. Montrer que $H \simeq H'$.

- (b) Soit finalement G' un groupe et

$$e \xrightarrow{i} H \xrightarrow{\varphi'} G' \xrightarrow{\psi'} K \xrightarrow{p} e$$

une suite exacte de groupe. Est-ce que G est isomorphe à G' ? (Indication : on pourra considérer \mathbb{Z}_n et le groupe de Klein $G' = \langle \tau_1, \tau_3 \rangle \leq S_4$ engendré par les deux transpositions simples τ_1 et τ_3 qui commutent.

- (c) Soit K' un groupe et

$$e \xrightarrow{i} H \xrightarrow{\varphi} G \xrightarrow{\psi'} K' \xrightarrow{p'} e$$

une suite exacte courte de groupe. Montrer que $K \simeq K'$.

Exercice 3.23 (Groupes alternés simple). Le but de ce problème est de montrer que le groupe alterné A_n est simple si et seulement si $n \geq 5$. Soit C_r l'ensemble des cycles de longueur r dans S_n .

- (a) Montrer que A_3 est simple et que A_4 n'est pas simple.
- (b) Montrer que S_n agit transitivement par conjugaison sur C_r pour tout $2 \leq r \leq n - 2$.
- (c) Montrer que A_n agit transitivement par conjugaison sur C_r si $2 \leq r \leq n - 2$.
- (d) Montrer que A_n est engendré par les cycles de longueur 3.
- (e) On suppose à partir de maintenant que $n \geq 5$. On considère un sous-groupe normal H de A_n non réduit à l'identité. Montrer que si H contient un cycle de longueur 3 alors $H = A_n$.
- (f) En conclure que A_n est simple.

Exercice 3.24 (Groupes résolubles). Un groupe G est dit **résoluble** s'il existe une chaîne de groupes

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G,$$

où chaque G_i est un sous-groupe normal de G_{i+1} et G_{i+1}/G_i est abélien. On dit alors que la chaîne ci-haut est une résolution du groupe G .

Remarque. 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.

- (a) Montrer que les groupes abéliens sont résolubles.
- (b) Montrer que si G est résoluble, alors tout les sous-groupes et tous les quotients de G sont résolubles.
- (c) Le *commutateur* de $x, y \in G$, noté $[x, y]$ est l'élément de G défini par $[x, y] = x^{-1}y^{-1}xy$. Le *groupe dérivé* de G est le sous-groupe $D(G)$ de G engendré par les commutateurs de G :

$$D(G) = \langle [x, y] \mid x, y \in G \rangle.$$

Le i ème groupe dérivée de G est défini par récurrence de la façon suivante : $D_1(G) = D(G)$ et $D_i(G) = D(D_{i-1}(G))$ pour $i \geq 2$.

- (i) Montrer que $D_i \triangleleft D_{i+1}$ et que D_{i+1}/D_i est abélien.
- (ii) Montrer que G est résoluble si et seulement si il existe $n \geq 1$ tel que $D_n(G) = \{e\}$.
- (d) Montrer que si G est fini, G est résoluble si et seulement si il existe une chaîne de résolution du groupe G dont tous les quotients sont cycliques d'ordre premier.
- (e) Montrer que les seuls groupes simples résolubles sont les groupes cycliques d'ordre premier.

(f) Montrer que S_n n'est pas résoluble si $n \geq 5$.

Exercice 3.25. Soit S un ensemble fini.

(a) Montrer qu'il existe un unique mot de A_S^* de longueur minimale dans chaque classe d'équivalence pour la relation \sim .

(b) Montrer le Théorème 3.9.

(c) Montrer le Théorème 3.12.

(d) Montrer que tout sous-groupe d'un groupe libre est isomorphe à un groupe libre.

Exercice 3.26 (Une présentation du groupe symétrique). Soit $n \geq 2$ un entier. On note $\tau_i = (i \ i+1)$ la transposition simple qui échange i et $i+1$, pour $1 \leq i \leq n-1$. Le but de ce problème est de montrer que le groupe symétrique S_n admet la présentation suivante :

$$S_n = \langle \tau_1, \dots, \tau_{n-1} \mid \tau_i^2, (\tau_i \tau_j)^2, (\tau_i \tau_{i+1})^3, |i-j| > 1 \rangle.$$

(a) Soit $S = \{a_1, \dots, a_{n-1}\}$ un alphabet à $n-1$ lettres. Montrer qu'il existe un morphisme de groupe surjectif φ du groupe libre F_S dans S_n qui envoie a_i sur la transposition simple τ_i pour tout $1 \leq i < n$. Montrer que les relations vérifient

$$R = \{a_i^2, (a_i a_j)^2, (a_i a_{i+1})^3, |i-j| > 1\} \subseteq \ker \varphi.$$

En déduire l'existence d'un morphisme de groupe surjectif $\bar{\varphi}$ de $G_n := F_S/N(R)$ dans S_n .

(b) Montrer par récurrence sur n que $|G_n| \leq n!$.

Indication : On pourra regarder $G_{n-1} \leq G_n$ et considérer les éléments $y_0 = e$, $y_1 = a_{n-1}$, $y_i = a_{n-i} \cdots a_{n-1}$ ($1 \leq i \leq n-1$). On montrera alors que G_n est l'union des $y_i G_{n-1}$.

(c) En déduire que $S_n \simeq G_n = \langle S \mid a_i^2, (a_i a_j)^2, (a_i a_{i+1})^3, |i-j| > 1 \rangle$.

(d) Conclure.

Exercice 3.27. Les **groupes de Coxeter** sont les groupes qui admettent une présentation $W = \langle S \mid R \rangle$, avec les relations 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) $m(s, t) \geq 2$ 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.

Exercice 3.28. On rappelle que le groupe $\mathrm{SL}_2(\mathbb{Z})$ est un groupe infini engendré par les matrices

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

et qu'on a les relations $S^4 = \mathrm{Id}$ et $R^3 = S^2$. Pour toute représentation linéaire $\rho : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathbb{C}^*$,

(a) Montrer que

$$\rho \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{12} = 1, \quad \text{pour tout} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

En conclure que $\rho(A) = \exp(2ki\pi/12)$ pour un certain $0 \leq k < 12$, pour tout A dans $\mathrm{SL}_2(\mathbb{Z})$.

(b) Montrer qu'il y a un nombre fini de morphismes de groupes de $\mathrm{SL}_2(\mathbb{Z})$ dans $GL(\mathbb{C}^*)$. Les trouver toutes.

Exercice 3.29 (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 $\{1, 2, \dots, 15\}$, 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} .

- Montrer que G est constitué de permutations paires.
- En trouvant assez de générateurs de G , montrer que $G = A_{15}$.
- En déduire que le problème de Sam Loyd (voir ci-haut) est impossible à résoudre.
- 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, Schutzenberger² a introduit une adaptation du **jeu de taquin** à la combinatoire des **tableaux de Young**, ainsi nommé en l'honneur d'un des pionniers³ de la théorie de la représentation des groupes.

Exercice 3.30. Montrer que le groupe de transformation du Cube de Rubik se décrit comme (voir **Rubik's Cube group**)

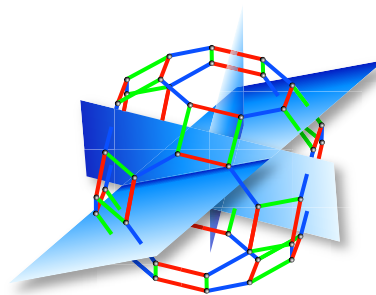
$$(\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11}) \rtimes ((A_8 \times A_{12}) \rtimes \mathbb{Z}_2).$$

2. **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.

3. **Alfred Young** (1863-1942).

Chapitre 4

Actions de groupes

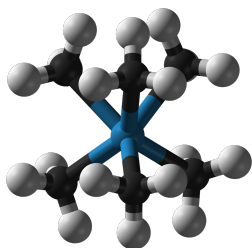


Le théorème de Cayley prouve l'existence pour un groupe G d'un groupe symétrique dans lequel G est (à isomorphisme près) un sous-groupe. Ceci nous amène à nous poser la question de la construction du plus petit groupe symétrique ayant cette propriété.

Dans ce chapitre nous allons étudier, étant donnée un groupe G et un ensemble E , les morphismes de groupes de G dans S_E . Nous allons voir que ceci revient à étudier les actions du groupe G sur l'ensemble E , 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 Galilée¹ 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.

1. Galilei Galileo, 1564–1642.

Dans le cas où G agit par translation sur l'un de ses sous-groupes, cela nous permet de démontrer un outil puissant pour l'étude des groupes : le Théorème de Lagrange². Ce théorème donne une information primordiale sur le calcul des ordres des sous-groupes d'un groupe fini : ceux-ci divisent l'ordre du groupe.

4.1 Groupe opérant sur un ensemble

Définition. Soit G un groupe et E un ensemble. Une **action (à gauche) de G sur E** est la donnée d'une loi de composition externe (à gauche)

$$\begin{aligned} G \times E &\longrightarrow E \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

vérifiant les conditions suivantes :

- (i) $e \cdot x = x$, où e désigne l'élément neutre de G ;
- (ii) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

Dans ce cas on dit aussi que G **opère (à gauche)** sur E , ou encore que G **agit sur E** . L'ensemble E s'appelle un **G -ensemble**.

Remarque. Il existe des actions à droites de G sur E : on considère alors une loi de composition externe à droite $E \times G \rightarrow E$, définie par $(x, g) \mapsto x \cdot g$, et vérifiant les hypothèses à droite $x \cdot e = x$ et $x \cdot (g_1 g_2) = (x \cdot g_1) \cdot g_2$.

Exemple (Translation à gauche). La multiplication à gauche de G munit G de la structure d'un G -ensemble appelé **translation à gauche**. En effet, la loi de composition externe

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

vérifie bien pour tout $x \in E$ et $g_1, g_2 \in G$ que $ex = x$ et $(g_1 g_2)x = g_1(g_2 x)$ (la loi de G est associative).

Exemple (Action à gauche par translation sur les classes à gauche). Soit G un groupe et H un sous-groupe de G , alors G agit sur G/H de la façon suivante :

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g, xH) &\longmapsto g \cdot xH := gxH. \end{aligned}$$

En effet, pour tout $xH \in G/H$ on a $e \cdot xH = exH = xH$, puis pour $g, h \in G$ on a :

$$(gh) \cdot xH = ghxH = g \cdot hxH = g \cdot (h \cdot xH).$$

2. **Joseph Louis Lagrange** (1736–1813).

Exemple (Action par conjugaison). L'**action par conjugaison** de G est définie comme suit :

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto g \cdot x = gxg^{-1}. \end{aligned}$$

L'action par conjugaison est bien une action car pour tout $x \in E$ et $g_1, g_2 \in G$ on a $e \cdot x = exe = x$ et

$$(g_1g_2) \cdot x = (g_1g_2)x(g_1g_2)^{-1} = g_1g_2xg_2^{-1}g_1^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = g_1 \cdot (g_2 \cdot x).$$

Exemple (Actions sur $\mathcal{P}(G)$). La translation à gauche de G sur G s'étend plus généralement à l'ensemble $\mathcal{P}(G)$ de G :

$$\begin{aligned} G \times \mathcal{P}(G) &\longrightarrow \mathcal{P}(G) \\ (g, A) &\longmapsto gA := \{gx \mid x \in A\}. \end{aligned}$$

Le lecteur vérifiera que la loi de composition externe ci-dessus définit bien une action.

De même, l'action par conjugaison de G s'étend naturellement en une action de G sur $\mathcal{P}(G)$:

$$\begin{aligned} G \times \mathcal{P}(G) &\longrightarrow \mathcal{P}(G) \\ (g, x) &\longmapsto gAg^{-1} := \{gxg^{-1} \mid x \in A\}. \end{aligned}$$

De façon générale, si E est un G -ensemble alors l'action $(g, x) \mapsto g \cdot x$ de G sur E s'étend en une action de G sur $\mathcal{P}(E)$ de la façon suivante :

$$\begin{aligned} G \times \mathcal{P}(E) &\longrightarrow \mathcal{P}(E) \\ (g, A) &\longmapsto g \cdot A := \{g \cdot a \mid a \in A\}. \end{aligned}$$

En effet, $e \cdot A = \{e \cdot a \mid a \in A\} = \{a \mid a \in A\} = A$ en vertu de la Condition (i) de la définition et pour $g, h \in G$ on a

$$(gh) \cdot A = \{(gh) \cdot a \mid a \in A\} = \{g \cdot (h \cdot a) \mid a \in A\} = \{g \cdot a' \mid a' \in h \cdot A\} = g \cdot (h \cdot A).$$

en vertu de la Condition (ii) de la définition.

Exemple (Action de S_n sur \mathbb{R}^n). Le groupe symétrique S_n , où $n \in \mathbb{N}^*$ agit sur \mathbb{R}^n par permutation des coordonnées.

Nous montrons maintenant que la donnée d'une action d'un groupe G sur un ensemble E est la même que la donnée d'un morphisme de groupes de G dans S_E .

Proposition 4.1. *Soit G un groupe et E un ensemble.*

1. Si E est un G -ensemble, avec l'action de G sur E définie par $(g, x) \mapsto g \bullet x$, alors l'application

$$\begin{aligned} \rho_\bullet : G &\longrightarrow S_E \\ g &\longmapsto \rho_g, \end{aligned}$$

est un morphisme de groupes, où la bijection $\rho_g : E \rightarrow E$ est définie par $\rho_g(x) = g \bullet x$ pour tout $x \in E$.

2. Si $\rho : G \rightarrow S_E$ est un morphisme de groupes, alors la loi de composition externe

$$\begin{aligned} \bullet_\rho : G \times E &\longrightarrow E \\ (g, x) &\longmapsto g \bullet_\rho x := \rho(g)(x) \end{aligned}$$

est une action de G sur E .

De plus, l'application $\bullet \mapsto \rho_\bullet$ est une bijection entre l'ensemble des actions de G sur E et les morphismes de groupes de G dans S_E .

Démonstration. Voir la question d'auto-évaluation 4.1. ■

On définit grâce à cette proposition le **noyau d'une action \bullet de G sur E** comme le noyau $\ker \rho_\bullet$ de son morphisme de groupes associé ρ_\bullet . On dira qu'une action de G sur E est **fidèle** si son noyau est réduit à l'élément neutre de G .

Exemple. L'action de S_n sur \mathbb{R}^n est fidèle. En effet son morphisme de groupes associé est

$$\begin{aligned} \rho : G &\longrightarrow S_{\mathbb{R}^n} \\ \sigma &\longmapsto \rho_\sigma, \end{aligned}$$

où $\rho_\sigma : \mathbb{R}^n \rightarrow \mathbb{R}^n$ est la bijection définie par $\rho_\sigma(x_1, \dots, x_n) = (x_{\sigma(1)}, \dots, x_{\sigma(n)})$. Si $\sigma \in \ker \rho$ alors $\rho_\sigma = \text{Id}_{\mathbb{R}^n}$. Donc pour tout $1 \leq i \leq n$ on a : $x_{\sigma(i)} = x_i$, ce qui implique $\sigma(i) = i$. Donc $\sigma = e$. Le noyau de cette action est donc bien réduit à l'identité.

