# INTRODUCTION À LA THÉORIE DES GROUPES
# MAT 2600

ABRAHAM BROER

*Date*: 31 août 2017.

## Table des matières


0. Préambule : petit cours d'arithmétique 4
   - 0.1. Introduction 4
   - 0.2. Un rappel de définitions 4
   - 0.3. Division avec reste 6
   - 0.4. Le pgcd 7
   - 0.5. Factorisation unique 8
   - 0.6. Relations d'équivalence 9
   - 0.7. Les rationnels 10
   - 0.8. Congruence modulo $n$ 11
   - 0.9. Nombres réels 13
   - 0.10. Nombres $p$-adiques 13

1. Définitions et notions élémentaires 14
   - 1.1. Introduction 14
   - 1.2. Définitions 15
   - 1.3. Notation 19
   - 1.4. Homomorphisme de groupes 20

2. Permutations et groupe symétrique 23
   - 2.1. Définition du groupe $S_n$ 23
   - 2.2. Matrices de permutation 26

3. Corps et groupes linéaires 29

4. Sous-groupes et théorème de Lagrange 34
   - 4.1. Sous-groupes 34
   - 4.2. Sous-groupe engendré par un sous-ensemble 38
   - 4.3. Sous-groupe dérivé 40
   - 4.4. Théorème de Cayley 42
   - 4.5. Théorème de Lagrange 43
   - 4.6. Le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ 46

5. Les théorèmes d'isomorphisme 48
   - 5.1. Sous-groupes normaux 48
   - 5.2. Simplicité 54
   - 5.3. Le théorème fondamental des homomorphismes 55
   - 5.4. Le premier théorème d'isomorphisme 57
   - 5.5. Le deuxième théorème d'isomorphisme 59
   - 5.6. Le troisième théorème d'isomorphisme 61
   - 5.7. Morphismes vers un groupe abélien 62
   - 5.8. Le théorème de correspondance 62
   - 5.9. Le théorème de Jordan–Hölder 63

6. Action d'un groupe sur un ensemble 68
   - 6.1. Actions de groupe 68
   - 6.2. Théorème fondamental des actions 71
   - 6.3. L'équation des classes 75
   - 6.4. Existence de points fixes 76

6.5. Le théorème de Cayley généralisé 76
6.6. Action d'un groupe $G$ sur lui-même 77

7. Applications dans la théorie des groupes 79
7.1. Un critère suffisant pour la normalité d'un sous-groupe 79
7.2. Action par conjugaison 79
7.3. Théorème de Cauchy 80
7.4. Produits semi-direct 83

8. Théorèmes de Sylow 86
8.1. Première preuve du théorème de Sylow 87
8.2. Une autre preuve du théorème de Sylow 88

Références 91

Index 92

## 0. Préambule : petit cours d'arithmétique

0.1. **Introduction.** Nous allons rappeler quelques propriétés élémentaires et bien connues des nombres entiers, rencontrées déjà dans le cours MAT1500. Par exemple, que chaque nombre entier est un produit de nombres premiers et ce produit est unique à permutation près. Comme point de départ nous prenons l'idée qu'on sait compter !

Les nombres entiers se trouvent vraiment à la base de toutes les mathématiques, leur *existence* en est même un de ses axiomes ! On suppose que les nombres entiers existent. Mais après, en acceptant les nombres naturels, on *construit* les nombres entiers négatifs, les fractions, les nombres réels et les nombres complexes. [1] Nous rappelons des définitions des fractions et des nombres réels.

0.2. **Un rappel de définitions.** Essayez avant tout de vous rappeler ou de vous imaginer comment les nombres ou entiers naturels peuvent être caractérisés exactement (peut-être à l'école primaire ?) et puis l'addition et la multiplication.

L'idée est qu'il est possible de compter aussi loin qu'on veut à partir de 1 :

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, \ldots$$

Les nombres qu'on obtient ainsi sont les nombres naturels. Donc implicitement, chaque nombre naturel a un unique successeur et chaque nombre sauf 1 a un unique nombre naturel comme prédécesseur.

*Il existe un unique ensemble* $\mathbb{N}$ *(l'ensemble des nombres naturels) avec un élément spécial noté* 1*, dont chaque élément a un unique* successeur *et dont chaque élément sauf* 1 *a un* unique prédécesseur*, et aucun sous-ensemble propre et contenant* 1 *a la même propriété.* En particulier, si $S \subseteq \mathbb{N}$ est un sous-ensemble avec les deux propriétés que $1 \in S$ et que, lorsque $s$ est un élément de $S$ son successeur l'est également, alors on a nécessairement que $S = \mathbb{N}$.

Nous allons accepter l'existence de $\mathbb{N}$. En conséquence nous allons aussi accepter le principe d'induction mathématique ! Supposons que $P(n)$ est une proposition logique qui dépend du nombre naturel $n \in \mathbb{N}$. Supposons que $P(1)$ est vraie et que pour chaque $n \in \mathbb{N}$ la proposition $P(n)$ implique $P(n')$, où $n'$ est le successeur de $n$. Alors, parce que $P(1)$ implique $P(2)$ et $P(1)$ est vraie, on a que $P(2)$ est aussi vraie. Donc $P(3)$ est vraie. Donc $P(4)$ est vraie, et cetera. Donc $P(n)$ est vraie pour chaque $n \in \mathbb{N}$, parce qu'on peut compter jusqu'à $n$. De façon analogue pour les *définitions* inductives.

Pour donner la définition d'addition sur $\mathbb{N}$ correctement, il faut nécessairement utiliser l'induction (c'est-à-dire une propriété définissant l'ensemble des nombres naturels !).

Soit $n \in \mathbb{N}$ on va définir $n + m \in \mathbb{N}$ par induction sur $m$. Si $m = 1$ nous *définissons* $n + 1$ comme le successeur (unique) de $n$. Supposons que $n + m$ a été défini. Alors on *définit* :

$$n + (m + 1) := (n + m) + 1$$

(c'est-à-dire, le successeur de $n+m$). Alors par le principe d'induction on a maintenant défini $n+m$ pour chaque $n, m \in \mathbb{N}$.

1. L. Kronecker (1823–1891, un mathématicien allemand) a dit que Dieu a créé les nombres entiers et tout le reste est le travail d'homme. Voir le bouquin très lisible : Eric Temple Bell, Men of Mathematics, New York, Simon and Schuster, 1986. La bibliothèque a une version française.

Nous pouvons voir (comme pourrait le voir un enfant de 7 ans) que

$$a + b = b + a \text{ et } (a + b) + c = a + (b + c) \ :$$

*Démonstration.* Soient $a, b \in \mathbb{N}$. Nous allons montrer par induction sur $n$ que $(a+b)+n = a+(b+n)$. Si $n = 1$, alors $(a+b)+1 = a+(b+1)$ par définition de $+$. Supposons maintenant que $(a+b)+n = a + (b + n)$. Alors

$$\begin{aligned}
(a + b) + (n + 1) &= ((a + b) + n) + 1 \quad \text{(par définition de } +) \\
&= (a + (b + n)) + 1 \quad \text{(par hypothèse d'induction)} \\
&= a + ((b + n) + 1) \quad \text{(par définition de } +) \\
&= a + (b + (n + 1)) \quad \text{(par définition de } +).
\end{aligned}$$

Donc par induction nous avons montré la règle d'associativité.

Pour montrer la commutativité, nous commençons par montrer que $a + 1 = 1 + a$ par induction sur $a$. Si $a = 1$ on a la tautologie $1 + 1 = 1 + 1$. Supposons que $a + 1 = 1 + a$. Alors

$$(a + 1) + 1 = (1 + a) + 1 = 1 + (a + 1)$$

et on conclut par induction.

Fixons $a$. Nous allons montrer par induction sur $n$ que $a + n = n + a$. On vient de montrer le cas où $n = 1$. Supposons maintenant que $a + n = n + a$, alors on a en utilisant l'associativité

$$a + (n + 1) = (a + n) + 1 = (n + a) + 1 = 1 + (n + a) = (1 + n) + a = (n + 1) + a.$$

On conclut par induction. □

Rappelons la définition de « $a$ est plus petit que $b$ », pour les nombres naturels $a$ et $b$. On a $n < m$ (ou $m > n$) si et seulement si il existe un $a \in \mathbb{N}$ tel que $m = n + a$. Si $n < m$ et $m < k$ alors $n < k$ (pourquoi ?). Pour deux nombres naturels $a$ et $b$ il existe trois alternatives : $a < b$ ou $b < a$ ou $a = b$ (pourquoi ?). On écrit $a \leq b$ si $a = b$ ou si $a < b$.

*Exercice* 0.1. Montrer que chaque sous-ensemble non-vide $S$ de $\mathbb{N}$ *contient* un *unique* élément qui est plus petit que tous les autres éléments de $S$.

La définition du produit de deux nombres naturels ? Soit $n, m \in \mathbb{N}$. On définit $n \cdot m \in \mathbb{N}$ par induction sur $n$. Si $n = 1$ on définit $1 \cdot m := m$. Supposons que $n \cdot m$ ait été défini. Alors on pose $(n + 1) \cdot m := (n \cdot m) + m$.

Pouvez-vous voir pourquoi

$$a \cdot b = b \cdot a, \ (a \cdot b) \cdot c = a \cdot (b \cdot c) \ ?$$

*Exercice* 0.2. Montrer la règle de distributivité :

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

pour chaque $a, b, c \in \mathbb{N}$.

Puis, à partir de $\mathbb{N}$ on *construit* par induction l'ensemble des nombres entiers

$$\mathbb{Z} := \{\ldots, -12, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots\}$$

en ajoutant à l'ensemble $\mathbb{N}$ un nombre appelé 0 premièrement (donc 0 n'était pas encore dans $\mathbb{N}$) et puis successivement pour chaque nombre naturel $n$ un nouveau nombre appelé $-n$ (alors $-n$ n'était pas encore dans $\{-(n-1), -(n-2), \ldots, -1, 0, 1, 2, \ldots\}$). On obtiendra une extension unique des opérations $+$ et $\cdot$ tels que

$$n + (-n) = (-n) + n = 0,\ (-1) \cdot n = (-n),\ 0 + n = n + 0 = n,$$

pour chaque $n \in \mathbb{N}$. Les règles d'associativité, de commutativité et de distributivité restent vraies. On pose $-(-n) := n$ et $-0 := 0$, pour $n \in \mathbb{N}$. Et $a - b := a + (-b)$. Si $n \in \mathbb{N}$ on pose $|n| = |(-n)| = n$ et $|0| = 0$. On a $|a|\,|b| = |ab|$ et $|a + b| \leq |a| + |b|$.

0.3. **Division avec reste.** En général, on ne peut pas diviser un nombre entier par un autre nombre entier et obtenir un nombre entier. Mais on peut diviser avec reste, comme on a vu dans MAT1500. Par exemple, si on divise 3599 par 112 on aura un reste :

$$3599 = 32 \cdot 112 + 15.$$

**Théorème 0.1** (Division avec reste)**.** *Soient $a, b \in \mathbb{Z}$, où $b \neq 0$. Alors il existe deux nombres entiers uniques, $q, r$ tel que*

$$a = qb + r \text{ et } 0 \leq r < |b|.$$

*Démonstration.* Premièrement nous allons montrer que si $a \geq 0$ et $b > 0$, alors il existe $q$ et $r$ tels que $a = qb + r$ et $0 \leq r < b$. Nous procédons par induction sur $a$. Si $a = 0$ alors $a = 0 = 0 \cdot b + 0$. Soit $0 < a$. Supposons par induction qu'il existe $q'$ et $r'$ tels que $a = q'b + r'$ et $0 \leq r' < b$. Il y a deux cas possible. (1) Si $r' + 1 = b$. Alors $a + 1 = q'b + r' + 1 = q'b + b = (q' + 1) \cdot b + 0$. (2) Si $r' + 1 < b$. Alors $a + 1 = q' \cdot b + (r' + 1)$. Donc il existe $q$ et $r$ tels que $a + 1 = qb + r$.

D'une manière analogue on montre le cas où $a \leq 0$ et $b > 0$.

Supposons maintenant $b < 0$. Alors $-b > 0$ et nous venons de montrer qu'ils existent $q$ et $r$ tels que $a = q(-b) + r$ et $0 \leq r < |b|$. Donc $a = (-q)b + r$.

Il reste à montrer l'unicité. Supposons que $a = qb + r$, $a = q'b + r'$, $0 \leq r < |b|$ et $0 \leq r' < |b|$. Alors $0 \leq |r - r'| < |b|$ et $|r - r'| = |q' - q| \cdot |b|$. Donc $0 \leq |q' - q| \cdot |b| < |b|$, et $0 \leq |q' - q| < 1$. Donc le nombre entier $|q' - q|$ est 0, d'où $q' = q$. Aussi $r = a - qb = a - q'b = r'$. $\square$

On dit que « $b$ divise $a$ », ou $b \mid a$, s'il existe $q \in \mathbb{Z}$ tel que $a = qb$ (alors un tel $q$ est unique). Voici des propriétés élémentaires de la relation « être divisible » :

$$c \mid b \wedge b \mid a \Rightarrow c \mid a$$

$$b \mid a \wedge b \mid a' \Rightarrow b \mid (na + ma')\ \forall n, m \in \mathbb{Z}$$

$$\forall b :\ b \mid 0 \ \text{ et } \forall a :\ 1 \mid a$$

$$b \mid a \Leftrightarrow |b| \mid |a|$$

$$b \mid a \wedge (a \neq 0) \ \Rightarrow |b| \leq |a|.$$

0.4. **Le pgcd.** Si $(a, b) \neq (0, 0)$, on définit le $\mathrm{pgcd}(a, b)$ comme le plus grand commun diviseur de $a$ et $b$, ou

$$\mathrm{pgcd}(a, b) := \mathrm{Max}\{d; d \mid a \wedge d \mid b\}.$$

Et on définit $\mathrm{pgcd}(0, 0) := 0$. On a $\mathrm{pgcd}(n, 0) = |n|$.

**Lemme 0.1.** *Soient $a, b, q, r \in \mathbb{Z}, b \neq 0$, tels que $a = qb + r$. Alors*

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r).$$

*Démonstration.* Soit $d \in \mathbb{N}$ tel que $d \mid a$ et $d \mid b$ ; donc $d \mid (a - qb) = r$. Si $d \in \mathbb{N}$ tel que $d \mid b$ et $d \mid r$, alors $d \mid (qb + r) = a$. Donc l'ensemble des diviseurs communs de $a$ et $b$ est égal à l'ensemble des diviseurs communs de $b$ et $r$. Donc par définition $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$. □

Le lemme donne une suggestion pour calculer le pgcd itérativement ; c'est l'algorithme d'Euclide. Nous donnons seulement un exemple.

$$\begin{aligned}
\mathrm{pgcd}(1057, 315) &= \mathrm{pgcd}(315, 112) \quad (\text{parce que } 1057 = 3 \cdot 315 + 112) \\
&= \mathrm{pgcd}(112, 91) \quad (\text{parce que } 315 = 2 \cdot 112 + 91) \\
&= \mathrm{pgcd}(91, 21) \quad (\text{parce que } 112 = 1 \cdot 91 + 21) \\
&= \mathrm{pgcd}(21, 7) \quad (\text{parce que } 91 = 4 \cdot 21 + 7) \\
&= \mathrm{pgcd}(7, 0) \quad (\text{parce que } 21 = 3 \cdot 7 + 0) \\
&= 7.
\end{aligned}$$

**Théorème 0.2.** *Soient $a, b \in \mathbb{Z}$. Alors il existe $x, y \in \mathbb{Z}$ tel que*

$$xa + yb = \mathrm{pgcd}(a, b).$$

*Démonstration.* Nous pouvons supposer que $a \neq 0$, parce que sinon $\mathrm{pgcd}(a, b) = |b| = 0 \cdot a + (\pm 1)b$. Soit $S \subset \mathbb{N}$ le sous-ensemble défini par

$$S := \{n \in \mathbb{N}; \exists x \in \mathbb{Z}, \exists y \in \mathbb{Z} : \ xa + yb = n\}$$

On a $|a| \in S$, donc $S$ n'est pas vide. Soit $s$ le plus petit élément de $S$. Donc $s \leq |a|$ et il existe $x, y$ tels que $xa + yb = s$. Soit $m = x'a + y'b \in S$ quelconque. Par division avec reste, il existe $q, r$ tels que $m = qs + r$ et $0 \leq r < s$, et

$$r = m - qs = (x'a + y'b) - q(xa + yb) = (x' - qx)a + (y' - qy)b.$$

Si $r > 0$, on aurait $r \in S$ et $r < s$, une contradiction avec le choix de $s$. Donc $r = 0$ et $s \mid m$. En particulier, $s$ divise $|a|$ et $|b|$ ($|a| \in S$, et $|b| \in S$, si $b \neq 0$) et alors aussi $a$ et $b$. Donc $s$ est un diviseur commun de $a$ et $b$ et $s \leq \mathrm{pgcd}(a, b)$.

Par contre, $\mathrm{pgcd}(a, b)$ divise $a$ et $b$, donc aussi $xa + yb = s$ et nécessairement $\mathrm{pgcd}(a, b) \leq s$. Donc $s = \mathrm{pgcd}(a, b) = xa + yb$. □

On peut aussi donner un algorithme (de Bézout) pour trouver $x$ et $y$. Un exemple suffit peut-être.

*Exemple* 0.1. Nous calculons des $x$ et $y$ tels que $x \cdot 1057 + y \cdot 315 = \text{pgcd}(1057, 315)$. On commence par deux équations triviales et puis on utilise la division avec reste :

$$\begin{aligned}
1 \cdot 1057 + 0 \cdot 315 &= 1057 \\
0 \cdot 1057 + 1 \cdot 315 &= 315 \\
1 \cdot 1057 + (-3) \cdot 315 &= 112 \quad (\text{parce que } 112 = 1057 - 3 \cdot 315) \\
(-2) \cdot 1057 + (7) \cdot 315 &= 91 \quad (\text{parce que } 91 = 315 - 2 \cdot 112) \\
3 \cdot 1057 + (-10) \cdot 315 &= 21 \quad (\text{parce que } 21 = 112 - 1 \cdot 91) \\
(-14) \cdot 1057 + (47) \cdot 315 &= 7 \quad (\text{parce que } 7 = 91 - 4 \cdot 21)
\end{aligned}$$

Donc $x = -14$ et $y = 47$. Les $x$ et $y$ ne sont pas uniques, parce que on a aussi

$$(-14 + 315) \cdot 1057 + (47 - 1057) \cdot 315 = 301 \cdot 1057 - 1010 \cdot 315 = 7.$$

*Exercice* 0.3. Calculer $\text{pgcd}(987654321, 123456789)$. Trouver $a, b$ tels que $-14a + 47b = \text{pgcd}(14, 47)$.

**Corollaire 0.1.** *Soient $a, b, d \in \mathbb{Z}$ tels que $d \mid a$ et $d \mid b$, et donc $d \mid \text{pgcd}(a, b)$. Si $c = xa + yb$, pour certains $x, y \in \mathbb{Z}$, alors $\text{pgcd}(a, b) \mid c$.*

*Démonstration.* Le nombre $d$ divise $xa + yb$ pour chaque $x, y$, donc en particulier divise le $\text{pgcd}(a, b)$ (par le théorème). L'autre proposition est montrée dans la preuve du théorème. □

Un *nombre premier* est un nombre naturel $p > 1$ ayant seulement 1 et $p$ comme diviseurs dans $\mathbb{N}$. Deux nombres sont relativement premiers si leur pgcd est égal à 1.

*Exercice* 0.4. Montrer que $a$ et $b$ sont relativement premiers si et seulement si il existe des entiers $x$ et $y$ tels que $xa + yb = 1$.

**Corollaire 0.2.** *Soit $p$ un nombre premier. Si $p \mid a_1 a_2 \ldots a_n$, alors il existe au moins un $i$ tel que $p \mid a_i$.*

*Démonstration.* Par induction sur $n$. Si $n = 1$, il n'y a rien à montrer. Supposons que si $p$ divise un produit de moins que $n$ facteurs, alors il divise au moins un des facteurs. Supposons que $p \mid a_1 a_2 \cdots a_n$ et que $p$ ne divise pas $a_n$. Alors $\text{pgcd}(p, a_n) = 1$, donc il existe $x, y$ tels que $xp + ya_n = 1$. Donc après multiplication par $(a_1 a_2 \cdots a_{n-1})$ on obtient que

$$(a_1 a_2 \cdots a_{n-1} x)p + y(a_1 a_2 \cdots a_{n-1} a_n) = a_1 a_2 \cdots a_{n-1}$$

est divisible par $p$, donc par l'hypothèse d'induction $p$ divise l'un des $a_i$. □

### 0.5. **Factorisation unique.**

**Théorème 0.3.** *Soit $1 < n$. Alors il existe un nombre naturel $m$ et $m$ nombres premiers $p_1, \ldots, p_m$ tels que $n = p_1 p_2 \ldots p_m$. Le nombre $m$ est unique et les nombres premiers sont uniques à une permutation près des facteurs $p_i$.*

*Démonstration.* Nous allons montrer l'existence d'une telle décomposition par induction sur $n$. Si $n$ est premier, par exemple si $p = 2$, on prend $m = 1$ et $p_1 := n$. Sinon, ils existent $a, b \in \mathbb{N}$ tels que $n = ab$, $n > a > 1$, $n > b > 1$. Par l'hypothèse d'induction il existe $s, t$ et décompositions $a = q_1 \cdots q_s$ et $b = r_1 \cdots r_t$, où les $q_i$ et $r_j$ sont premiers. Donc $n = q_1 \cdots q_s r_1 \cdots r_t$ est un produit de $s + t$ nombres premiers.

Maintenant nous montrons l'unicité par induction sur $n$. Si $n$ est premier, c'est clair. Supposons que $n$ n'est pas premier et

$$n = p_1 \cdots p_m = q_1 \cdots q_s,$$

où les $p_i$ et $q_j$ sont premiers et $m \geq 1, s \geq 1$. $p_m$ divise $n$ et est premier, donc divise un des facteurs $q_i$. Possiblement après avoir permuté les facteurs, on peut supposer que ce facteur est $q_s$. Mais $q_s$ est aussi premier, donc $p_m = q_s$. Soit $n'$ tel que $n = n' p_m = n' q_s$. Alors

$$n' = p_1 \cdots p_{m-1} = q_1 \cdots q_{s-1},$$

et donc par induction $m - 1 = s - 1$ et (possiblement après permutation des $q_1, \ldots, q_{s-1}$) on a $p_i = q_i$ pour chaque $i$. Alors par induction nous avons montré l'unicité. □

*Exercice* 0.5. Le théorème ne dit pas si le nombre de nombres premiers différents est fini ou non. Montrer qu'il existe un nombre infini de nombres premiers.

0.6. **Relations d'équivalence.** Soit $X$ un ensemble. Une *relation* (binaire) sur $X$ est un sous-ensemble $R \subseteq X \times X$ du produit cartésien. On utilisera la notation

$$x \sim y :\iff (x, y) \in R.$$

On dit que c'est une *relation d'équivalence* si les trois propriétés suivantes sont satisfaites :

(1) $x \sim x$ pour chaque $x \in X$ (réflexivité) ;
(2) $x \sim y$ implique $y \sim x$ (symétrie) ;
(3) $x \sim y$ et $y \sim z$ implique $x \sim z$ (transitivité).

Si $\sim$ est une relation d'équivalence sur $X$ et $x \in X$ on écrit

$$\mathrm{Cl}(x) := \{y \in X; x \sim y\},$$

la *classe d'équivalence contenant* $x$. Une *classe d'équivalence* est un sous-ensemble de la forme $\mathrm{Cl}(x)$ pour un $x \in X$.

**Proposition 0.1.** *Soit $\sim$ une relation d'équivalence sur un ensemble $X$.*

*(i) On a $\mathrm{Cl}(x) = \mathrm{Cl}(y)$ si et seulement si $x \sim y$.*
*(ii) Supposons $\mathrm{Cl}$ et $\mathrm{Cl}'$ sont deux classes d'équivalence. Si $\mathrm{Cl} \neq \mathrm{Cl}'$, alors $\mathrm{Cl}$ et $\mathrm{Cl}'$ sont disjointes.*
*(ii) $X$ est la réunion disjointe de ses classes d'équivalence.*

*Démonstration.* (i) Si $\mathrm{Cl}(x) = \mathrm{Cl}(y)$, alors $x \in \mathrm{Cl}(x) = \mathrm{Cl}(y)$, donc $x \sim y$. Si $x \sim y$ et $z \in \mathrm{Cl}(x)$, alors $z \sim x$ et par la transitivité $z \sim y$, d'où $z \in \mathrm{Cl}(y)$. (ii) et (iii) suivent de (i). □

On écrit $X/\sim$ pour l'ensemble des classes d'équivalence et on a une application

$$\mathrm{Cl} : X \to X/\sim : x \mapsto \mathrm{Cl}(x).$$

Faites attention : une classe d'équivalence $C$ peut être vu comme un *élément* de $X/\sim$ ou comme un *sous-ensemble* de $X$. On a $x \sim y$ si et seulement si $\mathrm{Cl}(x) = \mathrm{Cl}(y)$.

*Exercice* 0.6. Lesquelles des relations binaires suivantes sont des relations d'équivalence ?
(i) $X =$ l'ensemble des êtres humains et $x \sim y$ si $x$ a la même mère biologique que $y$.
(ii) $X =$ l'ensemble des triangles du plan et $T_1 \sim T_2$ s'il existe une transformation de similitude amenant $T_1$ sur $T_2$.
(iii) $X = \mathbb{Q}$ et $x \sim y$ si et seulement si $x = y$.
(iv) $X = \mathbb{R}$ et $x \sim y$ si et seulement si il existe $q \in \mathbb{Q}$ tel que $x = y + q$.
(v) $X = \mathbb{R}^n \setminus \{0\}$ et $v \sim w$ si et seulement si il existe $r \in R$ tel que $rv = w$.
(vi) $X =$ l'ensemble des droites dans $\mathbb{R}^3$ et $d_1 \sim d_2$ s'il existe un plan $P$ tel que $d_1 \cup d_2 \in P$.
(vii) $X = \mathbb{R}$ et $\theta \sim \phi$ s'il existe un entier $m \in \mathbb{Z}$ tel que $\theta = \phi + 2\pi m$.
(viii) $X = S_n$ et $\sigma \sim \pi$ si et seulement si il existe $\rho \in S_n$ tel que $\rho\sigma\rho^{-1} = \pi$. (À faire lorsque le groupe symétrique $S_n$ sera vu.)

*Exercice* 0.7. Identifier l'ensemble $X/\sim$ des classes d'équivalence pour les sous-questions de l'exercice précédent définissant des relations d'équivalence.