On observe que $\text{Im}(\rho) \subseteq \text{GL}(\mathbb{R}^n)$. On appelle de telles action des **représentations linéaires de groupe**. L'espace vectoriel \mathbb{R}^n est alors appelé un **S_n -module**. Cette théorie est en dehors du cadre du cours, voir l'Annexe ?? pour un aperçu.

On termine cette section avec la définition suivante, qui sera très utile afin de construire des actions de G à partir d'action existante.

Définition. Soit G un groupe et E un G -ensemble. Un sous-ensemble A de E est dit **G -stable** ou **G -invariant**, si on a $g \cdot x \in A$ pour tout $x \in A$, c.-à-d.

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

Proposition 4.2. Soit G un groupe, E un G -ensemble et $A \subseteq E$.

1. A est G -stable si et seulement si $g \cdot A = A$ pour tout $g \in G$.
2. Si A est un sous-ensemble de E stable par l'action G , alors est un G -ensemble pour l'action $G \times E \rightarrow E$ restreinte à $G \times A$. On dit que A est un **sous- G -ensemble de E** .

Démonstration. (2) est une conséquence du fait que l'image de la restriction de l'action $G \times E \rightarrow E$ à $G \times A$ est contenue dans A par définition, donc on obtient une action $G \times A \rightarrow A$. Pour (1) il suffit de montrer l'implication directe. On note que $g \cdot A \subseteq A$ pour tout $g \in G$ car A est G -stable. Donc en particulier $g^{-1} \cdot A \subseteq A$ pour tout $g \in G$. Le résultat est alors une conséquence de l'équation suivante :

$$A = e \cdot A = (gg^{-1}) \cdot A = g \cdot (g^{-1} \cdot A) \subseteq g \cdot A.$$

■

4.2 Orbites et stabilisateurs

Afin d'étudier une action d'un groupe sur un ensemble, deux notions sont particulièrement importantes. La notion d'orbites et celles de stabilisateurs.

Définition. Soit G un groupe et E un G -ensemble. L'**orbite de $x \in E$** est l'ensemble :

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

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.

$$E/G = \{\text{Orb}(x) \mid x \in E\}.$$

Exemple. (a) L'action par translation à gauche de G sur G n'a qu'une orbite qui est G .

(b) Les orbites de l'action par conjugaison de G sur G sont appelées les **classes de conjugaison de G** . Elles jouent un rôle très important dans la compréhension des groupes finis. En fait, les classes de conjugaison de S_n sont très bien décrites au moyen de la notion de **partage de l'entier n** : un partage λ de n est une liste décroissante d'entier strictement positif dont la somme fait n . À toute permutation $\sigma \in S_n$ on associe un partage $\lambda(\sigma)$ en décomposant σ en cycles disjoints, puis en réordonnant du plus grand au plus petit les longueurs de ces cycles. Par exemple $\lambda((145)(28)(369)) = (3, 3, 2, 1)$. On sait alors que σ et γ sont conjuguées si et seulement si $\lambda(\sigma) = \lambda(\gamma)$. De ce fait les classes de conjugaison de S_n sont en bijection avec les partages de l'entier n ; voir l'Exercice 4.14 pour plus de détails.



Orbites (selon la NASA).

La proposition suivante énonce en particulier que tout G -ensemble est une union disjointe de ses orbites.

Proposition 4.3. 1. Si $x \in E$, alors l'action de $\text{Orb}(x)$ est un sous- G -ensemble pour l'action de G sur E restreinte à $\text{Orb}(x)$. De plus cette action est transitive.

2. L'action de G sur E induit une relation d'équivalence sur E , définie en posant $x \equiv y$ si et seulement si $\text{Orb}(x) = \text{Orb}(y)$.

3. L'ensemble E/G est une partition de E , autrement dit :

$$E = \bigsqcup_{\mathcal{O} \in E/G} \mathcal{O} \quad (\text{union disjointe}). \quad (4.1)$$

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

$$E = \text{Orb}(x_1) \sqcup \text{Orb}(x_2) \sqcup \dots \sqcup \text{Orb}(x_n), \quad (4.2)$$

Démonstration. Voir la question d'auto-évaluation 4.5. ■

On peut donc, pour comprendre les actions en général, chercher à comprendre les actions transitives, ce que nous ferons dans la section suivante.

Définition. Soit G un groupe et E un G -ensemble. Le **stabilisateur** de x , noté $\text{Stab}_G(x)$ (ou $\text{Stab}(x)$ si il n'y a pas de confusion possible), est l'ensemble des éléments de G qui **fixe** $x \in E$:

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

Exemple. L'action par translation à gauche sur les classes à gauche G/H où H est un sous-groupe de G , est transitive car $\text{Orb}(H) = G/H$.

Exemple. Pour l'action par conjugaison de G sur G le stabilisateur

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

est appelé le **centralisateur de h** de h , et on le note alors $C(h)$. On note que le centre du groupe est l'intersection des centralisateurs :

$$Z(G) = \bigcap_{h \in G} C(h).$$

Plus généralement, pour l'action par conjugaison sur les parties de E ,

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

on regarde souvent l'orbite d'un sous-groupe H de G , alors $\text{Orb}(H)$ consiste en les conjugués de H , et

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

est appelé **le normalisateur de H** . On le note alors par $N(H)$. On observe que $N(H) = G$ si et seulement si H est normal dans G .

Proposition 4.4. *Soit G un groupe, E un G -ensemble.*

1. *Si $x \in E$, alors $\text{Stab}(x)$ est un sous-groupe de G .*
2. *Si $\text{Orb}(x) = \text{Orb}(y)$, où $x, y \in E$, alors $\text{Stab}(x)$ et $\text{Stab}(y)$ sont conjugués.*

Démonstration. (1) Il est clair que $e \in \text{Stab}(x)$. Soit $g, h \in \text{Stab}(x)$, alors $h \cdot x = x$ implique que $h^{-1} \cdot x = h^{-1} \cdot (h \cdot x) = (h^{-1}h) \cdot x = x$. Donc $h^{-1} \in \text{Stab}(x)$. De plus $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$ car $g, h \in \text{Stab}(x)$. Donc gh est aussi élément de $\text{Stab}(x)$, ce qui conclut la preuve de la proposition.

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

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

et on a $h = g(g^{-1}hg)g^{-1}$. Cela montre la première inclusion. Soit $k \in \text{Stab}(x)$. 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. ■

Proposition 4.5. *Pour tout groupe G opérant sur un ensemble E , et $x \in E$, on a une bijection entre $\text{Orb}(x)$ et $G/\text{Stab}(x)$.*

Démonstration. Considérons les ensembles $\text{Orb}(x)$ et $\{g\text{Stab}(x) : g \in G\} = G/\text{Stab}(x)$. Notons que

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

On peut donc définir l'application

$$\text{Orb}(x) \rightarrow \{g\text{Stab}(x) : g \in G\}, \quad \text{avec} \quad g \cdot x \mapsto g\text{Stab}(x),$$

qui est bijective d'inverse l'application $g\text{Stab}(x) \mapsto g \cdot x$. ■

Corollaire 4.6 (du théorème de Lagrange). *Si $\text{Orb}(x)$ est fini, alors $\text{Stab}(x)$ est d'indice fini et $|\text{Orb}(x)| = [G : \text{Stab}(x)]$. Si de plus G est fini, alors le cardinal de $\text{Orb}(x)$ et de $\text{Stab}(x)$ divisent le cardinal de G .*

Corollaire 4.7. *Soit G opérant sur E , où G et E sont finis. Soit $E = \text{Orb}(x_1) \sqcup \dots \sqcup \text{Orb}(x_n)$, la partition de E en orbites pour cette action (voir (4.2)). Alors*

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

Ce dernier 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

$$G = \text{Orb}(h_1) \sqcup \dots \sqcup \text{Orb}(h_r),$$

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

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

où on rappelle que $Z(G)$ désigne le centre de G . On obtient ainsi la formule suivante.

Corollaire 4.8. *Soit G un groupe fini et $C(g) = \text{Stab}(g)$ le stabilisateur de $g \in G$ pour l'action de G sur G par conjugaison. Soit $h_1, \dots, h_r \in G$ des représentants des orbites de cette action. Alors :*

$$|G| = |Z(G)| + \sum_{h_i \notin Z(G)} [G : C(h_i)] \quad (4.3)$$

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

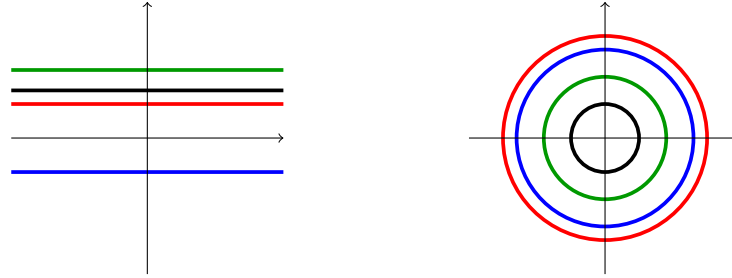
$$\mathbb{R} \times \mathbb{C} \rightarrow \mathbb{C}, \quad \text{avec} \quad (r, z) \mapsto r + z,$$

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

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

qui correspond aux **translations** du plan des complexes. Cette action est transitive et $\text{Stab}(z) = \{0\}$ si $z \in \mathbb{C}^*$ et $\text{Stab}(0) = \mathbb{C}$.

Maintenant, avec $G = (\mathbb{R}, +)$ et $E = \mathbb{C}$, l'action $\mathbb{R} \times \mathbb{C} \rightarrow \mathbb{C}$, où $(\theta, z) \mapsto e^{i\theta} z$, correspond aux **rotations centrales** du plan des complexes. Pour $z \in \mathbb{C}$, l'orbite $\text{Orb}(z)$ est donc le cercle de centre 0 passant par z . Encore une fois, $\text{Stab}(z) = \{e\}$. Enfin, pour $G = (\mathbb{R}^*, \cdot)$ et $E = \mathbb{C}$, on a l'action $\mathbb{R}^* \times \mathbb{C} \rightarrow \mathbb{C}$, avec

FIGURE 4.1 – Orbites respectives, dans \mathbb{C} , pour les actions par translations ou rotations.

$(r, z) \mapsto rz$, 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 $\text{Orb}(z)$ correspond à la droite de direction z , à laquelle on enlève l'origine, et que $\text{Stab}(z) = \{1\}$. D'autre part, pour $z = 0$, l'orbite est $\text{Orb}(0) = \{0\}$, et $\text{Stab}(0) = \mathbb{R}^*$.

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

Exemple (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^n , $n \in \mathbb{N}^*$, en posant

$$G \times E^n \longrightarrow E^n, \quad \text{avec} \quad g \cdot (x_1, \dots, x_n) := (g \cdot x_1, \dots, g \cdot x_n).$$

Il est facile de vérifier directement que ceci donne bien une action de G . On a déjà vu que l'action de G sur E s'étend en une cation de G sur $\mathcal{P}(E)$. En particulier, l'ensemble vide est toujours un point fixe pour cette dernière action, c.-à-d. $\text{Orb}(\emptyset) = \{\emptyset\}$. Il y a un grand nombre d'autres actions qui peuvent ainsi être construites. Ainsi, on a l'action de G sur l'ensemble $\text{Fonct}(F, E)$ des fonctions de F vers E , quelque soit F . En effet, pour $f : F \rightarrow E$ et g dans G , il suffit de considérer la fonction $(g \cdot f) : F \rightarrow E$, 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 :

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

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 voit dans l'exemple suivant comment le groupe symétrique joue un rôle central dans ce contexte.

Exemple (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**

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

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

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

pour les $x_i \in E$. On obtient aussi, en combinant cette action avec l'action de S_E sur l'ensemble $\mathcal{P}(E)$ des parties de E , une 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 $f : E \rightarrow E$; 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**³. Les notions de stabilisateurs, d'orbites, et plusieurs autres concepts de la théorie des groupes y jouent un rôle 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

3. 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>.

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'algorithmes, Programmation fonctionnelle, Sémantique des langages de programmation, etc.), et dans l'étude de certains processus stochastiques.

4.3 Actions transitives et classes modulo un sous-groupe

On est maintenant prêt à classer les actions transitives d'un groupe G . Pour comparer deux actions

$$G \times E \rightarrow E, \quad \text{et} \quad G \times F \rightarrow F,$$

de G , on considère les fonctions $\theta : E \rightarrow F$ qui « préservent » l'action.

Définition. Soit E et F deux G -ensembles. On note \cdot l'action de G sur E et \bullet l'action de G sur F . Une application $\theta : E \rightarrow F$ est un **morphisme de G -ensembles** si :

$$\theta(g \cdot x) = g \bullet \theta(x), \tag{4.4}$$

pour tout g dans G , et tout x dans E .

Si θ est une fonction bijective, alors on dit que c'est un **isomorphisme d'action** et que E et F sont des **G -ensembles isomorphes**.

Théorème 4.9. 1. *Tout G -ensemble se décompose en union disjointe de G -ensembles transitifs.*

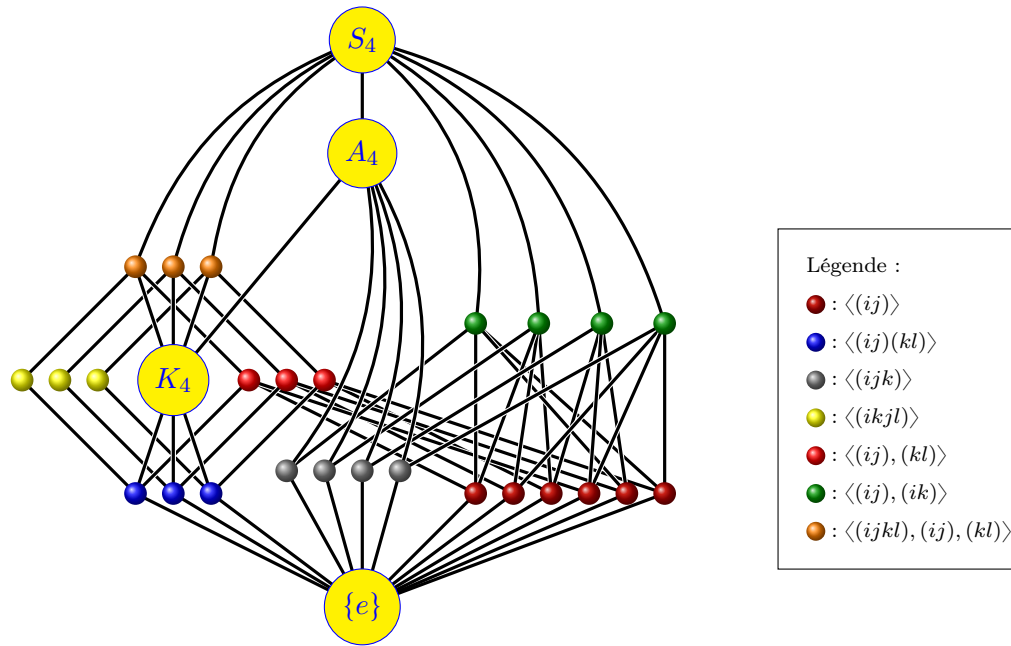
2. *Toute action transitive d'un groupe G est isomorphe à une action de G sur l'ensemble G/H , pour H un sous-groupe de G . Deux telles actions G/H et G/K sont isomorphes, si et seulement si H et K sont conjugués.*

Démonstration. Voir l'exercice 4.12. ■

Corollaire 4.10. *Pour G fini, le nombre d'actions transitives distinctes de G est égal au nombre de classes de conjugaison de sous-groupes de G .*

Remarque. Avec un système de calcul formel, on peut calculer explicitement tous les sous-groupes d'un groupe G fini, et ainsi leur classes de conjugaison et les actions transitives de SG . Dans le cas particulier du groupe symétrique S_4 , on obtient qu'il y a 30 tels sous-groupes, qui sont inclus⁴ les uns

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

FIGURE 4.2 – Le treillis des 30 sous-groupes de S_4 .

dans les autres de la manière illustrée à la Figure 4.2. 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 sous-groupes normaux sont ceux qui sont étiquetés, 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, **30**, 156, 1455, 11300, 151221, 1694723, 29594446, 404126228, 10594925360, 175238308453, ...

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, **11**, 19, 56, 96, 296, 554, 1593, 3094, 10723, 20832, 75154, 159129, 686165, 1466358, 7274651, ...

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.

4.4 Formule 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 lemme⁵ 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 $\text{fix}_g(E)$, l'ensemble des **points fixés** par g dans E , c.-à-d.

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

On a alors l'énoncé suivant.

Théorème 4.11 (Lemme de Burnside-Cauchy-Frobenius). *Pour toute action d'un groupe fini G , sur un ensemble fini E , on a*

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

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,

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

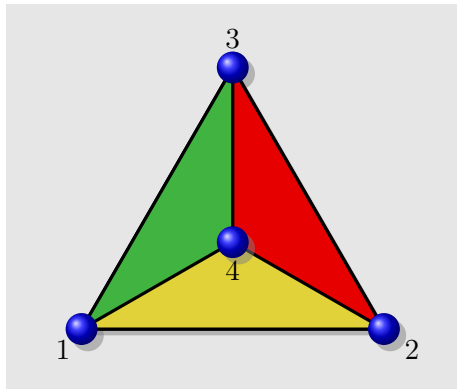
Utilisant la première partie de la proposition 4.5, c.-à-d. $|G| = |\text{Stab}(x)| \cdot |\text{Orb}(x)|$, on trouve d'autre part

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

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.

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 simplement une fonction $\{A, B, C, D\} \rightarrow \{1, 2, \dots, k\}$.



Coloration du tétraèdre.
(La face cachée est bleue)

Les symétries du tétraèdre correspondent exactement aux permutations de $\{A, B, C, D\}$, et l'action de $\sigma \in S_4$ sur une coloration f est de produire la nouvelle coloration

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

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 permu-

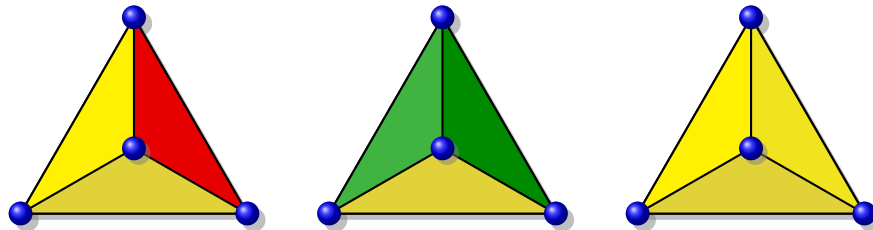


FIGURE 4.3 – Autres colorations possibles du tétraèdre (la face cachée aussi est colorée).

tation, il suffit de considérer sa 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 :

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

Les applications de ce genre mènent à la Théorie de Pólya⁶, qui considère en général l'énumération des structures discrètes modulo l'action d'un groupe.

4.5 Exercices

Questions d'auto-évaluation

Question 4.1. Écrire une preuve de la Proposition 4.1.

Question 4.2. On considère le groupe symétrique S_3 et l'ensemble E des sous-groupe de S_3 . Décrire les orbites et les stabilisateurs pour l'action par conjugaison et pour l'action par translation de S_3 sur E .

Question 4.3. On considère le groupe diédral \mathcal{D}_4 et l'ensemble E des sommets d'un carré. Décrire les orbites et les stabilisateurs pour l'action de \mathcal{D}_4 sur E .

Question 4.4. Soit G un groupe et $H \leq G$, vérifier que $\text{Orb}(H) = G/H$ pour l'action par translation à gauche sur les classes à gauche G/H et donc que cette action est transitive sur G/H .

Question 4.5. Écrire une preuve de la Proposition 4.3.

Réponse : Pour (2) et (3), appliquer ce que l'on sait sur les partitions d'ensemble.

Question 4.6. Soit G un groupe et E un G -ensemble. Vérifier que pour tout $x, y \in E$ on a $\text{Orb}(x) = \text{Orb}(y)$ si et seulement si $x \in \text{Orb}(y)$.

Question 4.7. Un groupe d'ordre 35 opère sur un ensemble de cardinal 19. Combien y a-t-il d'orbites ? Cette action est-elle transitive ?

Question 4.8. Soit G un groupe agissant sur un ensemble X , $g \in G$ et $x, x' \in X$.

(a) Montrer que si $x' = g \cdot x$, alors $x = g^{\text{inv}} \cdot x'$.

(b) Montrer que si $x \neq x'$, alors $g \cdot x \neq g \cdot x'$.

Question 4.9. Soit H le sous-groupe de S_4 engendré par les transpositions $(1, 2)$ et $(3, 4)$. On fait agir H sur l'ensemble $\{1, 2, 3, 4\}$. Déterminer les orbites et les stabilisateurs pour cette action.

Question 4.10. Soit G un groupe. Montrer que la cardinalité de toute classe de conjugaison de G divise l'ordre de G .

Réponse : On fait G agir sur lui-même par conjugaison. La classe de conjugaison d'un élément $h \in G$ est l'orbite de h pour cette action. Donc, $|\text{Orb}(h)| \times |\text{Stab}(h)| = [G : \text{Stab}(h)] \times |\text{Stab}(h)| = |G|$.

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**.

Exercices

Exercice 4.1. 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 4.2. On fait agir S_4 sur les sous-groupe de S_4 d'ordre 4 par conjugaison. Explicitement, si H est un sous-groupe de S_4 et $\sigma \in S_4$, alors $\sigma \cdot H = \{\sigma h \sigma^{-1} \mid h \in H\}$.

(a) Montrer que

$$\{\varepsilon, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\} \quad \text{et} \quad \{\varepsilon, (2, 1, 3, 4), (2, 3)(1, 4), (2, 4, 3, 1)\}$$

appartiennent à la même orbite \mathcal{O} .

(b) Est-ce que $\{\varepsilon, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ appartient à l'orbite \mathcal{O} de la partie précédente ?

Exercice 4.3. Soient H et K deux sous-groupes d'un groupe fini G . Montrer que l'application suivante définit une action de $H \times K$ sur HK : $(h, k) \bullet x = h x k^{-1}$, pour tout $(h, k) \in H \times K$ et $x \in HK$.

Exercice 4.4. Soit G un groupe d'ordre 143 et E un G -ensemble d'ordre 108. Montrer que l'action de G sur E n'est pas transitive et donner le nombre d'orbites.

Exercice 4.5. Soit G un groupe d'ordre 33 et E un G -ensemble d'ordre 19. Montrer que cette action a au moins un point fixe, c'est-à-dire qu'il existe $x \in E$ tel que $g \cdot x = x$ pour tout $g \in G$. Même question avec G un groupe d'ordre 143 et E un G -ensemble d'ordre 108.

Exercice 4.6. Soit G un groupe. On considère l'action par conjugaison de G sur l'ensemble de ses sous-groupes. On note $N(H) = \text{Stab}(H)$ le normalisateur d'un sous-groupe H de G . Soit $H \leq G$, montrer que :

- (a) $N(H)$ est le stabilisateur de H pour l'action par conjugaison ;
- (b) $N(H) = G$ si et seulement si $H \triangleleft G$;
- (c) si G fini, le nombre de sous-groupes de G conjugués à H est égal à l'indice de H dans G et qu'il divise l'ordre de G . Que peut-on dire dans le cas où G est infini.

Exercice 4.7. Soit G un groupe agissant sur un ensemble E .

1. Montrer que pour tout $x \in E$ et pour tout $g \in G$ on a

$$g \text{Stab}_G(x) g^{-1} = \text{Stab}_G(g \cdot x).$$

2. Soit H un sous-groupe de G . Montrer que pour tout $x \in E$ et pour tout $g \in G$ on a

$$g \operatorname{Stab}_H(x) g^{-1} = \operatorname{Stab}_{gHg^{-1}}(g \cdot x).$$

Exercice 4.8. Soit p un nombre premier et $n \in \mathbb{N}^*$. Soit G un groupe d'ordre p^n et $Z(G)$ son centre.

- (a) Montrer que si $G/Z(G)$ est monogène, alors G est abélien.
 (b) Soit $H \triangleleft G$ non réduit à l'élément neutre e de G , on considère l'action de G sur H par conjugaison :

$$(g, h) \mapsto ghg^{-1}.$$

Montrer que $Z(G) \cap H \neq \{e\}$. En déduire que $|Z(G)| = p^k$, où $1 \leq k \leq n$.

- (c) Si $n = 2$, montrer que G est abélien.
 (d) Si $n = 3$ et G est non abélien, montrer que $|Z(G)| = p$ et que le nombre de classes de conjugaison de G est $p^2 + p - 1$,
 (e) Montrer que si G est simple, alors G est abélien.
 (f) En déduire que G est simple si et seulement si $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Exercice 4.9 (Théorème de Cauchy). Soit G un groupe fini et p un nombre premier qui divise $|G|$. Le but de cet exercice est de démontrer le théorème de Cauchy : il existe un élément dans G d'ordre p .

On note $E = \{(g_1, \dots, g_p) \in G^p \mid g_1 g_2 \dots g_p = e\}$.

- (a) Montrer que E est en bijection avec G^{p-1} .
 (b) Pour $n \in \mathbb{Z}$ et $k \in \mathbb{Z}_p$, on note $\rho_k(n)$ l'unique représentant de la classe de $n + k$ modulo p dans l'intervalle $[1, p]$. Montrer que l'application $\mathbb{Z}_p \times E \rightarrow E$ définie par $k \cdot (g_1, \dots, g_p) = (g_{\rho_k(1)}, \dots, g_{\rho_k(p)})$ est une action de \mathbb{Z}_p sur E .

On note x le nombre d'orbites réduites à un élément et y le nombre d'orbite à p éléments.

- (c) Montrer que $n^{p-1} = x + py$.
 (d) Conclure.

Exercice 4.10. 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 $\operatorname{Stab}_B(A) = A \cap B$.

Exercice 4.11. 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 4.12. Soit G un groupe, E un G -ensemble et E' un G' -ensemble dont on note l'action \bullet . Soit $f : E \rightarrow E'$ un morphisme de G -ensembles.

- (a) Montrer que si f est bijective, alors f^{-1} est aussi un morphisme de G -ensembles.
 (b) Soit $x \in E$, montrer que $\operatorname{Stab}(x) \subseteq \operatorname{Stab}(f(x))$. Quand y a-t-il égalité?

- (c) Soit $x \in E$, montrer que le G -ensemble $\text{Orb}(x)$ est isomorphe au G -ensemble $G/\text{Stab}(x)$.
- (d) Montrer que le G -ensemble E est transitif si et seulement si E est isomorphe à $G/\text{Stab}(x)$ pour $x \in E$.

Exercice 4.13. Soit G et G' deux groupes. Soit E un G -ensemble et E' un G' -ensemble. On notera $G_x = \text{Stab}_G(x)$ le stabilisateur de $x \in E$ dans G et $G'_y = \text{Stab}_{G'}(y)$ le stabilisateur de $y \in E'$ dans G' . On dit que le G -ensemble E et le G' -ensemble E' sont équivalents si il existe un isomorphisme de groupes $\theta : G \rightarrow G'$ et une bijection $f : E \rightarrow E'$ tel que

$$\theta(g) \cdot f(x) = f(g \cdot x), \quad \forall g \in G, \forall x \in E.$$

On suppose E et E' équivalents. Montrer que :

1. $G_x \simeq G'_{f(x)}$;
2. l'action de G sur E est transitive si et seulement si l'action de G' sur E' est transitive ;
3. l'action de G sur E est fidèle si et seulement si l'action de G' sur E' est fidèle.

Exercice 4.14. (Classe de conjugaison de S_n)

- (a) Soit $\sigma \in S_n$ et $\alpha = (a_1, \dots, a_k)$ un k -cycle. Montrer que $\sigma\alpha\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k))$ 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.
- (c) Pour une décomposition d'un entier n sous la forme d'une somme

$$n = \mu_1 + \mu_2 + \dots + \mu_k, \quad \text{avec} \quad \mu_1 \geq \mu_2 \geq \dots \geq \mu_k \geq 1,$$

on dit que $\mu = (\mu_1, \mu_2, \dots, \mu_k)$ 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 suivantes :

$$4, \quad 3 + 1, \quad 2 + 2, \quad 2 + 1 + 1, \quad 1 + 1 + 1 + 1.$$

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 bijection avec les partages de n .

- (d) Montrer que le nombre de permutations, dans la classe de conjugaison qui correspond à un partage μ , est donné par la formule

$$\frac{n!}{1^{d_1} d_1! 2^{d_2} d_2! \dots n^{d_n} d_n!} \tag{4.5}$$

où chaque $d_\ell = d_\ell(\mu)$ est le nombre de parts égale à ℓ dans μ .

Exercices exploratoires

Exercice 4.15 (Représentations linéaires des groupes). Soit G un groupe et V un \mathbb{C} -espace vectoriel. On suppose que V est munit d'une structure de G -ensemble de morphisme associé $\rho : G \rightarrow S_V$. On dit que V est un G -module, ou de manière équivalente que ρ est une représentation de G sur V , si $\rho(G) \subseteq \text{GL}(V)$. On suppose G fini d'ordre n , montrer que les valeurs propres de $\rho(g)$ sont toutes des racines n ième de l'unité.

Exercice 4.16. Si X est un espace topologique (voir Exercice 1.52), et G est un groupe topologique, on dit qu'on a une **action continue de groupes**

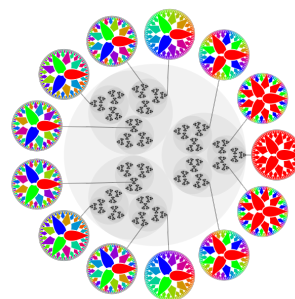
$$X \times G \rightarrow X,$$

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.