*Exercice* 0.8. VRAI ou FAUX. Soit $X$ un ensemble et $\sim$ une relation d'équivalence sur $X$.
(i) Les éléments de $X/\sim$ sont des sous-ensembles de $X$ qui ont tous la même cardinalité.
(ii) Si la cardinalité de $X$ est infinie, alors les éléments de $X/\sim$ sont de cardinalité infinie.
(iii) L'ensemble vide $\emptyset$ peut être une des classes d'équivalence de $X/\sim$.
(iv) Sur tout $X$, il exite une relation $\sim$ telle que $X/\sim = \{X\}$.

0.7. **Les rationnels.** Maintenant on va rappeler comment on définit les fractions. Soit

$$X = \{(n, d) \in \mathbb{Z}^2; d \neq 0\},$$

avec la relation d'équivalence

$$(n, d) \sim (n', d') \iff nd' = n'd \quad \text{(une égalité dans } \mathbb{Z}).$$

Nous vérifions la transitivité. Si $(n, d) \sim (n', d')$ et $(n', d') \sim (n'', d'')$ alors $nd' = n'd$ et $n'd'' = n''d'$. Donc

$$(nd'' - n''d)d' = nd'd'' - n''dd' = nd'd'' - n'dd'' = nd'd'' - nd'd'' = 0,$$

et parce que $d' \neq 0$ il suit que $nd'' = n''d$, d'où $(n, d) \sim (n'', d'')$.

La classe d'équivalence de $(n, d)$ est appelé une *fraction*, et s'écrit comme d'habitude comme $\frac{n}{d}$ :

$$\frac{n}{d} := \mathrm{Cl}(n, d).$$

On a $\frac{n}{d} = \frac{n'}{d'}$ si et seulement si $\mathrm{Cl}(n, d) = \mathrm{Cl}(n', d')$ si et seulement si $nd' = n'd$. Maintenant

$$\mathbb{Q} := X/\sim = \{\frac{n}{d}; d \neq 0\}$$

est l'ensemble des fractions.

On définit l'addition et la multiplication sur $\mathbb{Q}$ par

$$\frac{n}{d} \cdot \frac{n'}{d'} := \frac{nn'}{dd'}; \qquad \frac{n}{d} + \frac{n'}{d'} := \frac{nd' + n'd}{dd'}.$$

Il y a encore une chose à faire ! Les formules sont données en termes de représentants de classes d'équivalence ; changer les représentants ne change pas les classes, mais change les formules. Pour que les définitions proposées soient acceptables (soit « bien définies »), il faut que le résultat ne dépende pas du choix des représentants. Vérifions par exemple que l'addition est *bien définie*. Supposons $\frac{n}{d} = \frac{r}{s}$ et $\frac{n'}{d'} = \frac{r'}{s'}$. Il faut vérifier si

$$\frac{nd' + n'd}{dd'} = \frac{rs' + r's}{ss'},$$

c'est-à-dire si

$$(nd' + n'd)ss' = (rs' + r's)dd'.$$

On a $ns = rd$ et $n's' = r'd'$ et donc on a en effet

$$(nd' + n'd)ss' = ns \cdot d's' + n's' \cdot ds = rd \cdot d's' + r'd' \cdot ds = (rs' + r's)dd'.$$

On considère $\mathbb{Z}$ comme un sous-ensemble par l'inclusion $\mathbb{Z} \to \mathbb{Q}; n \mapsto \frac{n}{1}$. Il y a une extension de l'ordre partiel : soit $\frac{n}{d}$ et $\frac{n'}{d'}$ deux fractions où on peut supposer que $d, d' \in \mathbb{N}$. On écrit

$$\frac{n}{d} \leq \frac{n'}{d'} \iff nd' \leq n'd$$

et $|\frac{n}{d}| := \frac{|n|}{|d|}$.

*Exercice* 0.9. (i) Soit la relation définie sur l'ensemble $\mathbb{Q}$ par $\frac{p}{q} \sim \frac{r}{s}$ si il existe un entier $n$ tel que $\frac{p}{q} = \frac{r}{s} + n$. Montrer que $\sim$ est une relation d'équivalence. On notera par $\widehat{\frac{p}{q}}$ la classe d'équivalence de $\frac{p}{q}$ et par $\mathbb{Q}/\mathbb{Z}$ l'ensemble de ces classes d'équivalence. Ainsi $\widehat{\frac{3}{4}} = \{\ldots, -\frac{5}{4}, -\frac{1}{4}, \frac{3}{4}, \frac{7}{4}, \frac{11}{4}, \ldots\}$.
(ii) On tente de définir deux opérations $\widehat{+}$ et $\widehat{\cdot}$ sur l'ensemble $\mathbb{Q}/\mathbb{Z}$ :

$$\widehat{\frac{p}{q}} \,\widehat{+}\, \widehat{\frac{r}{s}} = \widehat{\left(\frac{p}{q} + \frac{r}{s}\right)} \qquad \text{et} \qquad \widehat{\frac{p}{q}} \,\widehat{\cdot}\, \widehat{\frac{r}{s}} = \widehat{\left(\frac{p}{q} \cdot \frac{r}{s}\right)}.$$

Sont-elles « bien définies » ?

*Exercice* 0.10. (i) Soit $\sim$ la relation sur $\mathbb{N} \times \mathbb{N}$ donné par $(d, m) \sim (d', m')$ si $d + m' = d' + m$. Montrer que c'est une relation d'équivalence.
(ii) Montrer que l'ensemble $\mathbb{N} \times \mathbb{N}/\sim$ peut être identifié à l'ensemble des entiers $\mathbb{Z}$.
(iii) Proposer des définitions de $+$ et $\times$ sur l'ensemble $\mathbb{N} \times \mathbb{N}/\sim$ qui reproduisent les opérations usuelles sur $\mathbb{Z}$. Vérifier que ces définitions sont bien définies.

0.8. **Congruence modulo $n$.** Pour chaque entier $n$ on a une relation d'équivalence « $\cdot \equiv \cdot \bmod n$ » sur $\mathbb{Z}$. On écrit $a \equiv a' \bmod n$ et on dit que $a$ est *congruent à $a'$ modulo $n$* si $n \mid (a - a')$, ou si $a$ et $a'$ ont le même reste après division par $n$ :

$$a \equiv a' \bmod n \iff n \mid (a - a').$$

Pour $n$ fixé, ça donne une relation d'équivalence sur $\mathbb{Z}$, parce que

(1) $a \equiv a \bmod n$ (on a $n \mid (a - a)$) ;

(2) $a \equiv a' \bmod n \iff a' \equiv a \bmod n$ (on a $n \mid (a - a') \iff n \mid (a' - a)$) ;

(3) $a \equiv a' \bmod n$ et $a' \equiv a'' \bmod n \Rightarrow a \equiv a'' \bmod n$, (on a $n \mid (a - a')$ et $n \mid (a' - a'') \Rightarrow n \mid (a - a'')$.)

Écrivons $\overline{a} = \mathrm{Cl}(a)$ pour la classe d'équivalence de $a$ pour l'équivalence « $\cdot \equiv \cdot \bmod n$ », donc

$$\overline{a} := \{m \in \mathbb{Z};\ m \equiv a \bmod n\} = \{a + mn;\ m \in \mathbb{Z}\}.$$

Donc $\overline{a} = \overline{a'}$ si et seulement si $a \equiv a' \bmod n$.

On écrit $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv \bmod n$ pour l'ensemble des classes d'équivalence pour « $\cdot \equiv \cdot \bmod n$ ».

L'addition et la multiplication des classes d'équivalence sont définies par

$$\overline{a} + \overline{a'} := \overline{a + a'}; \qquad \overline{a} \cdot \overline{a'} := \overline{aa'}.$$

*Exercice* 0.11. (i) Montrer que $+$ et $\cdot$ sont bien définies et que les règles de commutativité, associativité et distributivité sont satisfaites.

(ii) Montrer que si $n \neq 0$, alors $\mathbb{Z}/n\mathbb{Z}$ est d'ordre fini $|n|$.

*Démonstration.* Par exemple la règle de distributivité

$$\begin{aligned}
\overline{a_1} \cdot (\overline{a_2} + \overline{a_3}) &= \overline{a_1} \cdot \overline{(a_2 + a_3)} \ \text{(par la définition de } +) \\
&= \overline{a_1 \cdot (a_2 + a_3)} \ \text{(par la définition de } \cdot) \\
&= \overline{a_1 a_2 + a_1 a_3} \ \text{(par la distributivité dans } \mathbb{Z}) \\
&= \overline{a_1 a_2} + \overline{a_1 a_3} \ \text{(par la définition de } +) \\
&= \overline{a_1} \cdot \overline{a_2} + \overline{a_1} \cdot \overline{a_3} \ \text{(par la définition de } \cdot)
\end{aligned}$$

□

Par exemple, si $n = 2$, alors $\mathbb{Z}/2\mathbb{Z}$ a deux éléments $\overline{0} =$ « pair » et $\overline{1} =$ « impair ». On a

$$\overline{0} + \overline{0} = \overline{0},\ \overline{0} + \overline{1} = \overline{1} + \overline{0} = \overline{1},\ \overline{1} + \overline{1} = \overline{2} = \overline{0}; \qquad \overline{0} \cdot \overline{0} = \overline{0},\ \overline{0} \cdot \overline{1} = \overline{1} \cdot \overline{0} = \overline{0},\ \overline{1} \cdot \overline{1} = \overline{1}.$$

Rappelons que deux nombres sont relativement premiers si leur pgcd est égal à 1.

**Proposition 0.2.** *$a$ et $n$ sont relativement premiers si et seulement si il existe un $x \in \mathbb{Z}$ tel que $\overline{a} \cdot \overline{x} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

*Démonstration.* Si $\mathrm{pgcd}(a, n) = 1$ alors il existe $x$ et $y$ tels que $xa + yn = 1$. On a $\overline{n} = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$, donc $\overline{xa} + \overline{yn} = \overline{xa} = \overline{1}$. Par contre, si $\overline{ax} = \overline{1}$, alors $\overline{ax - 1} = \overline{0}$, donc $ax - 1$ est divisible par $n$, disons $ax - 1 = -yn$. Alors $ax + yn = 1$ et $a$ et $n$ sont donc relativement premiers (voir exercice 0.4). □

*Exercice* 0.12. Résoudre l'équation $14x \equiv 1 \bmod 47$. Suggestion : utiliser l'exercice 0.3.

*Exercice* 0.13. VRAI ou FAUX.
(i) Si $ab \equiv ac \bmod n$, alors $b \equiv c \bmod n$.
(ii) Si $\mathrm{pgcd}(a, n) = 1$, alors $ab \equiv ac \bmod n$ implique $b \equiv c \bmod n$.

*Exercice* 0.14. VRAI ou FAUX. (Il faut avoir vu les définitions d'homomorphisme de groupes pour faire cet exercice.)
(i) Soit $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/m\mathbb{Z}, +)$ avec $m, n$ deux entiers positifs. Si $m \mid n$, alors $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ défini par $\overline{i} \mapsto \phi(\overline{i}) = \overline{(i \bmod m)}$ est un morphisme de groupe.
(ii) Soit $(\mathbb{Z}/n\mathbb{Z}, \times)$ et $(\mathbb{Z}/m\mathbb{Z}, \times)$ avec $m, n$ deux entiers positifs. Si $m \mid n$, alors $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ défini par $\overline{i} \mapsto \phi(\overline{i}) = \overline{(i \bmod m)}$ est un morphisme de groupe.

0.9. **Nombres réels.** (Les deux sous-sections finales ne seront pas utilisées dans le cours Algèbre 1.) On donnera une définition d'un nombre réel (est-ce qu'on a déjà donné dans un de vos cours une définition d'un nombre réel qui ne soit pas basée sur l'intuition géométrique ?) Une suite $(a_i)_{i\in\mathbb{N}}$ où $a_i \in \mathbb{Q}$ est appelé une *suite de Cauchy*, si pour chaque $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, il existe un $N \in \mathbb{N}$ tel que $|a_i - a_j| \leq \epsilon$ pour chaque $i, j \geq N$. Chaque fraction $a \in \mathbb{Q}$ définit une suite de Cauchy $(a_i)_{i\in\mathbb{N}}$, si on pose $a_i = a$ pour chaque $i \in \mathbb{N}$. Soit $X$ la collection de toutes les suites de Cauchy. On définit une relation d'équivalence sur $X$, comme $(a_i)_{i\in\mathbb{N}} \sim (a'_i)_{i\in\mathbb{N}}$ si et seulement si pour chaque $\epsilon \in \mathbb{Q}, \epsilon > 0$ il existe un $N \in \mathbb{N}$ tel que pour chaque $i \geq N$ on a $|a_i - a'_i| \leq \epsilon$.

Les classes d'équivalence $X/\sim$ sont appelées « nombres réels » et $\mathbb{R} := X/\sim$. Comment définir la somme et le produit de deux « nombres réels » ?

Une autre définition courante de nombre réel (pas basée sur l'intuition) est basée sur les *coupures de Dedekind*.

0.10. **Nombres $p$-adiques.** Presque la même définition définit un autre genre de nombre, nommé *$p$-adique*, étrange mais quand même très utile. Pour chaque nombre premier $p$, il existe une valeur absolue $|x|_p$ sur $\mathbb{Q}$ différente de la valeur absolue usuelle. Soit $\frac{n}{d}$ une fraction. Écrivons $n = p^i n'$, où $p \nmid n'$, et $d = p^j d'$ où $p \nmid d'$. On définit alors

$$\left|\frac{n}{d}\right|_p := p^{j-i} \text{ (dans } \mathbb{Q}).$$

Donc un entier est petit pour cette valeur absolue si et seulement si cet entier est divisible par une haute puissance de $p$.