Chapitre 5

Les p -groupes, et théorèmes de Sylow



Les théorèmes de Sylow¹ permettent de prédire l'existence de certains sous-groupes dans un groupe fini, seulement en considérant le cardinal du groupe. En particulier, les théorèmes de Sylow sont un premier outil de détection de sous-groupes normaux dans un groupe fini, et ainsi un premier outil de classification des groupes simples.

5.1 Les p -groupes

Un **p -groupe fini** est un groupe fini qui possède p^n éléments où $n \in \mathbb{N}$ et p est un nombre premier.

Proposition 5.1. *Soit G un p -groupe.*

1. *Tout sous-groupe de G est un p -groupe.*
2. *Si G n'est pas le groupe trivial alors son centre n'est pas non plus trivial.*
3. *Si G est d'ordre p ou p^2 , alors G est abélien et isomorphe à \mathbb{Z}_p , \mathbb{Z}_{p^2} ou $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Démonstration. (1) est une conséquence du théorème de Lagrange. (2) Voir Exercice 4.8. (3) Le fait que un groupe d'ordre p ou p^2 est abélien est l'exercice ??. On sait déjà qu'un groupe d'ordre p est isomorphe à \mathbb{Z}_p . On considère G d'ordre p^2 . Si il existe dans G un élément d'ordre p^2 alors G est cyclique d'ordre p^2 . Donc G est isomorphe à \mathbb{Z}_{p^2} . Si il n'existe pas d'élément d'ordre p^2 dans G alors,

1. **Ludwig Sylow**, (1832-1918).

en vertu du théorème de Lagrange, tous les éléments de G sauf e sont d'ordre p . Soit $x \in G$ d'ordre p , on note $H = \langle x \rangle$. Soit $y \in G \setminus H$. On note $K = \langle y \rangle$. On note que tous les éléments de H et K différent du neutre sont d'ordre p . Soit $z \in H \cap K$. Alors $z = x^k = y^l$ avec $1 \leq k, l \leq p$. Si $l = k = p$ alors $z = e$. Si $k \neq p$ alors $y \neq e$ et $y^l \in H$. Comme y^l est d'ordre p on en déduit que $K = \langle y^l \rangle = H = \langle x^k \rangle$, contredisant ainsi $y \notin H$. On en déduit alors (exercice) que $G = HK \simeq H \times K \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. ■

Proposition 5.2. *Soit G un p -groupe et E un G -ensemble fini. Alors le nombre de point fixe de E sous l'action de G est congrus à $|E|$ modulo p .*

Démonstration. On sait que $|E|$ est somme du cardinal des orbites. Soit a le nombre d'orbites réduites à un élément, c'est-à-dire, la somme des cardinaux des orbites réduites à un élément. Soit x_1, \dots, x_k des représentants des orbites non réduites à un élément. Comme le cardinal d'une orbite divise $|G|$, le nombre premier p divise $|\text{Orb}(x_i)|$, pour tout $1 \leq i \leq k$. Donc :

$$|E| = a + \sum_{i=1}^k |\text{Orb}(x_i)|$$

est congrus à a modulo p . ■

5.2 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 général² 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 2.30). 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.

Définition. Soit G un groupe fini d'ordre $|G| = p^n m$, avec $n \in \mathbb{N}^*$ et p premier ne divisant pas m . On dit qu'un sous-groupe de G est un **sous-groupe de Sylow** si son ordre est p^n . Autrement dit, c'est un p -sous-groupe d'ordre le plus grand possible.

On remarque que l'ordre de tout groupe fini G peut s'écrire $|G| = p^n m$, avec $n \in \mathbb{N}^*$ et p premier ne divisant pas m .

2. Bien qu'elle le soit pour les groupes abéliens. Voir l'exercice 6.2.

- Exemples.**
1. Si $G = \mathbb{Z}_N$ avec $N = p^n m$, $n \in \mathbb{N}^*$ et p ne divise pas m , alors pour tout $1 \leq k \leq n$ le sous-groupe engendré par la classe de $p^{n-k}m$ est d'ordre p^k . Il existe donc un p -sous-groupe de Sylow.
 2. Si $G = S_3$ d'ordre $6 = 2 \cdot 3$, il existe exactement trois 2-sous-groupes de Sylow qui sont conjugués, ceux engendré par les transpositions, et exactement un 3-sous-groupe de Sylow, qui est engendré par le cycle $(1\ 2\ 3)$ et est normal dans S_3 .

Théorème 5.3 (Premier théorème de Sylow). *Soit G un groupe fini d'ordre $|G| = p^n m$, avec $n \in \mathbb{N}^*$ et p premier ne divisant pas m . Alors le groupe G possède un sous-groupe d'ordre p^s pour tout $0 \leq s \leq n$. En particulier, G contient un p -sous-groupe de Sylow.*

Comme les sous-groupes d'ordre p premier sont cycliques, on en déduit le corollaire suivant, qui peut aussi être démontré sans le théorème de Sylow (voir Exercice 4.9).

Corollaire 5.4 (Théorème de Cauchy). *Soit G un groupe fini et p un nombre premier qui divise $|G|$, alors G possède un élément d'ordre p .*

Lemme 5.5 (Théorème de Cauchy pour les groupes abéliens). *Soit G un groupe abélien fini et p un nombre premier qui divise $|G|$. Alors il existe un élément d'ordre p dans G .*

Démonstration. Pour $N \geq 2$ un entier et $N = p_1^{a_1} \dots p_l^{a_l}$ sa décomposition en nombres premiers on note $P(N) = a_1 + \dots + a_n \geq 1$.

On démontre par récurrence sur $a \in \mathbb{N}^*$ la propriété suivante : si G est groupe fini abélien tel que $P(|G|) = a$, alors possède un élément d'ordre p premier pour tous les nombres premiers p qui divisent $|G|$.

Si $a = 1$ alors G est d'ordre un nombre premier p et est donc cyclique engendré par un élément d'ordre p .

Supposons maintenant $a > 1$. Soit p un nombre premier qui divise $|G|$ et soit $x \in G \setminus \{e\}$. On note $H = \langle x \rangle \triangleleft G$, car G abélien. Si p divise $h = |H|$ alors l'élément $x^{h/p}$ est un élément d'ordre p (exercice). Supposons que p ne divise pas H . Comme $H \triangleleft G$, on peut considérer le groupe quotient G/H . Comme $|G| = |G/H| \cdot |H|$ et $H \neq \{e\}$, on a $P(G/H) \leq a - 1$, et comme p ne divise pas $|H|$, p divise nécessairement $|G/H|$. Donc par récurrence, il existe un élément yH dans G/H d'ordre p . D'où $H = y^p H$ et donc $y^p \in H$. Comme H est fini, on a $(y^p)^k = e$ avec $k := \text{ord}(y^p)$. Finalement, on a donc $\text{ord}(y^k) = p$ ce qui conclut la preuve. ■

Démonstration du théorème 5.3. On procède par récurrence sur l'ordre du groupe $|G| = p^n m$.

On sait que $|G| > 1$ car p divise le cardinal de G . Considérons l'action de G sur lui-même par conjugaison, et soit $G = \text{Orb}(x_1) \sqcup \dots \sqcup \text{Orb}(x_r)$ la partition de G en orbites, avec les orbites ordonnées

en ordre croissant de cardinalité. Considérons la relation déjà vue

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

Soit $1 \leq s \leq n$, on distingue deux cas.

Dans le premier cas, 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 sous-groupe de G d'ordre p^s .

Dans le deuxième cas, p divise $|Z(G)|$. Alors $Z(G)$ possède un élément d'ordre p , disons c , en vertu du Lemme 5.5 car $Z(G)$ abélien. 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 $H = \pi^{-1}(K)$, où π est le morphisme naturel $G \rightarrow G/H_0$. C'est un sous-groupe de G tel que $H_0 \subseteq H$ 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. ■

Théorème 5.6 (Deuxième théorème de Sylow). *Soit G un groupe fini. Pour chaque diviseur premier p de $|G|$, les p -sous-groupes de Sylow sont conjugués.*

Démonstration. 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' . Par le théorème de Lagrange, $|G/S| = m$ et on rappelle que le groupe G agit 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

$$|G/S| = \sum_i [S' : \text{Stab}_{S'}(T_i)]$$

où T_1, T_2, \dots sont les translatés de S par les éléments de S' . On note que tous les $[S' : \text{Stab}_{S'}(T_i)]$ divise p^n alors que p ne divise pas $|G/S|$. Il doit donc y avoir au moins un $[S' : \text{Stab}_{S'}(T_i)]$ qui soit égal à 1, disons pour $T_i = gS$. On a donc $x \cdot gS = xgS = gS$, pour tout $x \in S'$. 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. ■

Le troisième théorème de Sylow donne une formule pour le nombre de p -sous-groupes de Sylow.

Théorème 5.7 (Troisième théorème de Sylow). *Soit G un groupe fini, et p un diviseur premier de $|G|$. Soit N_p le nombre de p -sous-groupes de Sylow de G . Alors $N_p = [G : N(S)]$ divise $|G|$, où S est n'importe quel p -sous-groupe de Sylow, et $N_p \equiv 1 \pmod{p}$.*

Démonstration. Exercice 5.3 ■

Remarque. (a) Comme $N_p \equiv 1 \pmod{p}$, N_p ne divise pas p^n , donc N_p divise m .

- (b) 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 $N_p \equiv 1 \pmod{p}$.
- (c) 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 $[G : N(S)]$.
- (d) 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, c'est à dire si et seulement si $N_p = 1$.
- (e) Si $N_{p,s}$ désigne le nombre de sous-groupes d'ordre p^s , alors on peut montrer que $N_{p,s} \equiv 1 \pmod{p}$.

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, $N_5 \equiv 1 \pmod{5}$. 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, \dots, K_{10} les 3-sous-groupes de Sylow, d'ordre 3, et H_1, \dots, 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.

La proposition suivante peut s'avérer très utile afin de montrer qu'un groupe possède un sous-groupe normal, comme l'illustre l'exemple qui suit.

Proposition 5.8. 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. Voir Exercice 1.22. ■

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 $|N(H \cap K)| \geq |HK| = 32$. Puisque $|N(H \cap K)|$ doit aussi être un facteur de 48 on doit avoir $|N(H \cap K)| = 48$. Donc $N(H \cap K) = G$, autrement dit $H \cap K$ est normal dans G , et on a trouvé un sous-groupe normal de G .

5.3 Exercices

Questions d'auto-évaluation

Question 5.1. Déterminer (en justifiant votre réponse) tous les sous-groupes de Sylow de S_4 et S_5 .

Question 5.2. Montrer qu'un groupe d'ordre 12 n'est jamais simple.

Réponse : Il suffit de calculer le nombre de sous-groupes de Sylow et d'observer qu'il y a toujours un sous-groupe normal d'ordre 4.

Question 5.3. Démontrer le troisième théorème de Sylow. (Indication : reprendre la preuve du deuxième théorème de Sylow et la raffiner).

Exercices

Exercice 5.1. Montrez que tout groupe d'ordre 96 possède au moins un sous-groupe normal propre.

Exercice 5.2. Un groupe d'ordre 105 peut-il être simple ? (justifier votre réponse)

Exercice 5.3. 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 5.4. Soit G un groupe fini et $T \triangleleft G$. 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 5.5. Soit p un nombre premier.

- Montrer que dans un groupe d'ordre $4p$, un p -sous-groupe de Sylow est toujours normal si $p \geq 5$.
- Est-ce vrai pour $p = 3$? Justifier.

Exercice 5.6. Soit G un groupe non abélien d'ordre $182 = 2 \cdot 7 \cdot 13$.

- Montrer que G a un unique 7-sous-groupe de Sylow, on le note H .
- Montrer que et que le nombre de 13-sous-groupe de Sylow de G est égal à 1 ou 14.

- (c) Soit K un 13-sous-groupe de Sylow. Montrer que $L = HK$ n'a qu'un seul 13-sous-groupe de Sylow. En déduire le nombre de 13-sous-groupes de Sylow de G .
- (d) Montrer que $L \triangleleft G$.
- (e) Soit $x \in G$ d'ordre 2. Prouver que G est isomorphe au produit semi-direct $L \rtimes \langle x \rangle$.
- (f) Montrer qu'à isomorphisme près, il existe au moins 4 groupes d'ordre 182 et qu'ils sont classés par leur nombre d'éléments d'ordre 2.
- (g) Donner le nombre exact de groupes d'ordre 182. Pour cela on regardera le nombre de produit semi-direct externe, c'est-à-dire, compter le nombre de morphisme de \mathbb{Z}_2 dans $\text{Aut}(\mathbb{Z}_{91})$.

Exercice 5.7. 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 5.8.

- (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 $\text{Stab}(z)$ et décrire géométriquement $\text{Orb}(z)$ dans le plan complexe.
- (c) Vérifier que le groupe des isométries de l'icosaèdre possède un sous-groupe d'ordre 2 qui est normal.

Exercice 5.9. Soit G un groupe d'ordre 8. Montrer que G est isomorphe à l'un des groupes suivants : le groupe des quaternions $Q_8 = \langle s, t \mid s^4 = e, s^2 = t^2, tst^{-1} = s^{-1} \rangle$; $\mathbb{Z}/8\mathbb{Z}$; $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou \mathcal{D}_4

Exercice 5.10. Soit G un groupe fini et p un nombre premier. Soit $N \triangleleft G$ tel que p divise $|N|$.

- (a) Soit P un p -sous-groupe de Sylow de N , montrer que $G = N_G(P)N$. On rappelle que le normalisateur $N_G(H)$ pour $H \leq G$ est le sous-groupe stabilisateur de H pour l'action de G par conjugaison sur l'ensemble des parties de G : $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.
- (b) Soit P un p -sous-groupe de Sylow de G et $H \leq G$ tel que $N_G(P) \subseteq H$, montrer que $N_G(H) = H$.
- (c) On suppose que $|G/N| = p^n$ avec $n \geq 2$, montrer qu'il existe $H \triangleleft G$ tel que $|G/H| = p$.

Exercice 5.11. Soit G un groupe d'ordre 63. Montrer que G n'est pas simple.

Exercice 5.12. Soit G un groupe fini simple et p un nombre premier divisant l'ordre de G . On note N_p le nombre de p -sous-groupes de Sylow dans G . Montrer qu'il existe un morphisme de groupe injectif de G dans S_{N_p} . En déduire que $|G|$ divise $N_p!$

Exercice 5.13. Soit G un groupe d'ordre $2p$ avec p premier impair.

- (a) On suppose G abélien, montrer que $G \simeq \mathbb{Z}/2p\mathbb{Z}$.

On suppose à partir de maintenant que G est non abélien.

- (b) Montrer qu'il existe un unique sous-groupe H d'ordre p et que $H = \langle r \rangle$ est cyclique.
- (c) Montrer qu'il existe $K \leq G$ d'ordre 2 tel que $G = H \rtimes K$ (produit semi-direct interne).
- (d) On pose $K = \langle s \rangle$, montrer que $sr \notin H$. En déduire que $(sr)^2 = e$.
- (e) Montrer que $G \simeq \langle a, b \mid a^2, b^p, abab \rangle$ est une présentation de G par générateurs et relations et que G est isomorphe au groupe diédral \mathcal{D}_p .