Une suite $(a_i)_{i\in\mathbb{N}}$ où $a_i \in \mathbb{Q}$ est appelé une suite $p$-adique de Cauchy, si pour chaque $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, il existe un $N \in \mathbb{N}$ tel que $|a_i - a_j|_p \leq \epsilon$ pour chaque $i, j \geq N$. Chaque fraction $a \in \mathbb{Q}$ définit une suite de Cauchy $(a_i)_{i\in\mathbb{N}}$, si on pose $a_i = a$ pour chaque $i \in \mathbb{N}$. Soit $X_p$ la collection de toutes les suites $p$-adique de Cauchy. On définit une relation d'équivalence sur $X_p$, comme $(a_i)_{i\in\mathbb{N}} \sim (a'_i)_{i\in\mathbb{N}}$ si et seulement si pour chaque $\epsilon \in \mathbb{Q}, \epsilon > 0$ il existe un $N \in \mathbb{N}$ tel que pour chaque $i \geq N$ on a $|a_i - a'_i|_p \leq \epsilon$.

Les classes d'équivalence $X_p/\sim$ sont appelées *nombres $p$-adiques* et $\mathbb{Q}_p := X_p/\sim$. Comment définir la somme et le produit de deux nombres $p$-adiques ?

## 1. Définitions et notions élémentaires

1.1. **Introduction.** En mathématiques plusieurs *langues* sont utilisées, ou modes de penser, d'argumenter ou de communiquer : les langues géométrique, analytique, topologique, probabiliste, statistique, fonctionnelle, algébrique, fonctorielle, et cetera. Chaque mathématicien devrait au moins maîtriser les éléments de base de chaque branche. Ce cours donnera une introduction à l'orientation algébrique, à l'aide de la notion de *groupe*.

Partout dans les mathématiques des *groupes* jouent un rôle considérable, mais aussi dans les autres domaines scientifiques comme la physique (par exemple la mécanique quantique) ou la chimie (par exemple la cristallographie). Souvent les groupes décrivent les symétries d'une structure : le groupe des mouvements dans l'espace, le groupe de Lorentz, le groupe symétrique, le groupe de monodromie, le groupe de tresses, le groupe de l'icosaèdre, le groupe d'une équation de degré 5, et cetera. Chaque fois qu'il y a des symétries dans un problème scientifique, il y a un certaine groupe associé et, règle générale, il vaut la peine d'expliciter ce groupe et d'utiliser ses propriétés.

Un *groupe* est un ensemble muni d'une opération associative, qui possède un neutre (qui « ne fait rien ») et dont chaque élément a un inverse (« on peut neutraliser chaque élément »).

Voici quelques exemples typiques.

L'ensemble des nombres entiers $\mathbb{Z}$ avec l'opération $+$ usuelle. On a bien sûr l'associativité, $(a+b)+c = a+(b+c)$, le nombre 0 est le neutre, $a+0 = 0+a = a$, et l'inverse du nombre $a$ est $-a$, $a+(-a) = (-a)+a = 0$. C'est un groupe *commutatif*, c'est-à-dire que $a+b = b+a$ est toujours vrai.

Considérons l'ensemble des fractions non nulles $\mathbb{Q} - \{0\}$ avec, comme opération, la multiplication usuelle $\cdot$. L'associativité fonctionne, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, le neutre est 1 (parce que $1 \cdot x = x \cdot 1 = x$ pour chaque $x$), et l'inverse de $x$ est $x^{-1} = 1/x$ (parce que $x \cdot x^{-1} = x^{-1} \cdot x = 1$). C'est aussi un groupe commutatif, car $x \cdot y = y \cdot x$ est toujours vrai.

Soit $M :=$ { I, II, III, IV, ..., XI, XII} l'ensemble des heures d'une montre de douze heures et l'opération $+$ (l'addition sur la montre) est définie comme $h_1 + h_2 = h_3$ si et seulement si $h_2$ heures plus tard que $h_1$ heures est $h_3$ heures sur la montre. Par exemple, X+X = VIII. Maintenant le neutre est XII, l'inverse de III est IX, de IV est VIII, et cetera. C'est un groupe commutatif d'ordre fini.

Un exemple d'un groupe non commutatif est le groupe linéaire général $\mathrm{GL}(n, \mathbb{R})$ des matrices réelles de taille $n \times n$ et de déterminant non nul :

$$\mathrm{GL}(n, \mathbb{R}) := \{A \text{ matrice réelle } n \times n \mid \det(A) \neq 0\}$$

avec l'opération $\cdot$, la multiplication matricielle usuelle. En algèbre linéaire on montre que cette multiplication est associative ; la matrice identité $\mathbf{1}$ est le neutre ($A \cdot \mathbf{1} = \mathbf{1} \cdot A = A$) et chaque matrice réelle de déterminant non nul $A$ a une matrice inverse de déterminant non nul $A^{-1}$ (on a $A \cdot A^{-1} = A^{-1} \cdot A = \mathbf{1}$). Ce groupe n'est pas commutatif si $n > 1$, parce qu'il y a des matrices inversibles $A$ et $B$ telles que $A \cdot B \neq B \cdot A$.

Un autre exemple est le groupe symétrique $S_n$, l'ensemble de toutes les bijections de $\{1, 2, \ldots, n\}$, avec la composition $\circ$ comme opération. Ce groupe joue un rôle important dans la théorie du déterminant d'une matrice carrée. La composition d'applications est toujours associative, le neutre

est l'application identité et chaque bijection a un inverse (presque par définition). Si $n > 2$ le groupe symétrique n'est pas commutatif. C'est un autre exemple d'un groupe d'ordre fini.

1.2. **Définitions.** Soyons plus exacts maintenant.

Une *opération interne* $\circ$ (ou *opération binaire* ou *produit*) sur un ensemble $E$ est une application

$$E \times E \to E \ : \ (a, b) \mapsto a \circ b.$$

Alors à chaque paire (sans exceptions !) ordonnée $(a, b)$ d'éléments de $E$ est associé un nouvel élément (unique) de $E$, noté $a \circ b$. À la place de $\circ$ on emploie aussi autres symboles comme $*, \bullet, \cdot, +, \triangle, \ldots$. L'opération interne est *associative* si

$$(x \circ y) \circ z = x \circ (y \circ z)$$

pour chaque $x, y, z \in E$.

Un *demi-groupe* est une paire ordonnée $(E, \circ)$ d'un ensemble et d'une opération interne associative.

*Exemples* 1.1. Une opération bien connue sur $\mathbb{Z}$ est la soustraction $-$. Cette opération interne n'est pas associative, car par exemple $1-(2-3) \neq (1-2)-3$. Alors $(\mathbb{Z}, -)$ n'est pas un demi-groupe. Nous allons seulement étudier les opérations internes associatives, mais ils existent aussi des opérations internes très intéressantes, mais non associatives. Par exemple, considérons l'ensemble de toutes les matrices $n \times n$ réelles antisymétriques ($A = -A^t$, où $A^t$ est la matrice transposée de $A$) avec l'opération interne « crochet de Lie »

$$A \times B := A \cdot B - B \cdot A,$$

où $\cdot$ est la multiplication de matrices usuelle. Alors $A \times B$ est aussi une matrice antisymétrique.

*Exercice* 1.1. Montrer que le crochet de Lie $A \times B$ est une opération interne associative sur l'ensemble de toutes les matrices antisymétriques $n \times n$ *si et seulement si* $n \leq 2$. Montrer par contre que l'identité suivante de Jacobi est toujours satisfaite :

$$A \times (B \times C) + B \times (C \times A) + C \times (A \times B) = 0$$

et que $A \times B = -B \times A$. Ce sont les axiomes d'un anneau de Lie.

Soit $(E, \circ)$ un demi-groupe et soient $x_1, x_2, x_3$ et $x_4 \in E$. Alors par l'associativité de $\circ$, tous les produits

$$x_1 \circ (x_2 \circ (x_3 \circ x_4)) = x_1 \circ ((x_2 \circ x_3) \circ x_4) = (x_1 \circ (x_2 \circ x_3)) \circ x_4 =$$
$$= ((x_1 \circ x_2) \circ x_3) \circ x_4 = (x_1 \circ x_2) \circ (x_3 \circ x_4)$$

donnent le même élément de $E$. On écrit cet élément sans parenthèses comme

$$x_1 \circ x_2 \circ x_3 \circ x_4.$$

et de façon analogue pour les produits de plus de termes. Si par contre l'opération interne $\circ$ n'est pas associative nous ne donnons pas à $x_1 \circ x_2 \circ x_3$ un sens.

L'opération interne est *commutative* si

$$x \circ y = y \circ x$$

pour chaque $x, y \in E$. *Nous n'allons utiliser le symbole + (« plus ») que pour les opérations internes commutatives.*

Un élément *neutre* (simultanément à gauche et à droite) pour une opération $\circ$ sur $E$ est un élément $x \in E$ tel que

$$x \circ y = y \circ x = y$$

pour chaque $y \in Y$.

Un *monoïde* est un demi-groupe $(E, \circ)$ où l'opération interne possède un élément neutre. Nous obtenons un premier résultat. C'est un résultat facile à montrer, mais ce n'est pas évident.

**Lemme 1.1.** *Soit $(E, \circ)$ un monoïde. Alors l'opération interne $\circ$ ne possède qu'un seul élément neutre.*

*Démonstration.* Par la définition de monoïde il existe un élément neutre, disons $x$. Supposons que $y$ est aussi un élément neutre. Alors $y = x \circ y$ (parce que $x$ est un neutre) et $x \circ y = x$ (parce que $y$ est un neutre). Donc $x = y$. □

Alors on peut parler **du** *neutre* d'un monoïde $(M, \circ)$, parce que cet élément (qui existe par hypothèse d'un monoïde) est uniquement déterminé. Ce neutre est noté $\mathbf{1}_M$ (ou $\mathbf{1}$ s'il n'y a pas de confusion possible), si le symbole d'opération n'est pas $+$. Par contre, on écrit $\mathbf{0}_M$ ou $\mathbf{0}$ (« zéro ») pour le neutre si l'opération interne du monoïde $(M, +)$ est notée $+$.

*Exemples* 1.2. Par exemple, $(\mathbb{Z}_{\geq 0}, +)$ est un monoïde avec neutre 0, mais $(\mathbb{Z}_{>0}, +)$ est seulement un demi-groupe. Aussi $(\mathbb{Z}, \cdot)$ est un monoïde, dans lequel le nombre 1 est le neutre.

Soit $M(n \times n, \mathbb{R})$ l'ensemble de toutes les matrices réelles de taille $n \times n$ et $\cdot$ la multiplication matricielle usuelle. Alors $(M(n \times n, \mathbb{R}), \cdot)$ est un monoïde, le neutre étant la matrice identité $\mathbf{1}$.

Pour deux ensembles $X$ et $Y$ on écrit $X^Y$ pour l'ensemble de toutes les applications $f : Y \to X$. Si $Y = X$, la composition $f \circ g$ de deux applications $f, g \in X^X$ est définie comme d'habitude par

$$(f \circ g)(x) := f(g(x)).$$

Alors $(X^X, \circ)$ est un monoïde avec neutre l'application identité $\mathbf{1}$ (où $\mathbf{1}(x) = x$ pour chaque $x \in X$). On vérifie l'associativité :

$$(f_1 \circ (f_2 \circ f_3))(x) = f_1((f_2 \circ f_3)(x)) = f_1(f_2(f_3(x))) = (f_1 \circ f_2)(f_3(x)) = ((f_1 \circ f_2) \circ f_3)(x),$$

pour chaque $x \in X$ et $f_1, f_2, f_3 \in X^X$.

Soit $(E, \circ)$ un monoïde avec neutre $\mathbf{1}_E$. On dit que $x \in E$ a un *inverse* (simultanément à gauche et à droite) dans le monoïde s'il existe un élément $y \in E$ tel que

$$x \circ y = y \circ x = \mathbf{1}_E.$$

**Lemme 1.2.** *Soit $(E, \circ)$ un monoïde. Il est impossible qu'un élément de $E$ ait plus qu'un inverse.*

*Démonstration.* Supposons que $y$ et $z$ sont deux inverses de $x$ dans le monoïde avec neutre $\mathbf{1}_E$. Alors

$$y = y \circ \mathbf{1}_E = y \circ (x \circ z) = (y \circ x) \circ z = \mathbf{1}_E \circ z = z.$$

Ici on a utilisé les propriétés du neutre $\mathbf{1}_E$, de l'associativité et d'un inverse. Donc $y = z$. □

Ainsi, dans un monoïde, on peut parler de l'*inverse* de $x$ si $x$ possède un inverse, parce que cet élément est uniquement déterminé. Cet inverse de $x$ est noté $x^{-1}$, si l'opération n'est pas $+$. Mais on écrit $-x$ pour l'inverse si l'opération interne est notée $+$. Mais nous ne donnons pas de sens à $x^{-1}$ (ni à $-x$) si $x$ n'a pas d'inverse (ou si on ne sait pas si $x$ possède un inverse ou non).

*Exercice* 1.2. Déterminer si les opérations suivantes sont binaires sur les ensembles proposés.
(i) L'opération $\exp : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ qui associe à la paire d'entiers $(m, n)$ le nombre $m^n$.
(ii) La soustraction sur $\mathbb{Z}$.
(iii) L'opération « produit vectoriel » sur l'ensemble des vecteurs de $\mathbb{R}^3$ : $(\vec{u}, \vec{v}) \mapsto \vec{u} \times \vec{v}$.
(iv) L'opération sur l'ensemble des matrices $n \times n$ symétriques qui associe à la paire $S_1$ et $S_2$ la matrice $S_1 S_2$.
(v) Le produit défini sur $\mathbb{Z}/6\mathbb{Z}$. (La multiplication sur $\mathbb{Z}/n\mathbb{Z}$ a été définie à la section 0.8.)
(vi) L'opération intersection $\cap$ sur l'ensemble $\big\{\{\ \}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\big\}$.

*Exercice* 1.3. Quelles propriétés (associativité, existence d'un neutre, existence d'un inverse) sont satisfaites par les opérations définies sur les ensembles suivants ?
(i) L'exponentiation $(m, n) \mapsto m^n$ sur l'ensemble $\mathbb{N}$.
(ii) L'opération $x \circledast y$ définie pour $x, y \in \mathbb{R}$ par $x \circledast y = x + y - xy$.
(iii) L'opération multiplication sur $\mathbb{Z}/6\mathbb{Z}$.
(iv) L'opération union $\cup$ sur l'ensemble de tous les sous-ensembles de $\mathbb{Z}$.

Un *groupe* est un monoïde dont tous les éléments possèdent un inverse. Donc on peut parler du neutre du groupe et de l'inverse de chaque élément.

Un groupe *abélien*[2] (ou *commutatif* ) est un groupe dont l'opération interne est commutative.

Le nombre d'éléments dans un groupe $G$ est appelé l'*ordre* de $G$ et est noté $|G|$ ou $O(G)$. Si ce nombre est fini, le groupe est dit *fini* ; sinon le groupe est *infini*.

Un critère pour qu'un demi-groupe soit un groupe est donné dans l'exercice suivant.

*Exercice* 1.4. Soit $E$ un ensemble avec une opération interne associative notée $\circ$. On suppose l'existence d'un élément $e \in E$ avec les propriétés suivantes :

(i) pour chaque $a \in E$ on a $e \circ a = a$ (on dit que $e$ est un *neutre à gauche*) ;

(ii) pour chaque $a \in E$ il existe un $b \in E$ tel que $b \circ a = e$ (on dit que *l'inverse à gauche* existe).

Alors $(E, \circ)$ est un groupe.[3]

*Exercice* 1.5. L'ensemble des matrices $n \times n$ à coefficients entiers et de déterminant non nul, avec l'opération $\cdot$ (la multiplication matricielle) est un monoïde mais pas un groupe.

*Exercice* 1.6. Un groupe dans lequel chaque élément est son propre inverse (i.e., $x = x^{-1}$) est abélien.

*Exercice* 1.7. Soit $(G, +)$ un groupe abélien fini.

2. Niels Henrik Abel, mathématicien norvégien, 1802–1829.
3. Les exercices ne contenant qu'un énoncé consistent à démontrer cet énoncé.

(i) Supposons $x \in G$ est un élément tel que $x + x = \mathbf{0}$. Si $x \neq \mathbf{0}$ alors l'ordre de $G$ est pair. Indice : montrer que $G$ est la réunion disjointe d'un certain nombre de jumeaux $\{a, a + x\}$, ce qui implique que l'ordre de $G$ est pair.

(ii) Soit $x$ la somme de tous les éléments du groupe. Alors $x + x = \mathbf{0}$ et si l'ordre de $G$ est impair alors $x = \mathbf{0}$.

*Exercice* 1.8. Soit $n \in \mathbb{Z}_{\geq 1}$. Le groupe *cyclique* d'ordre $n$ est la paire $(C_n, \cdot)$, où

$$C_n := \{e^{2\pi ik/n} \in \mathbb{C};\ k \in \mathbb{Z}\} = \{z \in \mathbb{C}; z^n = 1\}$$

est l'ensemble des $n$ racines $n$-ièmes de 1 dans $\mathbb{C}$ et où $\cdot$ est la multiplication des nombres complexes. Si on écrit $\rho := e^{2\pi i/n}$ alors

$$C_n = \{1, \rho, \rho^2, \rho^3, \ldots, \rho^{n-1}\}$$

a exactement $n$ éléments et $\rho^n = 1$, $\rho^{-1} = \rho^{n-1}$.

*Exercice* 1.9. Fixons $n \geq 2$.

(i) La rotation du plan réel par $2\pi k/n$ radian (ou par $360k/n$ degrés) est réalisée par la matrice orthogonale

$$\begin{pmatrix} \cos 2\pi k/n & -\sin 2\pi k/n \\ \sin 2\pi k/n & \cos 2\pi k/n \end{pmatrix}$$

et la réflexion par rapport à la droite qui fait l'angle $\pi k/n$ radian (ou par $180k/n$ degrés) avec l'axe des $x$ est réalisée par la matrice orthogonale

$$\begin{pmatrix} \cos 2\pi k/n & \sin 2\pi k/n \\ \sin 2\pi k/n & -\cos 2\pi k/n \end{pmatrix}.$$

(ii) Le groupe *diédral* est la paire $(D_n, \cdot)$, où

$$D_n := \left\{ \begin{pmatrix} \cos 2\pi k/n & -\sin 2\pi k/n \\ \sin 2\pi k/n & \cos 2\pi k/n \end{pmatrix};\ k \in \mathbb{Z} \right\} \cup \left\{ \begin{pmatrix} \cos 2\pi k/n & \sin 2\pi k/n \\ \sin 2\pi k/n & -\cos 2\pi k/n \end{pmatrix};\ k \in \mathbb{Z} \right\}$$

est une certaine collection de $2n$ matrices orthogonales et où $\cdot$ est la multiplication matricielle. C'est un groupe non commutatif si et seulement si $n > 2$. Décrire les éléments qui sont leur propre inverse.

(iii) Écrivons

$$\rho := \begin{pmatrix} \cos 2\pi/n & -\sin 2\pi/n \\ \sin 2\pi/n & \cos 2\pi/n \end{pmatrix} \text{ et } \sigma := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Alors

$$\sigma^2 = \rho^n = \mathbf{1} \text{ et } \sigma\rho\sigma = \rho^{-1} = \rho^{n-1}$$

et

$$D_n = \{\rho^i \sigma^j;\ 0 \leq i < n, 0 \leq j < 2\}.$$

Remarque : Soit $M$ une matrice $2 \times 2$ orthogonale quelconque. Alors $M \in D_n$ si et seulement si $M$ transforme le polygone régulier à $n$ côtés sur lui-même. Pour le voir, remarquons que, pour qu'une transformation linéaire envoie un polygone régulier sur lui-même, il faut que chacun des sommets soit envoyé sur un sommet. Il y a donc $n$ façons de choisir l'image $M(S)$ d'un sommet donné $S$. Supposons cette image fixée et étudions le côté qui suit le sommet $S$ (dans le sens anti-horaire). Ce

côté doit être envoyé par $M$ sur le côté qui suit $M(S)$ (dans le sens anti-horaire) ou qui le précède. Il y a donc deux choix possibles. Ainsi le groupe de matrices orthogonales qui envoie un polygone régulier à $n$ côtés sur lui-même possède $2n$ éléments. Si le côté qui suit $S$ est envoyé sur celui qui suit $M(S)$, alors le déterminant de $M$ est 1 et $M$ représente une rotation ; sinon son déterminant est $-1$ et $M$ est une réflexion.

*Exercice* 1.10. Soit $(M, \circ)$ un monoïde. On écrit

$$M^\times := \{m \in M | \ \ m \text{ possède un inverse dans le monoïde } (M, \circ)\}.$$

Montrer que $x \circ y \in M^\times$ si $x$ et $y \in M^\times$ et montrer que la paire $(M^\times, \circ)$ (où $\circ$ est l'opération interne sur $M^\times$ induite par l'opération interne sur $M$) est un groupe.

On a par exemple $(M(n, \mathbb{R})^\times, \cdot) = (\mathrm{GL}(n, \mathbb{R}), \cdot)$ et $((X^X)^\times, \circ) = (S_n, \circ)$, si $X = \{1, 2, \ldots, n\}$. Décrire $(\mathbb{Z}^\times, \cdot)$. (Le groupe $S_n$ est le groupe de permutations de $n$ objets et sera décrit à la section 2.)

*Exercice* 1.11. Dresser la liste des matrices orthogonales $3 \times 3$ qui transforment l'octaèdre régulier en lui-même. Vérifier que cet ensemble de matrices, muni de la multiplication matricielle, forme un groupe. Est-il abélien ? Note : les sommets de l'octaèdre peuvent être choisis en les six points $(\pm 1, 0, 0), (0, \pm 1, 0), (0, 0, \pm 1)$. Ce groupe contient 24 éléments dont le déterminant est $+1$. [4]

1.3. **Notation.** Dans un groupe $(G, \circ)$ on écrit souvent $ab$ à la place de $a \circ b$ (sauf si le symbole de l'opération interne est le $+$, dans ce cas on ne supprime jamais le symbole $+$).

Souvent on dénote un groupe $(G, \circ)$ par son ensemble $G$ seulement. Dans ce cas il faut que ce soit clair, par le contexte, quelle opération interne $\circ$ est utilisée. Si le symbole de l'opération interne n'est pas explicitement donné on utilise généralement $x \cdot y$ ou $xy$ pour l'opération interne. Mais si le groupe est abélien on écrit généralement (mais pas exclusivement) $x + y$ pour l'opération.

Soit $(G, \circ)$ un groupe. On pose $x^0 := \mathbf{1}_G$, $x^1 := x$ et $x^{-1}$ pour l'inverse de $x$. On définit par induction sur l'entier $n \geq 0$

$$x^n := (x^{n-1}) \circ x \text{ et } x^{-n} := x^{-n+1} \circ x^{-1}.$$

Par exemple, $x^5 = x \circ x \circ x \circ x \circ x$ et $x^{-2} = x^{-1} \circ x^{-1}$. De façon analogue, si $(G, +)$ est un groupe abélien avec opération interne $+$, on définit $0x = \mathbf{0}$, $1x := x$ et $-1x = -x$ pour l'inverse de $x$ et par induction sur l'entier $n$

$$nx := ((n-1)x) + x \text{ et } \ -nx := (-n+1)x + (-x).$$

Si l'opération interne n'est pas $+$, alors $2x$ n'est pas défini, et si l'opération interne est notée par $+$ alors $x^2$ n'est pas défini a priori.

4. Il est possible de montrer que le groupe laissant l'octaèdre invariant peut être engendré par des réflexions (transformations linéaires orthogonales de déterminant $-1$ dont le carré est l'identité). Les groupes engendrés par des réflexions forment une famille importante appelés groupes de Coxeter du nom du géomètre canadien H.S.M. Coxeter (1907–2003), né en Angleterre, qui a fait sa carrière à l'Université de Toronto. Voir H.S.M. Coxeter, *Regular Polytopes*, Dover (1993) ; J.E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge (1992).

*Exercice* 1.12. Soit $(G, \circ)$ un groupe et $x \in G$. Alors pour $n$ et $m \in \mathbb{Z}$ on a

$$x^{n+m} = x^n \circ x^m \text{ et } (x^n)^{-1} = x^{-n}.$$

1.4. **Homomorphisme de groupes.** Un *homomorphisme* ou un *morphisme* (de groupes) entre deux groupes $(G, \circ)$ et $(K, *)$ est une application $\phi : G \to K$ telle que

$$\phi(x \circ y) = \phi(x) * \phi(y)$$

pour chaque $x$ et $y \in G$.

Un *monomorphisme* est un homomorphisme injectif ; ceci veut dire que $x \neq y \in G$ implique que $\phi(x) \neq \phi(y) \in K$.

Un *épimorphisme* est un homomorphisme surjectif ; ceci veut dire que, pour chaque $k \in K$, il existe au moins un élément $g \in G$ tel que $\phi(g) = k$.

Un *isomorphisme* est un homomorphisme bijectif ; ceci veut dire que pour chaque $k \in K$ il existe un seul élément $g \in G$ tel que $\phi(g) = k$. Cet élément $g$ est noté $\phi^{-1}(k)$.

Un *endomorphisme* est un homomorphisme d'un groupe dans lui-même, c'est-à-dire lorsque $(G, \circ) = (K, *)$.

Un *automorphisme* est un endomorphisme bijectif. L'ensemble de tous les automorphismes d'un group $G$ est noté $\mathrm{Aut}(G)$.

*Exemples* 1.3. Le déterminant $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^\times$ définit un homomorphisme entre $(\mathrm{GL}(n, \mathbb{R}), \cdot)$ et $(\mathbb{R}^\times, \cdot)$ (rappel : $\mathbb{R}^\times = \mathbb{R} \backslash \{0\}$). Parce que (par l'algèbre linéaire)

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

pour toutes les matrices $n \times n$ $A$ et $B$. Le déterminant est un épimorphisme (pourquoi ?).

La fonction exponentielle $\exp : \mathbb{R} \to \mathbb{R}^\times$ définit un homomorphisme de groupes entre $(\mathbb{R}, +)$ et $(\mathbb{R}^\times, \cdot)$, parce que

$$\exp(x + y) = \exp(x) \cdot \exp(y).$$

C'est un monomorphisme mais pas un épimorphisme (pourquoi ?).

La fonction exponentielle $\exp : \mathbb{C} \to \mathbb{C}^\times$ définit un homomorphisme de groupes entre $(\mathbb{C}, +)$ et $(\mathbb{C}^\times, \cdot)$, parce que $\exp(x + y) = \exp(x) \cdot \exp(y)$. Maintenant c'est un épimorphisme mais pas un monomorphisme (pourquoi ?).

L'application inverse-transposé $\mathrm{GL}(n, \mathbb{R}) \to \mathrm{GL}(n, \mathbb{R})$ qui applique une matrice $A$ à son inverse transposée $(A^t)^{-1} (= (A^{-1})^t)$ est un automorphisme de $(\mathrm{GL}(n, \mathbb{R}), \cdot)$. (Exercice : le montrer !)