Exercices exploratoires

Exercice 5.14. 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 $H \triangleleft G$. Rappelons que G opère par translation à gauche sur l'ensemble $E := G/H = \{H, x_1H, \dots, x_{p-1}H\}$, et qu'il s'ensuit qu'il existe un morphisme de groupes $\varphi : G \rightarrow S_E$.

- (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 $L = \varphi(H)$, montrer 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 $H \triangleleft G$.

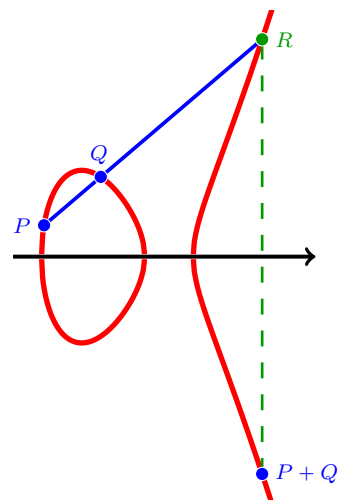
Exercice 5.15. Classifier, à isomorphisme près, les groupes de cardinal 12. (Dans le cas non abélien, on pourra distinguer les cas en fonction du nombre de 3-sous-groupes de Sylow, puis montrer que ce groupe est isomorphe à : $\mathcal{A}_4 \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}))$.)

Exercice 5.16. Classifier, à isomorphisme près, tous les groupes finis d'ordre plus petit ou égal à 15.

Exercice 5.17. Montrer que tout groupe simple d'ordre 60 est isomorphe au groupe alterné \mathcal{A}_5 .

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 (Théorème de Kronecker). *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. Comme on se trouve dans le cadre des groupes abéliens, tous les sous-groupes considérés sont automatiquement normaux. 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 $H_1 \oplus H_2 \oplus \dots \oplus H_n$.

6.1 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

$$G(p) := \{x \in G \mid \text{il existe } n \in \mathbb{N}, \text{ ord}(x) = p^n\}.$$

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

Proposition 6.2. *Soit p un nombre premier et G un groupe abélien, alors $G(p)$ est un sous-groupe de G .*

Démonstration. On a $e \in G(p)$ puisque $\text{ord}(e) = 1 = p^0$. D'autre part, si $x \in G(p)$, alors $x^{-1} \in G(p)$ car $\text{ord}(x^{-1}) = \text{ord}(x)$. 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 $\text{ord}(x) = p^{n_1}$ et $\text{ord}(y) = p^{n_2}$. On calcule alors que

$$(xy)^{(p^n)} = \underbrace{xy \cdot xy \cdot \dots \cdot xy}_{p^n \text{ fois}} = \underbrace{xx \dots x}_{p^n \text{ fois}} \cdot \underbrace{yy \dots y}_{p^n \text{ fois}} = x^{(p^n)} y^{(p^n)},$$

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 $\text{ord}(xy)$, de sorte que $\text{ord}(xy)$ est forcément une puissance de p . ■

Considérons par exemple $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. On a évidemment $\text{ord}(1) = 6$, $\text{ord}(2) = 3$, $\text{ord}(3) = 2$, $\text{ord}(4) = 3$, $\text{ord}(5) = 6$, et $|G| = 2 \cdot 3$. On constate que $G(2) = \{0, 3\}$, $G(3) = \{0, 2\}$. D'autre part, pour $\mathbb{Z}_{24} = \{0, 1, 2, \dots, 24\}$. 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 est une puissance de p .

Proposition 6.3. *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. Voir Exercice 3.1 ■

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.

Corollaire 6.4. *La composante primaire $G(p)$ est l'unique p sous-groupes de Sylow de G .*

Démonstration. Comme G est abélien, tous les sous-groupes sont normaux et donc il existe un unique p -sous-groupe de Sylow. Comme les éléments de l'unique p -sous-groupes de Sylow sont d'ordre une puissance de p , on a forcément qu'il est contenu dans $G(p)$. Or $G(p)$ est un p -sous-groupe de G dont l'ordre maximal possible est celui du p -sous-groupe de Sylow, ce qui entraîne l'égalité. ■

6.2 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 $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ où les p_i sont premiers. Alors G est produit direct interne de ses composantes primaires $G(p_i)$, en particulier $G \simeq G(p_1) \times \dots \times G(p_k)$.*

Par exemple, comme on l'a 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 $y_1, \dots, y_n \in G$, respectivement tels que $\text{ord}(y_i) = m_i$, avec les m_i relativement premiers deux à deux. Alors $\text{ord}(y_1 \dots y_n) = m_1 \dots m_n$.*

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 $\text{ord}(y_1) = m_1$ et $\text{ord}(y_2) = m_2$. À voir : $\text{ord}(y_1 y_2) = m_1 m_2$. Il suffit de voir que si $(y_1 y_2)^m = e$ alors m est un multiple de $m_1 m_2$. Notons que $\langle y_1 \rangle \cap \langle y_2 \rangle = \{e\}$; en effet posons $H = \langle y_1 \rangle \cap \langle y_2 \rangle$, alors H est un sous-groupe de $\langle y_1 \rangle$ et $\langle y_2 \rangle$, donc $|H|$ divise m_1 et m_2 , d'où $|H| = 1$ car m_1 et m_2 sont premiers entre eux. Supposons $(y_1 y_2)^m = e$. On a $(y_1 y_2)^m = y_1^m y_2^m$ car G est abélien. On obtient $y_1^m = y_2^{-m} \in H$, donc $y_1^m = e$ et $y_2^{-m} = e = y_2^m$. Il s'ensuit que m est un multiple de m_1 et m_2 , donc un multiple de $m_1 m_2$, car m_1 et m_2 sont premiers entre eux. ■

Lemme 6.7. *Soient G un groupe abélien et H_1, \dots, H_n des sous-groupes de G . Alors*

$$\langle H_1 \cup \dots \cup H_n \rangle = H_1 H_2 \dots H_n$$

est un sous-groupe de G

Démonstration. Voir exercice 2.27. On a

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

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

Démonstration du théorème 6.5. On sait que les $G(p_i)$ sont des sous-groupes normaux car G abélien. Par le lemme précédent, on a

$$\left\langle \bigcup_{1 \leq i \neq j \leq k} G(p_j) \right\rangle = \prod_{i \neq j}^n G(p_j).$$

Afin de mon montrer que G est le produit direct interne de ses sous-groupes primaires, il faut montrer les deux énoncés suivants (voir l'exercice 2.27 qui concerne le produit direct interne de plusieurs sous-groupes).

(1) Il faut voir que $G(p_i) \cap \prod_{i \neq j}^n G(p_j) = \{e\}$, puis que $G = G(p_1) \dots G(p_k)$. 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 $\text{ord}(x) = p_i^{t_i}$ pour un certain $t_i \leq \alpha_i$. D'autre part, on peut écrire x comme un produit

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

avec les $x_j \in G(p_j)$, et donc ayant $\text{ord}(x_j) = p_j^{t_j}$, pour certains $t_j \leq \alpha_j$. En vertu du lemme 6.6 ci-dessus on a

$$\text{ord}(x_1 \dots \widehat{x_i} \dots x_k) = p_1^{t_1} \dots \widehat{p_i^{t_i}} \dots p_k^{t_k}.$$

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 $x = e$.

(2) Maintenant, pour $x \in G$, on cherche à construire des $x_i \in G(p_i)$ tels on a $x = x_1 x_2 \dots x_k$. Pour ce faire, rappelons que $\text{ord}(x)$ divise $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, et donc

$$\text{ord}(x) = n = p_1^{t_1} \dots p_k^{t_k}, \quad \text{pour} \quad 0 \leq t_i \leq \alpha_i.$$

Ainsi, si on pose $n_i := n/p_i^{t_i}$, on a que $\text{pgcd}(n_1, \dots, n_k) = 1$. 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 $|G(p_i)| = p_i^{\alpha_i}$.

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.*

La preuve est une conséquence des deux lemmes suivants.

Lemme 6.10. *Soit G un p -groupe abélien fini qui contient un unique sous-groupe d'ordre p , alors G est cyclique.*

Démonstration. ■

Lemme 6.11. *Soit G un p -groupe abélien fini et H un sous-groupe cyclique d'ordre maximal. Alors il existe $K \leq H$ tel que $G = HK$ est un produit direct interne.*

Démonstration. ■

Démonstration du Théorème 6.9. ■

6.3 Théorème principal

Théorème 6.12. *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 6.13. *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*

$$G \simeq G_1 \times \dots \times G_r$$

et

$$G \simeq H_1 \times \dots \times H_s$$

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 6.14. *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.*

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 :

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

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

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \text{et} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

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 .

6.4 Exercices

Exercice 6.1. Désignons par $\text{ord}(z)$ l'ordre de l'élément z dans un groupe donné. Donnez un contre-exemple pour vérifier que la relation $\text{ord}(xy) = \text{ppcm}(\text{ord}(x), \text{ord}(y))$ 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. Montrer que si n_1, \dots, n_k sont des entiers premiers entre eux, alors

$$\mathbb{Z}_{n_1 \dots n_k} \simeq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}.$$

Exercice 6.4. 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 6.5. Énumérer tous les groupes abéliens d'ordre 72, à isomorphisme près.

Exercice 6.6. Les groupes $\mathbb{Z}_{12} \times \mathbb{Z}_{72}$ et $\mathbb{Z}_{18} \times \mathbb{Z}_{48}$ sont-ils isomorphes ?

Exercice 6.7. Soit G un groupe abélien, H_1, \dots, H_n des sous-groupes, et $H = H_1 H_2 \dots H_n$.

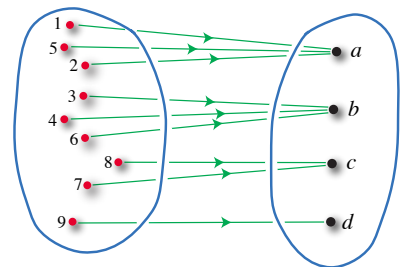
(a) Montrer que $H \leq G$.

(b) Montrer que H est le plus petit sous-groupe de G qui contienne $H_1 \cup \dots \cup H_n$.

Exercice 6.8. Faire la liste de tous les groupes abéliens finis d'ordre 252, à isomorphisme près. Justifier.

Annexe A

Rappels sur les ensembles et fonctions



A.1 Le langage ensembliste

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 $E = \{x_1, x_2, \dots, x_m\}$ signifie donc que E est composé des éléments x_1, x_2, \dots, 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 $A = \{x \in E \mid x \text{ possède } P\}$ 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

$$\begin{aligned} \mathcal{A} &:= \{a, b, c, d, \dots, z\}, \\ \mathbb{N} &:= \{0, 1, 2, 3, \dots\}, \\ \mathbb{Z} &:= \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}, \\ \mathbb{Q} &:= \{a/b \mid a \in \mathbb{Z}, \quad b \in \mathbb{N}, \text{ et } b \neq 0\}, \\ \mathbb{C} &:= \{x + iy \mid x, y \in \mathbb{R}\}, \end{aligned}$$

où \mathbb{R} désigne l'ensemble des **nombre réels**, ou encore des ensembles d'objets divers comme

$$\{\bullet, \blacklozenge, \heartsuit, \spadesuit\}, \quad \text{ou} \quad \{\clubsuit, \diamond, \heartsuit, \spadesuit\}.$$

L'ensemble qui ne contient aucun élément est, par définition, l'ensemble **vide**, et on le représente par le symbole \emptyset . 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 $E = \{x_1, \dots, x_n\}$, 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 $|\emptyset| = 0$. 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.

Sous-ensemble. 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**. Pour montrer $A \subseteq E$ il faut et il suffit de montrer que pour tout $a : a \in A \implies a \in E$.

Les ensembles \emptyset 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 $A \not\subseteq E$. 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 $\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, E\}$. 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 $A \setminus B$, est l'ensemble défini par

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

Si le contexte fait en sorte que l'ensemble E est clair, et si $A \subseteq E$, alors on écrit parfois $A^c := E \setminus A$. 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 $E \setminus \{0\}$.

Produit cartésien d'ensembles. 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

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

On observe que $\emptyset \times E = E \times \emptyset = \emptyset$. En effet, il n'existe pas de couple (a, b) tel que $a \in E$ et $b \in \emptyset$. 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

$$x = (x_1, x_2, \dots, x_n), \quad \text{où} \quad x_i \in E,$$

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

$$((x_1, \dots, x_k), (y_1, \dots, y_n)),$$

tandis que ceux du deuxième sont de la forme (très similaire, mais différente)

$$(x_1, \dots, x_k, y_1, \dots, y_n).$$

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

$$\eta : E \longrightarrow E \times \{\star\}, \quad \text{avec} \quad \eta(x) := (x, \star).$$

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

$$A \cup B := \{x \mid x \in A \text{ ou } x \in B\}.$$

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

$$A \cap B = \{x \mid x \in A \text{ et } x \in B\}.$$

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 $A \cap B = \emptyset$, 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. $A \cup \emptyset = A$ et $A \cap \emptyset = \emptyset$; et si $A \subseteq B$ alors $A \cup B = B$ et $A \cap B = A$ (existence d'éléments neutres) ;
4. $(A^c)^c = A$; $(A \cup B)^c = A^c \cap B^c$ et $(A \cap B)^c = A^c \cup B^c$ (Lois de Morgan).

La réunion de plusieurs ensembles A_1, A_2, \dots, A_n , où $n \in \mathbb{N}^*$ est notée

$$\bigcup_{1 \leq i \leq n} A_i = A_1 \cup A_2 \cup \dots \cup A_n.$$

Si l'on a une famille infinie d'ensembles $(A_i)_{i \in I}$, on écrit $\bigcup_{i \in I} A_i$ pour leur réunion ; ici, I est un *ensemble d'indices*.

Exemple. Si $A_n = \{0, 1, \dots, n\}$, on aura $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{N}$.

Pour l'intersection, on a des notations analogues.

Exemple. Avec A_n comme dans l'exemple précédent, $\bigcap_{n \in \mathbb{N}} A_n = \{0\}$.

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 $A \uplus B$.

Pour résumer, on a :

$$x \in \bigcup_{i \in I} A_i \iff \exists i \in I, x \in A_i$$

et

$$x \in \bigcap_{i \in I} A_i \iff \forall i \in I, x \in A_i.$$

Partitions d'ensemble Une partition d'un ensemble E est une famille $\{A_i\}_{i \in I}$ de sous-ensembles non vides de E tel que :

- (i) $E = \bigcup_{i \in I} A_i$;
- (ii) Les A_i sont disjoints deux à deux, i.e., pour tout $i, j \in I$ distincts, $A_i \cap A_j = \emptyset$ sont disjoints.

Par exemple, l'ensemble des nombres pairs et l'ensemble des nombres impairs forment une *partition* de \mathbb{Z} . Dans le cas d'un ensemble fini E , les partitions de E jouent souvent un rôle très important dans l'énumération de cet ensemble (c'est-à-dire le calcul de son cardinal).