En théorie des groupes, on considère deux groupes comme équivalents ou « pratiquement les mêmes groupes » s'il existe un isomorphisme entre les deux groupes. Le concept d'isomorphisme est donc extrêmement important.

*Exercice* 1.13. Soit

$$G := \left\{ \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} ;\ \phi \in \{0, 2\pi/3, 4\pi/3\} \right\}$$

et $\cdot$ la multiplication matricielle usuelle. Alors $(G, \cdot)$ est un groupe.

Soit $H := \{a, b, c\}$ avec l'opération interne $\blacklozenge$ définie par la table de composition

| $\blacklozenge$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $c$ | $a$ | $b$ |
| $b$ | $a$ | $b$ | $c$ |
| $c$ | $b$ | $c$ | $a$ |

Alors $(H, \blacklozenge)$ est un groupe.

Les deux groupes $(G, \cdot)$ et $(H, \blacklozenge)$ sont isomorphes. Montrer enfin que $(G, \cdot)$ est isomorphe à un des groupes cycliques introduits à l'exercice 1.8. Lequel ? Est-ce que cette observation implique que $H$ est aussi isomorphe à ce groupe cyclique ? Pourquoi ? (Tous les groupes de cardinalité trois sont « pratiquement le même groupe ».)

*Exercice* 1.14. VRAI ou FAUX.
(i) Soient $G$ et $H$ deux groupes et $f : G \to H$ la fonction qui envoie tous les éléments de $G$ sur le neutre $\mathbf{1}_H$. Alors $f$ est un morphisme de groupes.
(ii) Soit $x \in G$ un élément fixé d'un groupe $G$. La fonction $f : G \to G$ donnée par $f(g) = gx$ est un endomorphisme de $G$.
(iii) Soit $X$ l'ensemble de tous les groupes finis et $G \sim H$ la relation « $G$ est isomorphe à $H$ ». Alors $\sim$ est une relation d'équivalence.
(iv) Soit $G$ un groupe abélien et $f : G \to H$ un monomorphisme. Alors $H$ est abélien.
(v) Soit $G$ un groupe abélien et $f : G \to H$ un épimorphisme. Alors $H$ est abélien.

*Exercice* 1.15. Si $\phi : G \to K$ est un isomorphisme de groupes, alors l'application inverse $\phi^{-1} : K \to G$ est aussi un isomorphisme de groupes. La composition $\phi \circ \psi$ de deux automorphismes $\phi$ et $\psi$ de $G$ donne une opération interne sur $\operatorname{Aut} G$ ; $(\operatorname{Aut} G, \circ)$ est un groupe, le *groupe d'automorphismes* de $G$.

*Exercice* 1.16. Chaque élément $g \in G$ définit un automorphisme $c_g$ de $G$ par *conjugaison*, défini par

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

L'application $c : G \to \operatorname{Aut} G$ définie par $c(g) := c_g$ donne un homomorphisme de groupes.

*Exercice* 1.17. Soit un groupe $G$. L'*ordre* d'un élément $x \in G$ est le plus petit entier positif $n$ tel que $x^n = \mathbf{1}_G$, si cet entier existe. S'il existe, l'élément est dit d'ordre fini ; sinon, il est d'ordre infini. Montrer qu'un automorphisme préserve l'ordre d'un élément.

*Exercice* 1.18. Soit $G = \{g_1, g_2, \ldots, g_n\}$ un groupe fini. On définit son opération interne en donnant explicitement sa table de composition, comme pour la loi $\blacklozenge$ de l'exercice 1.13. Montrer que chaque élément $g_i$, $1 \leq i \leq n$, apparaît une et une seule fois dans chaque ligne et chaque colonne de cette table.

*Exercice* 1.19. Soit $n > 2$ et $(G, \cdot)$ un groupe. Supposons qu'il existe $a, b \in G$ tels que $a^n = b^2 = \mathbf{1}_G$ et $ba = a^{-1}b$ et $n$ est le plus petit $n \geq 1$ tel que $a^n = \mathbf{1}$. Montrer qu'il existe un monomorphisme du groupe diédral $D_n$ (exercice 1.9) dans $G$.

Le *noyau* d'un homomorphisme $\phi : G \to K$ (dénoté par $\operatorname{Ker}\phi$) est défini comme

$$\operatorname{Ker}\phi := \{g \in G |\ \phi(g) = \mathbf{1}_K\},$$

où $\mathbf{1}_K$ est le neutre du groupe $K$. Ainsi le noyau est l'ensemble des éléments de $G$ qui sont envoyés vers le neutre de $H$. L'*image* de $\phi$ est définie comme d'habitude par

$$\operatorname{Im}\phi := \{\phi(g) |\ g \in G\}.$$

**Lemme 1.3.** *Soit $\phi : G \to K$ un homomorphisme entre les groupes $(G, \circ)$ et $(K, *)$. Alors $\phi(\mathbf{1}_G) = \mathbf{1}_K$ et pour chaque $g \in G$ on a $\phi(g^{-1}) = (\phi(g))^{-1}$.*

*Démonstration.* On utilise que si $x^2 = x$ dans un groupe, alors $x = \mathbf{1}$. (Preuve : $x^2 = x$ implique que $x^2 \cdot x^{-1} = x \cdot x^{-1}$, donc $x = \mathbf{1}$.) On a maintenant

$$\phi(\mathbf{1}_G) = \phi(\mathbf{1}_G \circ \mathbf{1}_G) = \phi(\mathbf{1}_G) * \phi(\mathbf{1}_G),$$

donc $\phi(\mathbf{1}_G) = \mathbf{1}_K$. Le reste de la preuve est laissé en exercice. □

**Lemme 1.4.** *Un homomorphisme $\phi : G \to K$ est un monomorphisme si et seulement si le noyau de $\phi$ ne contient que le neutre de $G$.*

*Démonstration.* Le noyau contient au moins le neutre de $G$. Supposons que $\phi$ est un monomorphisme, alors $g \neq \mathbf{1}_G$ implique que $\phi(g) \neq \phi(\mathbf{1}_G) = \mathbf{1}_K$. Donc $g \notin \operatorname{Ker}\phi$.

Par contre, supposons que $\operatorname{Ker}\phi = \{\mathbf{1}_G\}$ et $x \neq y \in G$. Alors $x \circ y^{-1} \neq \mathbf{1}_G$ et $\phi(x \circ y^{-1}) \neq \mathbf{1}_K$. Alors $\phi(x) * \phi(y^{-1}) = \phi(x) * \phi(y)^{-1} \neq \mathbf{1}_K$ et $\phi(x) \neq \phi(y)$. Donc l'application $\phi$ est injective. □

*Exercice* 1.20. Soit $\log : (\mathbb{R}^\times_{>0}, .) \to (\mathbb{R}, +)$ le logarithme. Vérifier les deux lemmes précédents dans ce cas.

*Exercice* 1.21. Soient $D_3$ et $C_2$ les groupes diédral et cyclique définis aux exercices 1.8 et 1.9. Soit $f : D_3 \to C_2$ la fonction définie comme suit :

$$\begin{pmatrix} \cos 2\pi k/3 & -\sin 2\pi k/3 \\ \sin 2\pi k/3 & \cos 2\pi k/3 \end{pmatrix} \mapsto 1 \qquad \text{et} \qquad \begin{pmatrix} \cos 2\pi k/3 & \sin 2\pi k/3 \\ \sin 2\pi k/3 & -\cos 2\pi k/3 \end{pmatrix} \mapsto -1$$

quelque soit $k$.
(i) Montrer que $f$ est un morphisme de groupes.
(ii) Identifier son noyau et son image.
(iii) Est-ce un monomophisme ? un épimorphisme ? un isomorphisme ?

*Exercice* 1.22. Trouver tous les homomorphismes $\phi : C_n \to D_n$ et $\psi : D_n \to C_n$ entre le groupe cyclique et le groupe diédral, si $n = 2, 3, 4$.

## 2. Permutations et groupe symétrique

2.1. **Définition du groupe $S_n$.** Le groupe des permutations d'un ensemble fini est un des plus importants groupes finis. En fait il s'agit d'une famille de groupes finis $S_n$, étiquetée par les entiers positifs. Nous allons établir quelques-unes de leurs propriétés.

Soit $E$ un ensemble. On dit qu'une application $f : E \to E$ a un inverse, s'il existe une application $g : E \to E$ telle que les deux compositions $f \circ g$ et $g \circ f$ sont l'application identité, c'est-à-dire

$$f(g(x)) = g(f(x)) = x$$

pour chaque $x \in E$. Cette application $g$ est unique (pourquoi ?) et notée souvent $f^{-1}$, l'inverse de $f$. On dit alors que $f$ est une bijection ou une permutation de $E$. L'ensemble de toutes les permutations (ou bijections) de $E$ est notée

$$S_E.$$

On écrit $S_n := S_E$ dans le cas particulier où $E = \{1, 2, 3, \ldots, n\}$.

Si $f_1$ et $f_2 \in S_E$, alors la composition $f_1 \circ f_2$, définie par $(f_1 \circ f_2)(x) := f_1(f_2(x))$, est aussi un élément de $S_E$. La règle d'associativité est satisfaite :

$$(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3),$$

pour chaque $f_1, f_2, f_3 \in S_E$. Preuve :

$$\begin{aligned}((f_1 \circ f_2) \circ f_3)(x) &= ((f_1 \circ f_2)(f_3(x)) \\ &= f_1(f_2(f_3(x))) \\ &= f_1((f_2 \circ f_3)(x)) \\ &= (f_1 \circ (f_2 \circ f_3))(x)\end{aligned}$$

pour chaque $x \in E$ ; d'où le résultat.

La paire $(S_E, \circ)$ est appelée le *groupe symétrique* sur $E$.

*Exercice* 2.1. La cardinalité de $S_n$ est $n!$.

*Exercice* 2.2. Si $\beta : E \to F$ est une bijection entre deux ensembles, trouver un isomorphisme entre $S_E$ et $S_F$. Combien d'isomorphismes différents existent-t-ils entre $S_E$ et $S_F$ si $E$ et $F$ ont 2 ou 3 éléments ?

*Exercice* 2.3. (i) Le groupe diédral $D_3$ et le groupe symétrique $S_3$ sont isomorphes. (ii) Pour quels $n \geq 4$ les groupes $D_n$ et $S_n$ sont-ils isomorphes ?

Une permutation $f \in S_E$ est connue si (et seulement si) l'image de chaque élément de $E$ est connue. Si $E = \{a, b, \ldots, z\}$ est un ensemble fini, on peut donner toutes les images de $f$ dans un tableau

$$f = \begin{pmatrix} a & b & \ldots & z \\ f(a) & f(b) & \ldots & f(z) \end{pmatrix}.$$

Par exemple, si $E = \{1, 2, 3, 4, 5\}$, alors

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 2 & 3 & 1 & 4 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 2 & 3 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

est l'application $f : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ où

$$f(1) = 2,\ f(2) = 3,\ f(3) = 4,\ f(4) = 1 \ \text{ et } \ f(5) = 5.$$

Il y a une application inverse pour $f$, donc $f$ et $f^{-1} \in S_E = S_5$. On obtient l'inverse $f^{-1}$ de $f$ en changeant les deux lignes dans un tableau de $f$ :

$$f^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 3 & 4 & 2 & 1 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}.$$

Soit maintenant

$$g := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$$

alors la composition est

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} = g \circ f.$$

(Vérifier ! On va de droite à gauche.)

Une permutation $f : E \to E$ est dite *cyclique* d'ordre $m$, ou un $m$-cycle, s'ils existent $m$ éléments différents $x_1, x_2, \ldots, x_m \in E$ tels que $f(x_i) = x_{i+1}$, pour $1 \leq i < m$, $f(x_m) = x_1$ et $f(x) = x$ pour chaque autre $x \in E$ (si $x \in E \backslash \{x_1, \ldots, x_m\}$). Et on écrit $f = (x_1, x_2, \ldots, x_m)$.

*Exercice* 2.4. On a $(x_1, x_2, \ldots, x_m) = (x_2, x_3, \ldots, x_m, x_1) \in S_E$.

On remarque que dans $S_5$ on a

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

mais

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

et

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

*Exercice* 2.5. Calculer dans $S_5$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \circ (1,2,3,4,5) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \circ (1,5) \circ (1,5,4) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}.$$

On dit que les cycles $(x_1, \ldots, x_m)$ et $(y_1, \ldots, y_k)$ sont *disjoints*, si $x_i \neq y_j$ pour chaque $i$ et $j$.

*Exercice* 2.6. Si les cycles $f = (x_1, \ldots, x_m)$ et $g = (y_1, \ldots, y_k)$ sont disjoints alors $f$ et $g$ commutent, c'est-à-dire $f \circ g = g \circ f$.

**Proposition 2.1.** *$E$ soit un ensemble non vide. Supposons que $f \in S_E$ est tel que l'ensemble $\{x \in E; f(x) \neq x\}$ est fini. Alors $f$ est une composition finie de cycles deux à deux disjoints.*

*En particulier, si la cardinalité de $E$ est finie, alors chaque permutation dans $S_E$ est une composition finie de cycles deux à deux disjoints.*

Par exemple, dans $S_9$ on a

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 5 & 6 & 4 & 3 & 1 & 2 & 9 \end{pmatrix} = (1,7) \circ (2,8) \circ (3,5,4,6) = (1,7) \circ (2,8) \circ (3,5,4,6) \circ (9).$$

*Démonstration.* On va procéder pas induction sur la cardinalité de l'ensemble $\{x \in E; f(x) \neq x\}$. Si c'est 0, alors $f$ est l'identité, qu'on peut écrire comme un 1-cycle $(e)$, pour n'importe quel $e \in E$.

Supposons que $f$ ne soit pas l'identité et soit $n$ la cardinalité de $Y := \{x \in E; f(x) \neq x\}$ (donc $n > 0$). Supposons enfin par hypothèse d'induction que, si $g \in S_E$ est tel que $|\{x \in E; g(x) \neq x\}| < n$, alors $g$ peut s'écrire comme une composition finie de cycles deux à deux disjoints.

Fixons $y \in Y$, c'est-à-dire, $f(y) \neq y$. D'abord $f(y) \in Y$ aussi, car sinon $f(f(y)) = f(y)$ et donc

$$f(y) = (f^{-1} \circ f)(f(y)) = f^{-1}(f(f(y))) = f^{-1}(f(y)) = y,$$

une contradiction.

Considérons la suite d'éléments de $Y$ :

$$y,\ f(y),\ f^2(y) := f(f(y)),\ f^3(y) := f(f(f(y))),\ \ldots$$

Ils existent $n_1 < n_2$ tels que $f^{n_1}(y) = f^{n_2}(y)$, car sinon l'ensemble $Y$ serait infini. Après la composition avec $(f^{-1})^{n_1}$, on obtient un entier positif $m\,(= n_2 - n_1)$ tel que $y = f^m(y)$. Choisissons un tel $m$ de façon minimale. Alors par l'argument précédent les éléments

$$y, f(y), f^2(y), \ldots, f^{m-1}(y)$$

sont tous différents et font partie de $Y$, donc $m \leq n$.

Définissons le $m$-cycle $\sigma := (y, f(y), f^2(y), \ldots, f^{m-1}(y))$ et posons $h := f \circ \sigma^{-1}$. Alors $f = h \circ \sigma$ et, pour notre élément $y$ fixé, on a $\sigma(y) = f(y)$. Nous allons montrer que $\{x \in E; h(x) \neq x\}$ est un sous-ensemble inclus dans $Y$ mais strictement plus petit que lui.

Si $x \notin Y$, alors $f(x) = x$ et $x$ n'est pas un des éléments de $\{y, f(y), f^2(y), \ldots, f^{m-1}(y)\}$, donc $\sigma(x) = x$ et $\sigma^{-1}(x) = x$. On conclut que $h(x) = x$. Il suit que $\{x \in E; h(x) \neq x\} \subseteq Y$. Par contre, $f(y) \in Y$, pour notre élément fixé $y$ :

$$h(f(y)) = (f \circ \sigma^{-1})(f(y)) = (f \circ \sigma^{-1})(\sigma(y)) = f(\sigma^{-1}(\sigma(y))) = f(y).$$

De même façon $h(f^i(y)) = f^i(y)$ pour $0 \leq i \leq m$. On conclut que $\{x \in E; h(x) \neq x\}$ est un sous-ensemble inclus dans $Y$ mais strictement plus petit que lui.

Il est possible que $h$ soit l'identité. Dans ce cas $f = \sigma$ est un $m$-cycle. Supposons $h$ ne soit pas l'identité. Alors, on peut utiliser l'hypothèse d'induction et conclure que $h$ peut s'écrire comme un produit de cycles deux à deux disjoints, disons $h = \sigma_1 \circ \sigma_2 \ldots \circ \sigma_s$. On peut supposer que chaque cycle utilisé est de longueur $> 1$ (car on peut éliminer les 1-cycles et il restera au moins un cycle, car $h$ n'est pas l'identité). Si $x$ est utilisé dans un des cycles, alors $h(x) \neq x$ (pourquoi ?) et donc $x$ n'est pas de la forme $f^i(y)$ pour $0 \leq i < m$. Donc aussi les cycles $\sigma_j$ et $\sigma$ sont disjoints.

Alors $f = \sigma_1 \circ \sigma_2 \ldots \circ \sigma_s \circ \sigma$ est une composition finie de cycles deux à deux disjoints. □

*Exercice* 2.7. Soit $f = (x_1, x_2, \ldots, x_m)$ un $m$-cycle et $g \in S_E$. Montrer que $g \circ f \circ (g^{-1})$ est le $m$-cycle $(y_1, y_2, \ldots, y_m)$ avec $y_i := g(x_i)$.

Par exemple, si $f = (1,4,3)$ et $g = (1,2) \circ (3,4,5)$ dans $S_9$, alors

$$g \circ f \circ g^{-1} = (g(1), g(4), g(3)) = (2,5,4).$$

*Exercice* 2.8. Chaque permutation $f \in S_n$ est un produit de 2-cycles de la forme $(i, i+1)$, où $1 \leq i < n$. Par exemple,

$$(1,2,3,4,5,6,7,8) = (1,2) \circ (2,3) \circ (3,4) \circ (4,5) \circ (5,6) \circ (6,7) \circ (7,8) \text{ et } (1,3) = (2,3) \circ (1,2) \circ (2,3).$$

2.2. **Matrices de permutation.** Prenons $E := \{1, 2, \ldots n\}$. Nous allons associer à chaque permutation une matrice $n \times n$ à coefficients réels (ou à coefficients dans un autre corps comme $\mathbb{C}$, $\mathbb{Q}$ ou $\mathbb{F}_q$, voir plus loin). Si $f \in S_n$, alors la matrice $L_f$ est définie comme $(L_f)_{ji} = 1$ si $j = f(i)$ et $(L_f)_{ji} = 0$ si $j \neq f(i)$, pour $i, j \in E$. La matrice $L_f$ est appelée la *matrice de permutation* associée à la permutation $f$. Soit

$$e_1 := \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 := \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_3 := \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n := \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

la base naturelle de l'espace vectoriel $\mathbb{R}^n$ des vecteurs colonnes. La matrice $L_f$ est aussi déterminée par la propriété

$$L_f e_i = e_{f(i)}$$

pour $i \in E$. Si $f, g \in S_n$, alors

$$(L_f L_g) e_i = L_f e_{g(i)} = e_{f(g(i))} = e_{(f \circ g)(i)} = L_{f \circ g} e_i,$$

pour chaque $i \in E$. Donc $L_f L_g = L_{f \circ g}$ ; ceci veut dire le produit des deux matrices de permutation $f$ et $g$ est la matrice de permutation associée à la composition $f \circ g$. Il suit que l'application

$$L : S_n \to \mathrm{GL}(n, \mathbb{R}); \; L(f) := L_f$$

est un homomorphisme de groupes.

*Exemple* 2.1. Pour $n = 3$.

$$L_{(1,2,3)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, L_{(1,2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, L_{(2,3)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

et en effet $L_{(1,2,3)} = L_{(1,2)} L_{(2,3)}$.

On peut identifier l'ensemble des matrices $\{L_f \mid f \in S_n\}$ comme l'ensemble des matrices $n \times n$ ayant un et un seul coefficient 1 dans chacune de ses lignes et colonnes, ses autres coefficients étant 0. Notons cet ensemble de matrices par $P_n$.

**Lemme 2.1.** *Le déterminant de $L \in P_n$ est 1 ou $-1$.*

*Démonstration.* Après une permutation des lignes de $L$, on obtient la matrice identité ayant déterminant 1. □

On définit le *signe* $\mathrm{sg}(f)$ d'un élément de $S_n$ comme le déterminant de sa matrice de permutation $L_f$.

**Lemme 2.2.** *On a* $\mathrm{sg}(f)\mathrm{sg}(g) = \mathrm{sg}(f \circ g)$ *pour* $f, g \in S_n$.

*Démonstration.* On a $L_{f\circ g} = L_f L_g$ et $\det(L_{f\circ g}) = \det(L_f L_g) = \det(L_f)\det(L_g)$. □

Donc le signe est aussi un homomorphisme de groupes. Les permutations de signe $+1$ sont appelées *paires* et ceux de signe $-1$ sont appelées *impaires*.

*Exercice* 2.9. Soit $f$ est un produit d'un certain nombre de permutations cycliques, dont $n_m$ sont de longueur $m$, où $m = 1, 2, \ldots$ Mettons $N := \sum_m n_m(m-1)$. Montrer que $\mathrm{sg}(f) = (-1)^N$.

*Exercice* 2.10. Il pourrait exister un problème logique avec cette définition du signe à l'aide du déterminant, dépendant de la définition du déterminant adoptée ! Pour cette raison nous donnons une définition alternative du sg.

Considérons l'ensemble $\mathbb{R}[x_1, \ldots, x_n]$ de tous les polynômes $F(x_1, \ldots, x_n)$ en les variables $x_1, \ldots, x_n$ et à coefficients réels. Pour une permutation $\pi \in S_n$ et un polynôme $F$, on définit un autre polynôme $\pi * F$ par :

$$(\pi * F)(x_1, x_2, \ldots, x_n) := F(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)});$$

c'est-à-dire, on remplace la variable $x_i$ par le variable $x_{\pi(i)}$. Par exemple, si $F = x_1^2 + 7x_2x_3$ on a

$$(1,2)*F = x_2^2+7x_1x_3; (1,3,2)*F = x_3^2+7x_1x_2; (2,3)*[(1,2)*F] = (2,3)*(x_2^2+7x_1x_3) = x_3^2+7x_1x_2.$$

(i) Montrer que

$$\pi_1 * [\pi_2 * F] = (\pi_1 \circ \pi_2) * F,$$

pour chaque $F \in \mathbb{R}[x_1, \ldots, x_n]$ et $\pi_1, \pi_2 \in S_n$.

(ii) Fixons le polynôme $\Delta := \prod_{1\le i<j\le n}(x_i - x_j)$. Montrer que pour chaque $\pi \in S_n$, il existe un signe $\epsilon(\pi) \in \{1, -1\}$ tel que

$$\pi * \Delta = \epsilon(\pi)\Delta.$$

(En fait, $\epsilon(\pi) = (-1)^{\ell(\pi)}$, où $\ell(\pi)$ est le nombre de paires $i < j$ telles que $\pi(i) > \pi(j)$ (appelé *inversion*).)

(iii) Montrer que

$$\epsilon : S_n \to \{1, -1\} : \pi \mapsto \epsilon(\pi)$$

est un homomorphisme de groupes.

(iv) Montrer que $\mathrm{sg} = \epsilon$. [Puisque les 2-cycles $(i, i+1)$ (où $1 \le i < n$) engendrent $S_n$, il suffit de montrer $\mathrm{sg}((i, i+1)) = \epsilon((i, i+i)) = -1$.]

*Exercice* 2.11. Une permutation $f$ de $S_n$ est paire si et seulement si $f$ est la composition d'un nombre pair de 2-cycles. Une permutation $f$ est paire si et seulement si $f$ est la composition d'un nombre de 3-cycles.

Les permutations paires

$$\mathrm{Alt}_n := \{f \in S_n;\ \mathrm{sg}(f) = 1\}$$

avec, comme opération interne, la composition $\circ$ des permutations forment un groupe : le groupe *alterné* d'ordre $n$. C'est le noyau de l'homomorphisme sg.

*Exercice* 2.12. La cardinalité du groupe alterné $\mathrm{Alt}_n$ est $n!/2$.

## 3. Corps et groupes linéaires

Pour être capable de donner encore plus d'exemples de groupes, il faut introduire la notion de corps (*field*, en anglais). On a vu sa définition très vite en algèbre linéaire, mais pas beaucoup de ses propriétés. L'essentiel est qu'on peut faire de l'algèbre linéaire sur un corps quelconque.

Par définition, un corps est un ensemble $\mathbb{K}$ muni de deux opérations internes commutatives fixées, notées $+$ et $\cdot$, satisfaisant plusieurs axiomes.

Premièrement, la paire $(\mathbb{K}, +)$ doit être un groupe abélien ; le neutre pour l'opération $+$ est noté $\mathbf{0}$ et l'inverse de $x$ est $-x$.

Puis, la paire $(\mathbb{K}, \cdot)$ doit être un monoïde commutatif, le neutre étant noté $\mathbf{1}$.

Les deux éléments particuliers $\mathbf{0}$ et $\mathbf{1}$ doivent être distincts.

Chaque élément $k \neq \mathbf{0}$ dans $\mathbb{K}$ est supposé avoir un inverse pour l'opération $\cdot$, noté $x^{-1}$.

Finalement, les deux opérations internes soient liées par la loi de la distributivité :

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

pour chaque $x, y, z \in \mathbb{K}$.

La convention est que dans une formule $\cdot$ a une priorité plus élevée que $+$, par exemple

$$x + y \cdot z + t := x + (y \cdot z) + t, \text{ et } x \cdot y + z \cdot t := (x \cdot y) + (z \cdot t).$$

Aussi on supprime souvent le symbole $\cdot$, par exemple

$$xyz + t := x \cdot y \cdot z + t.$$

Ici $x, y, z, t \in \mathbb{K}$.

Comme pour chaque groupe additif $nk$ est définie pour chaque entier $n$ et chaque $k \in \mathbb{K}$. Mais $\mathbb{Z}$ n'est pas nécessairement un sous-ensemble de $\mathbb{K}$ ! Les exemples de corps les plus familiers sont les rationnels $\mathbb{Q}$, les réels $\mathbb{R}$ et les complexes $\mathbb{C}$. Les ensembles d'entiers $\mathbb{N}$ et $\mathbb{Z}$ ne sont pas des corps puisque leurs éléments n'ont pas tous un inverse multiplicatif.