Proposition A.1. Si $\{A_i\}_{i \in I}$ est une partition d'un ensemble fini E , alors I est fini et

$$|E| = \sum_{i \in I} |A_i|.$$

Démonstration. Exercice. ■

Exemples. (a) $2\mathbb{Z}, \mathcal{I}$ forment une partition de \mathbb{Z} . (b) $2\mathbb{Z}, 3\mathbb{Z}$ ne forment pas une partition de \mathbb{Z} car $6 \in 2\mathbb{Z} \cap 3\mathbb{Z}$. (c) Soit $A_x = [x, x + 1[$ où $x \in \mathbb{Z}$; alors $(A_x)_{x \in \mathbb{Z}}$ est une partition de \mathbb{R} .

A.2 Les fonctions

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. On rappelle qu'une **fonction f de A vers B** , on écrit $f : A \rightarrow B$, est une *relation sur* $A \times B$ qui associe à chaque élément de a un unique élément de B . Plus simplement, 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 $b = c$.

Soit $X \subseteq A$, la **restriction de $f : A \rightarrow B$ à X** est la fonction $f|_X : X \rightarrow B$ définie par $f|_X(a) = f(a)$ pour tout $a \in X$. Par soucis de simplification des notations on note souvent la restriction de f à X par $f : X \rightarrow B$; mais attention à ne pas utiliser f au lieu de $f : A \rightarrow B$ et $f : X \rightarrow B$ pour désigner à la fois la fonction de départ et sa restriction.

La **composition de la fonction $f : A \rightarrow B$ par la fonction $g : B \rightarrow C$** est la fonction $g \circ f : A \rightarrow C$ définie par $g \circ f(x) = g(f(x))$ pour tout $x \in A$. Une fonction f de A vers B , est une **bijection**, si on a une fonction **inverse** $f^{-1} : B \rightarrow A$, pour la composition, c.-à-d. :

$$f^{-1} \circ f = \text{Id}_A, \text{ et } f \circ f^{-1} = \text{Id}_B. \quad (\text{A.1})$$

Une fonction $f : A \rightarrow B$ est **injective** si et seulement si, pour tout a et tout b dans A

$$a \neq b \quad \implies \quad f(a) \neq f(b), \quad (\text{A.2})$$

ce qui équivaut (c'est la contraposée) à dire aussi que

$$f(a) = f(b) \quad \text{entraîne forcément} \quad a = b. \quad (\text{A.3})$$

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 définition², 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 $\text{Fonct}(A, B)$ l'ensemble des fonctions** de A dans B . Dans le cas où $A = B$, on notera S_A l'ensemble des fonctions de A dans A et on l'appellera *groupe symétrique sur A* .

A.3 Relations d'équivalences

Nous allons nous intéresser ici aux relations qui servent à regrouper les éléments d'un ensemble par « familles ». On pourrait par exemple définir une relation qui regroupe les cartes d'un jeu de cartes par couleurs : c'est une relation d'équivalence. Elles jouent un rôle primordial en mathématiques.

Soit E un ensemble et R une relation sur E . On dit que R est une *relation d'équivalence* si \sim est :

Réflexive : $\forall x \in E$, on a xRx .

Symétrique : $\forall x, y \in E$, $xRy \implies yRx$.

Transitive : $\forall x, y, z \in E$, xRy et yRz implique xRz .

2. La définition est nécessaire pour des ensembles infinis.

Exemple. (a) Si $E = \{\text{habitants du Québec}\}$, on peut définir la relation suivante : deux habitants du Québec x et y sont en relation xRy si et seulement si x et y ont le même nom. C'est une relation d'équivalence.

(b) Soit E un ensemble quelconque et considérons la relation R sur E définie par : xRy si $x = y$ (autrement dit, R est l'égalité sur E). Alors R est une relation d'équivalence ($x = x$, $x = y \iff y = x$ et si $x = y$, $y = z$ alors $x = z$).

(c) Prenons un ensemble E et $f : E \rightarrow F$ une fonction. Définissons la relation sur E : xRy si $f(x) = f(y)$. On vérifie que R est une relation d'équivalence sur E .

(d) Les relations d'ordre ne sont pas en général des relations d'équivalence.

Classes d'équivalence et ensemble quotient Soit E un ensemble et R une relation d'équivalence sur E .

1. La *classe d'équivalence* de $a \in E$ est le sous-ensemble de E

$$[a]_R = \{x \in E \mid xRa\}.$$

2. Une *classe d'équivalence* de R est un sous-ensemble A de E , tel qu'il existe $a \in E$ vérifiant $A = [a]_R$.
3. L'ensemble des classes d'équivalence est noté E/R et est appelé *l'ensemble quotient de E par R* .

Remarque. L'ensemble quotient E/R est un objet de première importance en mathématiques. Il est très important de bien en comprendre la nature : les éléments de E/R sont les classes d'équivalence de R , en d'autres termes, des sous-ensembles de E . Donc $E/R \subseteq \mathcal{P}(E)$.

Une classe d'équivalence n'est jamais vide : $a \in [a]_R$ car aRa .

Exemples. On reprend dans l'ordre les exemples précédents.

(a) E/R est en bijection avec l'ensemble des noms représentés au Québec.

(b) Dans ce cas, les classes d'équivalence sont les singletons de E , c'est-à-dire les sous-ensembles à un élément de E . Donc E/R est en bijection avec E .

(c) Une classe d'équivalence est ici de la forme $[x_0]_R = \{x \in E \mid xRx_0\} = \{x \in E \mid f(x) = f(x_0)\} = f^{-1}(f(x_0))$, où $x_0 \in E$. Donc $E/R = \{f^{-1}(f(x_0)) \mid x_0 \in E\} = \{f^{-1}(y) \mid y \in \text{Im}(f)\}$ est en bijection avec $\text{Im}(f)$.

En effet, la fonction $u : E/R \rightarrow \text{Im}(f)$ définie par $u([x_0]_R) = f(x_0)$ est une bijection : si $y \in \text{Im}(f)$ et $x \in f^{-1}(y)$ alors $u([x]_R) = f(x) = y$ donc u est surjective. Si $u([x]_R) = u([x']_R)$ alors $f(x) = f(x')$ et donc $x \in [x']_R$. D'où $[x]_R = [x']_R$ et u est injective.

Il faut noter que cette fonction *est bien définie*, i.e., que la relation u est bien une fonction : on vérifie que si $x \in [x_0]_R$ alors $f(x) = f(x_0)$.

La proposition suivante n'est pas très difficile à démontrer.

Proposition A.2. *Soit R une relation d'équivalence sur E et $x, y \in E$, alors*

1. $x \in [y]_R \iff [x]_R = [y]_R$;
2. $[x]_R \cap [y]_R \neq \emptyset \iff [x]_R = [y]_R$. Autrement dit, deux classes d'équivalence $\lambda, \lambda' \in E/R$ sont disjointes si et seulement si $\lambda \neq \lambda'$.

De plus, l'ensemble quotient E/R forme une partition de l'ensemble E . En particulier, si E est fini alors E/R est fini et

$$|E| = \sum_{A \in E/R} |A|.$$

Remarque. Il est bon de noter que si $\{A_i\}_{i \in I} \subseteq \mathcal{P}(E)$ est une partition de l'ensemble E , alors on peut construire une unique relation d'équivalence R sur E tel que $E/R = \{A_i \mid i \in I\}$: xRy si et seulement si x et y sont dans le même A_i .

Système de représentants des classes d'équivalence Si on prend la relation d'équivalence sur l'ensemble d'un jeu de cartes : deux cartes sont en relation si et seulement si elles ont même couleur. Alors les classes d'équivalences des cartes sont en bijection avec l'ensemble des couleurs : à chaque classe d'équivalence correspond une couleur. C'est là que réside l'idée de système de représentant.

Soit R une relation d'équivalence sur E . Un sous-ensemble I de E est un *système de représentants des classes d'équivalence* de R si la fonction

$$\begin{aligned} I &\longrightarrow E/R \\ x &\longmapsto [x]_R \end{aligned}$$

est une bijection. Les éléments de I sont les *représentants*.

Exemple. Prenons $f : \mathbb{R} \rightarrow \mathbb{R}$ la fonction définie par $f(x) = x^2$. Regardons à nouveau la relation d'équivalence sur E : xRy si $f(x) = f(y)$. Alors $I = \mathbb{R}^+$ est un système de représentants des classes d'équivalence de R . En effet, dans chaque classe $A = \{-x, x\} \in E/R$ il n'y a qu'un unique élément positif.

Remarque. I est un système de représentants de E/R si et seulement si pour tout $A \in E/R$ il existe un et un seul $x \in I$ tel que $A = [x]_R$. Cela provient directement des définitions.

Au sujet de la bonne définition de fonction Dans la pratique, on ne vérifie pas souvent si une fonction f est bien définie, c'est-à-dire, que la relation f est bien une fonction. Mais attention, dans certains cas c'est absolument nécessaire. Prenons $f : \mathbb{R} \rightarrow \mathbb{R}$ la fonction définie par $f(x) = x^2$. Regardons à nouveau la relation d'équivalence sur E : xRy si $f(x) = f(y)$. Alors $\mathbb{R}/R = \{\{-x, x\} \mid x \in \mathbb{R}^+\}$. Voilà le piège habituel : nous voulons considérer la « fonction ». (C'est certainement une relation, mais une fonction ?)

$$\begin{aligned} g : \mathbb{R}/R &\longrightarrow \{-, +\} \\ I = [x]_R &\longmapsto \text{signe de } x \end{aligned}$$

La faute ici est que l'image de $I = [x]_R = [-x]_R$ dépend du choix du représentant de I choisi : x ou $-x$. Donc si $I \neq \{0\}$, on va avoir deux images $-$ et $+$ et donc g **n'est pas une fonction**.

Conclusion. *Quand on veut définir une fonction f de E/R sur un ensemble F à partir d'un élément x de la classe $\lambda \in E/R$, il faut toujours s'assurer que tous les éléments de la classe λ auront la même image que celle de x !*

Exemple. La fonction

$$\begin{aligned} h : \mathbb{R}/R &\longrightarrow \mathbb{R}^+ \\ I = [x]_R &\longmapsto x^2 \end{aligned}$$

est bien définie et est une bijection. En effet, si xRx' alors $x^2 = x'^2$ et donc $[x]_R = [x']_R$ n'a qu'une seule image par la relation h qui est donc bien une fonction.

A.4 Exercices

Questions d'auto-évaluation

Question A.1. Répondre par vraie ou faux aux questions suivantes. Justifier votre réponse.

- (1) $\{4, 1, 2, 3\} \subseteq \{1, 2, 3, 4, 3, 2, 1\}$; (2) $\{4, 1, 2, 3\} \neq \{1, 2, 3, 4, 3, 2, 1\}$;
 (3) $\emptyset \subseteq \{a, b, f, g\}$; (4) $\emptyset \in \{\emptyset, \{\emptyset\}\}$; (5) $\emptyset \subseteq \{\emptyset, \{\emptyset\}\}$; (6) $\{\emptyset\} \in \{\emptyset, \{\emptyset\}\}$;
 (7) $\{\emptyset\} \subseteq \{\emptyset, \{\emptyset\}\}$; (8) $\{\{\emptyset\}\} \in \{\emptyset, \{\emptyset\}\}$; (9) $\{\{\emptyset\}\} \subseteq \{\emptyset, \{\emptyset\}\}$.

Réponse : seules (2) et (8) sont fausses.

Question A.2. Soit $A = \{1, 2, 3\}$, $B = \{4, 5\}$ et $C = \{2, 3, 4, 5\}$. Ecrire les ensembles suivants :

- (a) $\mathcal{P}(A)$; (b) $\mathcal{P}(\mathcal{P}(B))$; (c) $A \setminus B$; (d) $B \setminus A$; (e) B^c dans C ; (f) $C \setminus A$;
 (g) $C \setminus B$; (h) $A \setminus C$; (i) $B \setminus C$.

Question A.3. Soit $f : A \rightarrow B$ et $g : B \rightarrow C$ deux fonctions. Montrer que pour tout $X \subseteq A$ et pour tout $Y \subseteq C$ on a $(g \circ f)(X) = g(f(X))$ et $(g \circ f)^{-1}(Y) = f^{-1}(g^{-1}(Y))$.

Question A.4. La fonction $f : A \rightarrow B$ définie par $f(x) = x^2$ est-elle injective, surjective ou bijective dans les cas suivants :

- (a) $A = B = \mathbb{R}$; (b) $A = B = \mathbb{R}^+$; (c) $A = \mathbb{R}^+$ et $B = \mathbb{R}$; (d) $A = \mathbb{R}$ et $B = \mathbb{R}^+$.

Question A.5. Soit $f : A \rightarrow B$ une fonction, montrer que

- (a) Si $|A| = 1$ alors f est injective. (b) Si $|B| = 1$, A est non vide, alors f est surjective.

Question A.6. Soit $f : E \rightarrow F$ une fonction.

- (a) Montrer que f est injective si et seulement si $f^{-1}(y)$ est un singleton pour tout $y \in \text{Im}(f)$.
 (b) Montrer que f est surjective si et seulement si pour tout $y \in F$ il existe $x \in E$ tel que $f(x) = y$.
 (c) Montrer que f est bijective si et seulement si $f^{-1}(y)$ est un singleton pour tout $y \in F$.
 (d) On considère $f_0 : E \rightarrow f(E)$ définie par $f_0(x) = f(x)$. Vérifier que f_0 est surjective et que f_0 est une bijection si et seulement si f est injective.

Question A.7. Sur l'ensemble $E = \{1, 2, 3, \dots, 30\}$ définissons la relation R par iRj si tout nombre premier p qui divise i divise aussi j . Vérifier que R est bien une relation d'équivalence, écrire l'ensemble quotient et trouver un système de représentants.

Exercices

Exercice A.1. Soit A et B deux ensembles. Montrer que :

- $A \subseteq B$ si et seulement si $A \cap B = A$.
- $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$ (cet ensemble, noté $A \Delta B$, s'appelle la différence symétrique de A et B).
- $A \cap B = A \setminus (A \setminus B)$. 8. $(A \setminus B) \cap B = \emptyset$. 9. $B \setminus A = B \cap A^c$.

Exercice A.2. Soit A , B et C des ensembles. Montrer que

- $A \cup B \subseteq A \cup B \cup C$.
- $A \cap B \cap C \subseteq A \cap B$.
- $(A \setminus B) \setminus C \subseteq A \setminus C$.

4. $(A \setminus C) \cap (C \setminus B) = \emptyset$.
5. $(B \setminus A) \cup (C \setminus A) = (B \cup C) \setminus A$.

Exercice A.3. (a) Montrer que tout entier naturel est égal au produit d'un nombre impair par une puissance de 2.

(b) Soit $A_n = \{(2k + 1) \cdot 2^n \mid k \in \mathbb{N}\}$, montrer que $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{N}$.

(c) Soit $H_x = [x, +\infty[$, avec $x \in \mathbb{R}$. Montrer que $\bigcap_{x \in \mathbb{R}} H_x = \emptyset$.

Exercice A.4. Pour $i \in \mathbb{N}^*$, on note $A_i = \{x \in \mathbb{Z} \mid x \leq i\}$. Trouver, et justifier par récurrence :

$$(a) \bigcup_{i=1}^n A_i \qquad (b) \bigcap_{i=1}^n A_i$$

Exercice A.5. Soit $n \in \mathbb{N}^*$. Pour $0 \leq k \leq n - 1$ on note $A_k = \{np + k \mid p \in \mathbb{Z}\}$. Montrer que la famille $\{A_k\}_{0 \leq k \leq n-1}$ forme une partition de \mathbb{Z} .

Exercice A.6. Pour tout entier n on définit

$$A_n = \{x \in \mathbb{Q} : n \leq x < n + 1\}.$$

Montrer que $\{A_n : n \in \mathbb{Z}\}$ est une partition de \mathbb{Q} .

Exercice A.7. Pour tout nombre réel r on définit

$$A_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y = r\}.$$

Montrer que $\{A_r : r \in \mathbb{R}\}$ est une partition de $\mathbb{R} \times \mathbb{R}$.

Exercice A.8. Soit $f : E \rightarrow F$ une fonction.

1. Si $A_1, A_2 \subseteq E$, montrer que :
 - (a) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$ et trouver un exemple où l'égalité est fautive,
 - (b) $A_1 \subseteq A_2 \implies f(A_1) \subseteq f(A_2)$.
 - (c) Est-ce que $f(A_1 \setminus A_2) \subseteq f(A_1) \setminus f(A_2)$? (Trouver un exemple où l'inclusion est fautive).
2. Si $B_1, B_2 \subseteq F$, montrer que :
 - (a) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$,
 - (b) $B_1 \subseteq B_2 \implies f^{-1}(B_1) \subseteq f^{-1}(B_2)$,
 - (c) $f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$.
3. Si $A \subseteq E$ et $B \subseteq F$, montrer que $f(f^{-1}(B)) \subseteq B$ et $A \subseteq f^{-1}(f(A))$.

Exercice A.9. Soit A_1, A_2, B des ensembles, montrer que

- (a) $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ si et seulement si f est injective ;
- (b) $f(f^{-1}(B)) = B$ si et seulement si f est surjective.

Exercice A.10. 1. Soit $f : A \rightarrow B$ et $g : B \rightarrow C$ deux fonctions. Montrer que

- (a) f et g injectives $\implies g \circ f$ injective ;
- (b) f et g surjectives $\implies g \circ f$ surjective ;
- (c) $g \circ f$ injective $\implies f$ injective ;
- (d) $g \circ f$ surjective $\implies g$ surjective ;
- (e) $g \circ f$ injective et f surjective $\implies g$ injective.

2. Soit $f : E \rightarrow F$, $g : F \rightarrow G$, $h : G \rightarrow E$ des fonctions. On suppose que la fonction $h \circ g \circ f$ est surjective et que les fonctions $g \circ f \circ h$ et $f \circ h \circ g$ sont injectives.

- (a) Montrer que h est inversible.
- (b) Montrer que $g \circ f$ est bijective.
- (c) Montrer que f , g et h sont des bijections.

Exercice A.11. (a) Montrer que \mathbb{N} est infini. (b) Soit $A \subseteq E$ deux ensembles. Montrer que si E est fini alors A est fini et que $|A| \leq |E|$; et montrer que si A est infini alors E est infini.

Exercice A.12. Soit A et B deux ensembles finis.

- 1. Montrer que $|A| \leq |B|$ si et seulement si il existe une injection $i : A \rightarrow B$.
- 2. Montrer que $|A \times B| = |A| \cdot |B|$.
- 3. Montrer que $|A \cup B| = |A| + |B| - |A \cap B|$.
- 4. Montrer que $|\mathcal{P}(A)| = 2^{|A|}$.
- 5. On note B^A l'ensemble des fonctions de A dans B . Cette notation est expliquée par le résultat suivant : montrer par récurrence sur $|A|$ que $|B^A| = |B|^{|A|}$.

Exercice A.13. Soit \sim la relation sur \mathbb{R} définie par $x \sim y$ si $|x| = |y|$.

- (a) Montrer que c'est une relation d'équivalence et déterminer son ensemble quotient \mathbb{R}/\sim .
- (b) Montrer que \mathbb{R}^+ est un système de représentants des classes d'équivalence de \sim .
- (c) Les fonctions ci-dessous sont-elles bien définies? Justifier!

$$f : \mathbb{R}/\sim \longrightarrow \mathbb{R} \quad \text{et} \quad g : \mathbb{R}/\sim \longrightarrow \mathbb{R}$$

$$[x]_{\sim} \longmapsto x \quad \quad \quad [x]_{\sim} \longmapsto |x|$$

Exercice A.14. Soit $\{A_i\}_{i \in I}$ une partition de l'ensemble E et R la relation sur E définie par xRy si et seulement si x et y sont dans le même A_i . Montrer que R est une relation d'équivalence et que $E/R = \{A_i \mid i \in I\}$.

Exercice A.15. Soit R_1, R_2 deux relations d'équivalence sur E . Montrer que la relation R sur E définie par xRy si $(xR_1y$ et $xR_2y)$ est une relation d'équivalence. Décrire les classes d'équivalence de R en fonction de celles de R_1 et de R_2 .

Annexe B

Autres exemples d'actions de groupes

B.1 Actions linéaires

Pour une action $G \times V \rightarrow V$, 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 représentation¹ 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 $G \times V \rightarrow V$ à une action linéaire $G \times W \rightarrow W$ est une transformation linéaire inversible $\theta : V \rightarrow W$, telle qu'on ait le diagramme **commutatif**

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

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

1. 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 théorie² 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

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

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

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

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.

2. 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 $G \leq \text{GL}_n(\mathbb{C})$ 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

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

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

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

et on a les exemples suivants de tels polynômes

$$\begin{aligned} e_1(x, y, z) &= x + y + z, \\ e_2(x, y, z) &= xy + xz + yz \\ e_3(x, y, z) &= xyz. \end{aligned} \tag{B.1}$$

Le cas $n = 3$ du théorème fondamental des polynômes symétriques, dû à Newton³, 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

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

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

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

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

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

3. Sir Issac Newton (1643-1727).

a (au moins) deux racines⁴ égales si et seulement si son discriminant est nul, $D = 0$. 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 (B.1). Par exemple, pour le polynôme $t^3 + 3t^2 - 9t + 5$, 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 (B.2) pour calculer le discriminant. Par contre, la formule (B.3) 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.

B.2 Le groupe des isométries du cube

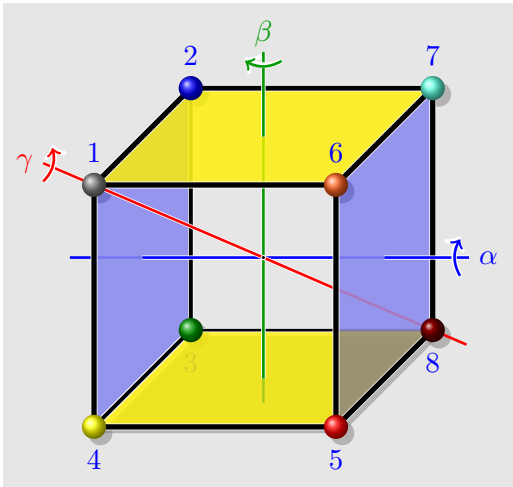


FIGURE B.1 – Rotations du cube.

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

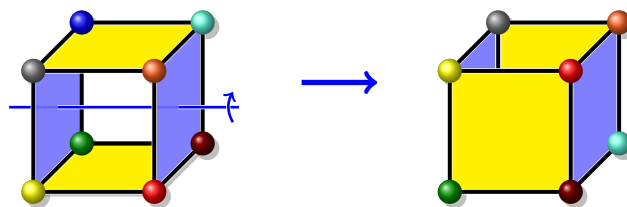
$$\text{ISO}_{\mathbb{R}^3} \times \mathcal{P}(\mathbb{R}^3) \rightarrow \mathcal{P}(\mathbb{R}^3),$$

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 $\rho : G \rightarrow S_8$, 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

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

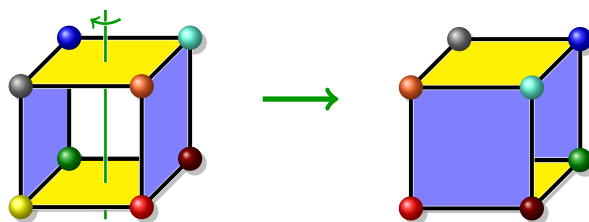
permutation, décomposée en cycles, α s'exprime comme

4. Ce sont ici x , y et z .



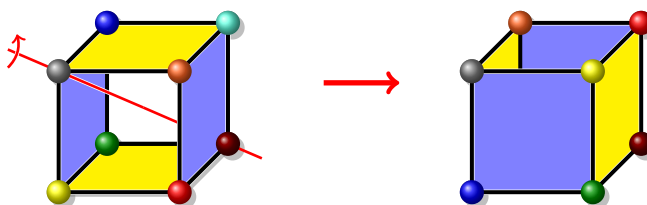
C'est donc un élément d'ordre 4. De même, on a la rotation β , d'angle $\pi/2$ autour de l'axe vertical passant par le centre des faces 1276 et 4385, qui s'exprime comme la permutation d'ordre 4

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



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

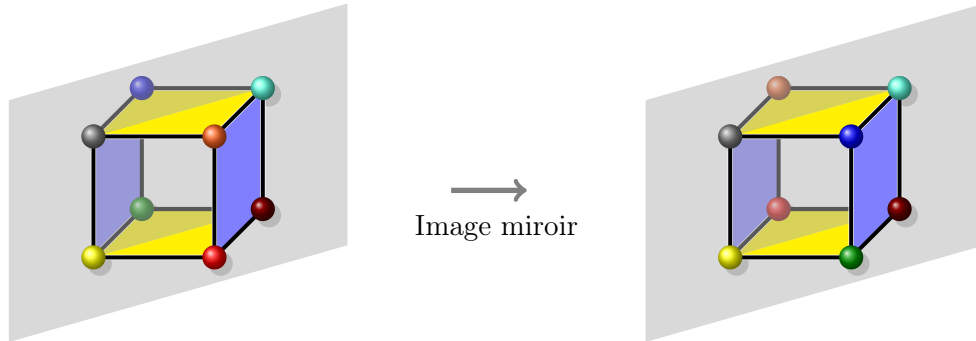
$$\gamma = (246)(357).$$



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'orientation⁵. 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

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

5. 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 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

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

et on calcule directement que

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

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

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

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

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

il suffit donc de calculer $|\text{Stab}(1)|$ pour connaître l'ordre de G . On sait que γ et δ fixent 1, et donc $\text{Stab}(1)$ 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

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

pour conclure qu'on a (au moins⁶) les 6 éléments distincts suivants dans $\text{Stab}(1)$:

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

On constate donc que $|\text{Stab}(1)| \geq 6$, ce qui entraîne que $|G| \geq 48$.

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

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

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

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

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 toutes les diagonales. En particulier, $\theta(g)(\{2, 5\}) = \{g(2), g(5)\} = \{2, 5\}$, et donc $g(2) = 5$ (puisque l'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 3.4), on obtient

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

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

B.3 A_5 comme groupe des rotations du dodécaèdre

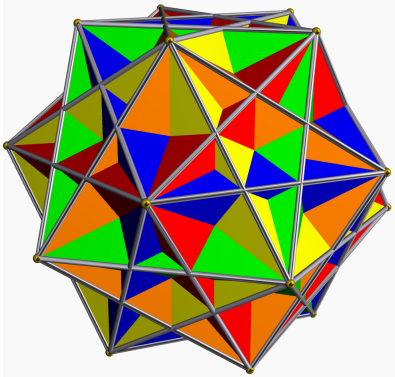


FIGURE B.2 – Les cinq cubes inscrits dans le dodécaèdre.

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 B.3 et B.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 .

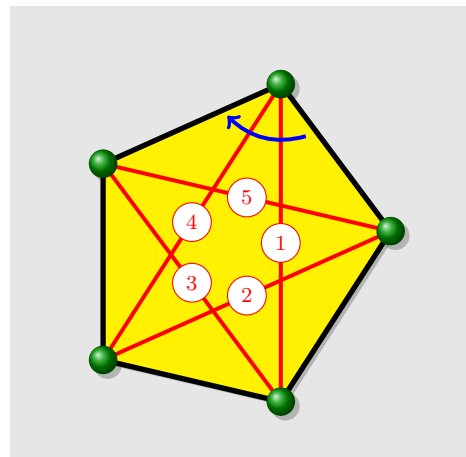
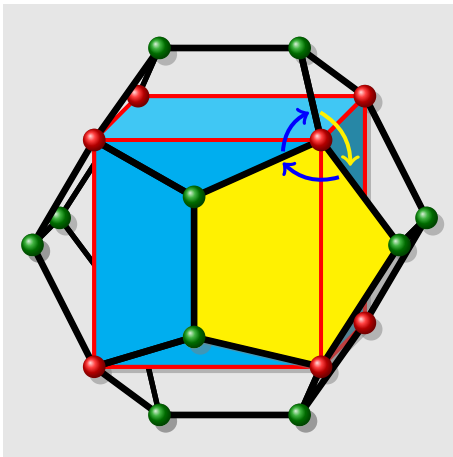


FIGURE B.3 – Une rotation du dodécaèdre autour de l'axe joignant deux sommets opposés, et la permutation des 5 cubes correspondante.

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 B.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).

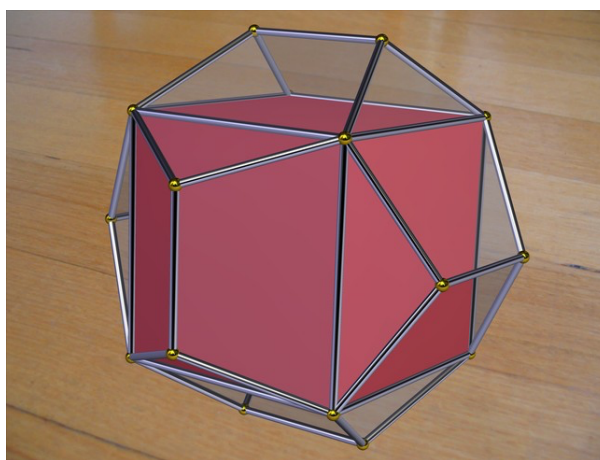


FIGURE B.4 – Version réaliste d'un cube inscrit dans le dodécaèdre.

Le dodécaèdre possède 20 sommets, et il leur 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 B.1) 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 B.1. *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 1.45), 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. ■

L'intuition derrière la preuve de la proposition suivante découle du fait que A_5 est le groupe des rotations du dodécaèdre.

Proposition B.2. *A_5 est un groupe simple.*

Démonstration. Voir exercice 3.23. ■

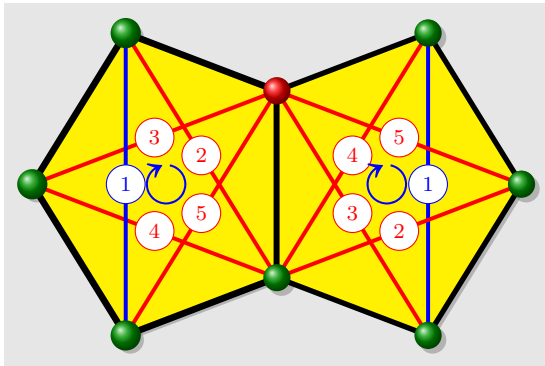


FIGURE B.5 – Permutation des 5 cubes, pour une rotation du dodécaèdre selon des faces.

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). ■

B.4 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 4.9, 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 7^e congrès international de mathématiques, qui a eu lieu en 1924 à Toronto, le mathématicien français **Elie Cartan** a 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.

B.5 Le groupe $SL_2(\mathbb{Z})$

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

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

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

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

Comme $T = S^3(ST)$, le groupe $SL_2(\mathbb{Z})$ est aussi engendré par les deux matrices S et ST .

On observe que

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

On peut exploiter ceci, et la division euclidienne dans \mathbb{Z} , pour déterminer comment écrire toute matrice de $\text{SL}_2(\mathbb{Z})$ 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 suivant⁷, en faisant agir le groupe sur lui-même par multiplication à gauche. Si $c \neq 0$ et $|a| \geq |c|$, appliquant la division euclidienne de a par c , on trouve q et r tels que $a = qc + r$, avec $|c| > r \geq 0$. Alors, on observe que

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

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

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

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

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

Action de $\text{SL}_2(\mathbb{Z})$ 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 dont la partie imaginaire est positive :

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

Pour chaque matrice dans $\text{SL}_2(\mathbb{Z})$, on a une transformation, dite de **Möbius**⁸, du plan hyperbolique, qui correspond à

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az + b}{cz + d}. \tag{B.4}$$

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

8. **August Ferdinand Möbius** (1790-1868). Voir le vidéo [expliquant les transformations de Möbius](#).

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 $SL_2(\mathbb{Z})$ sur \mathbf{H} , puisqu'on vérifie aussi par calcul direct que $A \cdot z$ est dans \mathbf{H} , pour

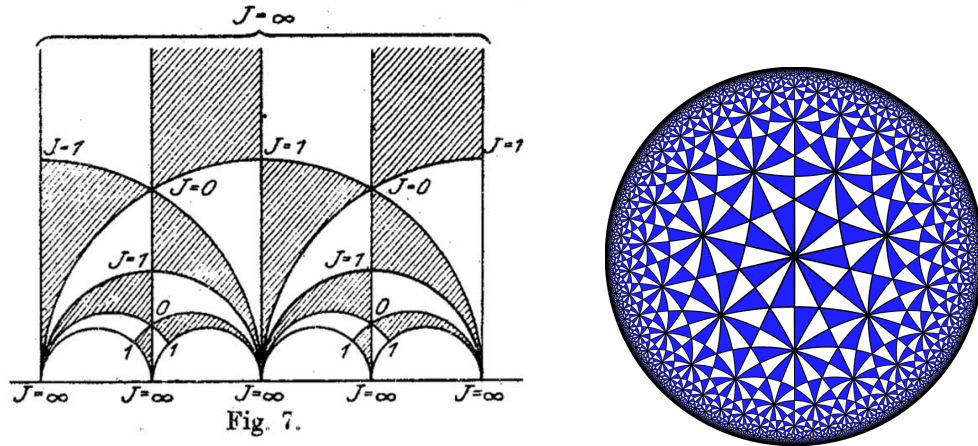


FIGURE B.6 – SL_2 -pavage de Klein du plan hyperbolique, et sa version circulaire.

tout $A \in SL_2(\mathbb{Z})$. On remarque, pour A dans $SL_2(\mathbb{Z})$, 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 **groupe modulaire**. Les transformations qui correspondent aux générateurs S et T sont respectivement

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

et ces transformations engendrent toutes celles qui correspondent à (B.4). Chaque orbite de cette action contient un et un seul élément dans la région

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

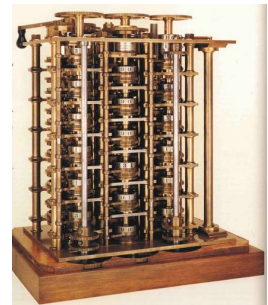
et le plan \mathbf{H} se pave avec des copies de cette région selon l'action de $\mathrm{SL}_2(\mathbb{Z})$, comme l'illustre la Figure B.6 d'ue à Klein⁹, dont il attribue l'idée à Dedekind¹⁰.

9. *Über die Transformation der elliptischen Funktionen und die Auflösung der Gleichungen fünften Grades*, *Mathematische Annalen*, 1878.

10. **Julius Wilhelm Richard Dedekind** (1831-1916).

Annexe C

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'interaction 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, primitivité, 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,%);
< (1, 2, 4, 6, 8, 7, 5, 3) >
< (1, 2, 5, 3)(4, 6, 8, 7), (1, 4)(2, 6)(3, 7)(5, 8) >
< (1, 2)(3, 7)(4, 6)(5, 8), (1, 3)(2, 5)(4, 8)(6, 7), (1, 4)(2, 6)(3, 8)(5, 7) >
< (1, 2, 6, 3)(4, 8, 5, 7), (1, 4, 6, 5)(2, 7, 3, 8), (1, 6)(2, 3)(4, 5)(7, 8) >
< (1, 2)(3, 5)(4, 6)(7, 8), (1, 3)(2, 5)(4, 7)(6, 8), (1, 4)(2, 6)(3, 7)(5, 8) >

```

Pour les groupes de permutations, comme le groupe du cube de Rubic :

```

> RubiksCubeGroup();
G := < (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) >

```

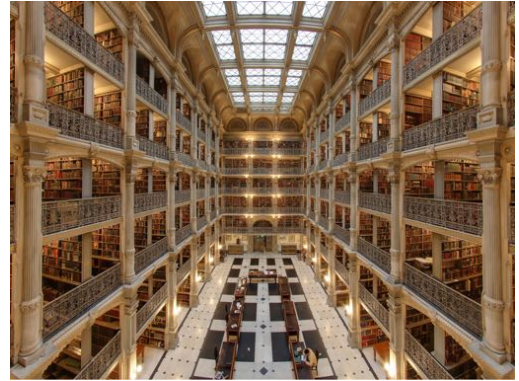
on peut calculer le stabilisateur et l'orbites d'éléments. Le groupe général linéaire, sur un corps fini à q éléments, correspond à $GL(n, q)$. Son ordre dépend de q de manière polynomiale, et on obtient son ordre comme suit :

```

> GroupOrder(GL(3, q));
(q6 - 1) (q6 - q) (q6 - q2) (q6 - q3) (q6 - q4) (q6 - q5)

```

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 réédition 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 Pölya, 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://groupeexplorer.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 1^{re} année, 2^e 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, \omicron :	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

- G -ensemble, 104
- p -groupe, 123
- Abel, Niels H., 13
- action
 - ensemble d'orbites, E/G , 107
 - fidèle, 106
 - fonctions
 - composition à droite, 112
 - composition à gauche, 112
 - conjugaison, 112
 - isomorphisme, 113
 - linéaire, 151
 - isomorphisme, 151
 - somme, 151
 - morphisme, 113
 - noyau, 106
 - orbite, 107
 - par conjugaison, 105, 108
 - sous-ensemble invariant, 106
 - sous-ensemble stable, 106
 - transitive, 107
 - triviale, 107
- action de groupe
 - continue, 121
 - sur un ensemble, 104
- alphabet, 25, 56, 89
- alterné, groupe A_n , 64
- automorphisme
 - intérieur, 72
- bijection, 144
- Burnside, William, 115
- Cantor, Georg, 139
- Cartan, Elie, 161
- Cauchy, Augustin Louis, 115
- Cayley, Arthur, 32, 69
- centralisateur, 108
- centralisateur, $C(H)$, 108
- centre, $Z(G)$, 21
- classe d'équivalence, 145
- commutateur, 93, 99
- composante primaire, 131
- concatenation, 57
- congruence
 - à droite, 22
 - à gauche, 22
- congruence modulo un sous-groupe
 - classe à gauche, 22
- conjugaison, 71, 105
- Coxeter, H.S.M., 40
- cryptographie RSA, 42
- Dedekind, Julius Wilhelm Richard, 164
- dense, 55
- diédral, D_m , 38
- Dirichlet, Johann, 143
- ensemble
 - \emptyset , 140
 - \mathbb{C} , 140
 - \subseteq , 140
 - de relations, 112
 - différence, 141

- élément, 139
- ensemble fini, 140
- ensemble vide, 140
- intersection, 142
- \mathbb{N} , 140
- $\mathcal{P}(E)$, 141
- paire, 140
- partition d'ensemble, 143
- produit cartésien, 141
- \mathbb{Q} , 140
- \mathbb{R} , 140
- réunion, 142
- singleton, 140
- sous-ensemble, 140
- union, 142
- union disjointe, 142
- \mathbb{Z} , 140
- ensemble d'orbites, E/G , 107
- ensemble quotient, 145
- ensemble quotient, G/H , 22, 104
- espace homogène, 161
- Euler, Leonhard, 42
- Fermat, Pierre, 42
- fixe, 108
- fonction, 143
 - action à droite, 112
 - action à gauche, 112
 - bien définie, 147
 - bijection, 16
 - composition, 16, 144
 - continue, 56
 - ensemble de, 16
 - identité, 16
 - injective, 144
 - inverse, 144
 - permutation, 16
 - restriction, 144
 - surjective, 144
- fonction d'Euler, $\varphi(x)$, 46
- Frobenius, Ferdinand Georg, 115
- générateur, 39
- Galileo, Galilei, 103
- Gauss, Carl Friedrich, 42
- groupe, 13
 - p -groupe, 123
 - p -groupe, 132
 - abélien, 13
 - somme directe, 131
 - action, 104
 - alterné, A_n , 64
 - centre, $Z(G)$, 21
 - commutatif, 13
 - cyclique, 28, 88
 - indécomposable, 136
 - de Coxeter, 100
 - des automorphismes intérieur, $\text{Int}(G)$, 72
 - diédral, D_m , 38
 - endomorphisme, 59
 - fini, 13
 - formule de l'indice, 50
 - général linéaire, $\text{GL}(V)$, 15
 - général linéaire, $\text{GL}_n(\mathbb{R})$, 11
 - générateurs, 25
 - groupe quotient, G/N , 84
 - groupe symétrique, 16
 - hyperoctaédral, B_n , 73
 - indice d'un sous-groupe, 24
 - isomorphe, 61
 - libre, 90
 - monogène, 26, 88
 - monstre, 28
 - morphisme de groupes, 59
 - ordre, 13
 - ordre d'un élément, 28
 - orthogonal, $O(n)$, 49
 - primaire, 132
 - résoluble, 99
 - simple, 70

- sous-groupe, 20
- sous-groupe de Sylow, 124
- sous-groupe engendré, 25
- sous-groupe propre, 20
- spécial linéaire, SL_n , 15
- spécial orthogonal, $SO(n)$, 49
- symétrique, 31
- symétrique, S_E et S_n , 16
- table de multiplication, 17
- topologique, 56
- groupe symétrique
 - longueur, 32
- homéomorphisme, 56
- homothéties, 111
- hyperoctaédral
 - groupe, 73
- hyperoctaèdre, HO_n , 74
- inclusion, 140
- indécidable, 93
- indice
 - d'un sous-groupe, $[G : H]$, 24
 - fini, 24
- invariant, 106
- involutions, 28
- isomorphisme, 113
 - deuxième théorème d', 89
 - premier théorème d', 87
 - troisième théorème d', 89
- jeu de taquin, 101
- Klein, Felix, 16
- Lagrange, Joseph Louis, 104
- lettre, 56
- libre, groupe, 90
- Lie, Sophus, 15
- loi de composition
 - élément inversible, 10
 - élément neutre, 10
 - associative, 8
 - commutative, 8
 - héréditaire, 9
 - hérite, 9
 - restriction, 9
 - sous-ensemble stable, 9
- loi de composition interne, 8
- magma, 8
 - sous-magma, 9
- Möbius, August Ferdinand, 162
- monoïde, 10
 - libre, 57
 - sous-monoïde, 10
- monoïdes
 - notation additive, 11
 - notation multiplicative, 11
- monstre, 28
- morphisme
 - épimorphisme, 63
 - automorphisme, 61
 - intérieur, 71
 - factorisation, 87
 - isomorphisme, 61
 - monomorphisme, 63
 - morphisme produit, 66
 - noyau, $\ker(\theta)$, 64
 - trivial, 59
- mot, 25, 56, 89
 - longueur, 56
 - vide, 57
- Newton, Sir Issac, 153
- nombre
 - addition, 14
 - complexe
 - racines de l'unité, 88
 - multiplication, 14
- normalisateur, $N(H)$, 109

- Novikov, Petr, 93
- orbite, $\text{Orb}(x)$, 107
- partage
 - notation $\mu \vdash n$, 120
 - part, 120
- partage d'un entier, 107
- permutation
 - circulaire, 36
 - cycle, 35
 - longueur, 35
 - paire, 64
 - signe, $\varepsilon(\sigma)$, 35
 - transposition, 36
- point fixe, $\text{fix}_g(E)$, 115
- Polya, George, 117
- polynôme
 - invariant, 153
- présentation, 39
- présentation de groupe, 92
 - générateurs, 89
 - relations, 92
- problème du mot, 93
- produit cartésien, 141
- produit direct, 19
 - externe, 19
 - inclusion, 67
 - interne
 - decomposition, 68
 - facteurs, 68
 - produit interne de plusieurs sous-groupes, 80
 - projection, 67
 - propriété universelle, 67
- produit direct interne, 68
- produit semi-direct, 72
- produit semi-direct interne, 71
- projection canonique, 84
- quotient de groupes
 - propriété universelle, 87
- réflexion, 39
- Redfield, John Howard, 117
- relation, 39
 - réflexive, 144
 - symétrique, 144
 - transitive, 144
- relation d'équivalence, 144
- représentation linéaire, 151
- représentation linéaire de groupe, 106
- rotation, 110
- Russell, Bertrand, 140
- Schutzenberger, Marcel Paul, 102
- sous-groupe
 - dérivé, 99
 - normal, 109
 - normal, $H \triangleleft G$, 70
 - normal, $N \triangleleft G$, 84
 - ordre, 20
 - sous-groupe trivial, 25
- sous-groupes de S_n
 - nombre de, 114
 - nombre de classes de conjugaison, 114
- stabilisateur, $\text{Stab}(x)$, 108
- stable, 106
- Sylow
 - théorèmes de, 124
- Sylow, Ludwig, 123
- théorème
 - Cauchy, 119
 - d'isomorphisme, 87
 - de Cayley, 69
 - de Lagrange, 24
 - de Wilson, 55
- topologie, 56
- transformation de Möbius, 162
- transitive, action, 107
- translation
 - du plan, 110

translation à gauche, [104](#)

Wilson, John, [55](#)

Young, Alfred, [102](#)