*Exercice* 3.1. Soit $N \geq 1$ un nombre naturel. Définissons

$$\mathbb{Q}(\sqrt{N}) := \{a + b\sqrt{N}; a, b \in \mathbb{Q}\} \subset \mathbb{R}.$$

Montrer que $\mathbb{Q}(\sqrt{N})$ est un corps, avec les opérations $+$ et $\cdot$ induites par celles de $\mathbb{R}$. Attention : est-ce que l'ensemble $\mathbb{Q}(\sqrt{N})$ contient l'inverse (multiplicatif) de tous ses éléments non nuls ?

Le plus petit corps contient seulement deux éléments et est noté $\mathbb{F}_2$. Les deux éléments sont appelés $\mathbf{0}$ et $\mathbf{1}$ et on a

$$\mathbf{0} = \mathbf{0} + \mathbf{0} = \mathbf{1} + \mathbf{1} = \mathbf{0} \cdot \mathbf{0} = \mathbf{0} \cdot \mathbf{1} = \mathbf{1} \cdot \mathbf{0}$$

et

$$\mathbf{1} = \mathbf{0} + \mathbf{1} = \mathbf{1} + \mathbf{0} = \mathbf{1} \cdot \mathbf{1}.$$

Il est utile de penser à $\mathbf{0}$ comme « pair » et à $\mathbf{1}$ comme « impair », par exemple $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$ est interprété comme « impair fois impair égale impair ». Ainsi les calculs se font « modulo 2 ». En fait, $\mathbb{F}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ (comme si on tenait le temps avec une montre à deux heures), avec les opérations comme dans le petit cours d'arithmétique (voir section 0.8).

Il existe aussi un corps de trois éléments $\mathbb{F}_3 = \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}$. Les tableaux des deux opérations internes sont :

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ |
|---|---|---|---|
| $\mathbf{0}$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ |
| $\mathbf{1}$ | $\mathbf{1}$ | $\mathbf{2}$ | $\mathbf{0}$ |
| $\mathbf{2}$ | $\mathbf{2}$ | $\mathbf{0}$ | $\mathbf{1}$ |

et

| $\cdot$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ |
|---|---|---|---|
| $\mathbf{0}$ | $\mathbf{0}$ | $\mathbf{0}$ | $\mathbf{0}$ |
| $\mathbf{1}$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ |
| $\mathbf{2}$ | $\mathbf{0}$ | $\mathbf{2}$ | $\mathbf{1}$ |

Il est donc naturel ici d'adopter le symbole « $\mathbf{2}$ » parce que $2\mathbf{1} = \mathbf{1} + \mathbf{1} = \mathbf{2}$. Mais $\mathbf{2} + \mathbf{1} = \mathbf{0}$. On calcule « modulo 3 »et $\mathbb{F}_3 \simeq \mathbb{Z}/3\mathbb{Z}$. (Exercice : quel est l'inverse additif de $\mathbf{2}$ ? Et son inverse multiplicatif ?)

Il existe un corps de quatre éléments $\mathbb{F}_4 = \{\mathbf{0}, \mathbf{1}, a, b\}$. Les tableaux des opérations internes sont :

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $a$ | $b$ |
|---|---|---|---|---|
| $\mathbf{0}$ | $\mathbf{0}$ | $\mathbf{1}$ | $a$ | $b$ |
| $\mathbf{1}$ | $\mathbf{1}$ | $\mathbf{0}$ | $b$ | $a$ |
| $a$ | $a$ | $b$ | $\mathbf{0}$ | $\mathbf{1}$ |
| $b$ | $b$ | $a$ | $\mathbf{1}$ | $\mathbf{0}$ |

et

| $\cdot$ | $\mathbf{0}$ | $\mathbf{1}$ | $a$ | $b$ |
|---|---|---|---|---|
| $\mathbf{0}$ | $\mathbf{0}$ | $\mathbf{0}$ | $\mathbf{0}$ | $\mathbf{0}$ |
| $\mathbf{1}$ | $\mathbf{0}$ | $\mathbf{1}$ | $a$ | $b$ |
| $a$ | $\mathbf{0}$ | $a$ | $b$ | $\mathbf{1}$ |
| $b$ | $\mathbf{0}$ | $b$ | $\mathbf{1}$ | $a$ |

Maintenant il n'y a pas de sens à adopter le symbole $\mathbf{2}$ à la place de $a$ ou $b$, parce que $2\cdot\mathbf{1} = \mathbf{1}+\mathbf{1} = \mathbf{0}$ et donc $2\cdot\mathbf{1}$ n'est pas un nouvel élément. Pour chaque élément $x$ de $\mathbb{F}_4$ on a $2x = x+x = \mathbf{0}$. L'élément $a$ satisfait l'égalité $a^2 + a + 1 = 0$ et, tout compte fait, on n'a pas vraiment besoin d'un symbole $b$ puisque $b = a^2 = a + 1$. Notons que $\mathbb{F}_4 \not\simeq \mathbb{Z}/4\mathbb{Z}$ !

*Exercice* 3.2. Calculer le déterminant des matrices

$$\begin{pmatrix} a & a & \mathbf{1} \\ \mathbf{1} & b & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & a \end{pmatrix}, \quad \begin{pmatrix} a & b & \mathbf{1} \\ \mathbf{1} & b & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & a \end{pmatrix}, \quad \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} \\ x & y & z \\ x^2 & y^2 & z^2 \end{pmatrix}$$

de coefficients dans le corps $\mathbb{F}_4$, pour n'importe quels $x, y, z$. Et ses inverses ?

*Exercice* 3.3. Vérifier que $\mathbb{F}_2$, $\mathbb{F}_3$ et $\mathbb{F}_4$ sont des corps. Trouver un corps de 5 éléments. Essayer de montrer qu'il n'existe pas un corps de 6 éléments. (Indice : On a $6\mathbf{1} = \mathbf{0}$ et soit $2\mathbf{1} \neq \mathbf{0}$ ou $3\mathbf{1} \neq \mathbf{0}$, contradiction.)

En fait, on peut montrer que la cardinalité d'un corps fini est toujours une puissance d'un nombre premier et il existe un unique corps fini $\mathbb{F}_q$ de la cardinalité $q = p^m$, où $p$ est un nombre premier et $m$ un entier positif. Nous ne montrons pas ces propositions ici (voyez par exemple [4, p.277–8]).

Si $\mathbb{K}$ est un corps, on indique le groupe multiplicatif par $\mathbb{K}^\times$ ; c'est alors l'ensemble $\mathbb{K}\backslash\{\mathbf{0}\}$ et l'opération interne est le produit $\cdot$.

Dès qu'on fixe un corps $\mathbb{K}$, on peut définir la notion d'espace linéaire et application linéaire sur $\mathbb{K}$ ; des matrices avec coefficients dans $\mathbb{K}$ ; l'addition et la multiplication matricielle ; le déterminant d'une matrice sera un élément de $\mathbb{K}$ ; le rang ; l'inverse ; l'existence d'inverse si et seulement si le déterminant n'est pas $\mathbf{0}$ ; les formes bilinéaires symétriques ; le groupe $\mathrm{GL}(n, \mathbb{K})$ ; le groupe $\mathrm{SL}(n, \mathbb{K})$ ; le groupe orthogonal $\mathrm{O}(n, \mathbb{K})$ ; $\mathrm{SO}(n, \mathbb{K})$, et cetera.

Mais la partie de l'algèbre linéaire qui utilise la relation d'ordre $\leq$ , comme « un produit scalaire défini positif », ne se généralise pas trivialement pour tous les corps.

Si le corps est fini, les groupes linéaires sont aussi finis. Le groupe $\mathrm{GL}(n, \mathbb{F}_q)$ est l'ensemble des matrices inversibles $n \times n$ dont les éléments appartiennent à $\mathbb{F}_q$. Sa loi de groupe est la multiplication matricielle usuelle et son ordre est $(q^n - 1)(q^n - q)(q^n - q^2) \ldots (q^n - q^{n-1})$. (Preuve : La première colonne d'un élément de $\mathrm{GL}(n, \mathbb{F}_q)$ peut être spécifiée par le choix de $n$ éléments dans $\mathbb{F}_q$. Il y a donc $q^n$ choix desquels on doit retirer le vecteur nul : il y a donc $q^n - 1$ choix pour cette première colonne. À nouveau il y a $q^n$ choix pour la seconde desquels on doit retirer les vecteurs linéairement dépendants de la première colonne, c'est-à-dire les multiples de cette première colonne. Ces multiples sont au nombre de $q$ et il y a donc $q^n - q$ choix pour la seconde colonne. Pour la $i$-ième colonne, il y aura toujours $q^n$ choix, les combinaisons linéraires des $i - 1$ colonnes précédentes sont décrites par les poids devant chacune des $i - 1$ colonnes précédentes et il y en a donc $q^{i-1}$. Le résultat suit.)

*Exercice* 3.4. Soit $g$ un élément du groupe orthogonal sur $\mathbb{F}_2$ :

$$\mathrm{O}(4, \mathbb{F}_2) = \{g \in \mathrm{GL}(4, \mathbb{F}_2);\ g \cdot g^t = 1\}.$$

Montrer qu'il y a deux possibilités. Soit chaque ligne et chaque colonne de $g$ contient un unique coefficient $\mathbf{1}$ (une matrice de permutation), soit chaque ligne et chaque colonne de $g$ contient un unique coefficient $\mathbf{0}$. Est-ce vrai également pour $\mathrm{O}(5, \mathbb{F}_2)$ ou $\mathrm{O}(4, \mathbb{F}_3)$ ? Montrer que $\mathrm{O}(3, \mathbb{F}_2)$ est isomorphe à $S_3$.

*Exercice* 3.5. Pour un corps $\mathbb{K}$ nous posons $\mathbb{K}[T]$ pour l'ensemble des polynômes en la variable $T$ et à coefficients dans $\mathbb{K}$. La notion de degré est l'usuelle (le plus grand exposant de $T$ qui y apparaît). Montrer qu'on peut diviser avec reste, c'est-à-dire : donnés $f$ et $g$ deux polynômes dans $\mathbb{K}[T]$, où $g \neq 0$, il existe deux polynômes $q$ et $r$ dans $\mathbb{K}[T]$ tels que

$$f = qg + r$$

et, si $r \neq 0$, le degré de $r$ est plus petit que le degré de $g$.

*Exercice* 3.6. Comme dans le petit cours d'arithmétique donner une définition du $\mathrm{pgcd}(f, g)$ et montrer qu'il existe deux polynômes $a$ et $b$ tels que

$$af + bg = \mathrm{pgcd}(f, g).$$

On peut généraliser d'autres propriétés des polynômes à coefficients réels. Comme la factorisation unique (la notion de « nombre premier » est remplacée par « polynôme irréductible »). De plus chaque polynôme de degré $n$ a au plus $n$ solutions dans un corps. Nous en donnons une preuve.

**Proposition 3.1.** *Soit $F(T) = a_0 + a_1 T + a_1 T^2 + \ldots + a_n T^n$ un polynôme de degré $n$ de coefficients $a_i$ dans un corps $\mathbb{K}$ et on suppose que $a_n \neq \mathbf{0}$. Alors $F$ a au plus $n$ racines, c'est-à-dire, il existe au plus $n$ éléments différents $k \in \mathbb{K}$ tels que*

$$F(k) := a_0 + a_1 k + a_1 k^2 + \ldots + a_n k^n = \mathbf{0}$$

*dans $\mathbb{K}$.*

*Démonstration.* Par induction sur $n$. Si $n = 0$, il n'y a aucune racine (parce que $a_0 \neq \mathbf{0}$). Supposons $k \in \mathbb{K}$ est une solution. Par la division avec reste (exercice 3.5) il existe un polynôme $G(T)$ de

degré $n-1$ et un scalaire $c \in \mathbb{K}$, tels que $F(T) = (T-k)G(T) + c$. Donc $c = F(k) = 0$ et $F(T) = (T-k)G(T)$. Soit $k'$ une solution de $F(T) = (T-k)G(T) = \mathbf{0}$, alors $k' - k = \mathbf{0}$ où $G(k') = \mathbf{0}$. Par induction on peut supposer que $G(T) = \mathbf{0}$ a au plus $n-1$ solutions différents dans $\mathbb{K}$, donc $F(T) = \mathbf{0}$ a au plus $n$ solutions distinctes dans $\mathbb{K}$. $\square$

L'équation $2x = 0$ a une solution dans un corps, mais deux dans $\mathbb{Z}/4\mathbb{Z}$.

*Exercice* 3.7. Trouver tous les zéros de $F(T) := T^6 + aT^5 + bT^4 + \mathbf{1}$ dans le corps $\mathbb{F}_4$. Et les zéros de $F'(T)$ (la dérivée du polynôme $F$) ?

*Exercice* 3.8. Soit $a, b, c, d \in \mathbb{F}$ où $\mathbb{F}$ est un corps quelconque. Si $ad - bc \neq 0$ dans $\mathbb{F}$, alors l'inverse de $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est-il donné par

$$\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}?$$

*Exercice* 3.9. (i) Montrer qu'il n'y a pas de solution à l'équation $x^2 + x + 1 = 0$ dans $\mathbb{F}_2$
(ii) ni à l'équation $x^3 + 2x + 1 = 0$ dans $\mathbb{F}_3$,
(iii) mais qu'il y en plus d'une à $x^2 + x + 1 = 0$ dans $\mathbb{F}_4$.
Attention : si le corps est fini, il est possible de vérifier si chacun des éléments du corps vérifie l'équation proposée.

*Exercice* 3.10. Soit

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

une matrice sur le corps $\mathbb{F}$ et où 0 et 1 dénotent le neutre pour $+$ et $\times$ respectivement. Calculer $\det A$ pour (i) $\mathbb{F} = \mathbb{Q}$, (ii) $\mathbb{F} = \mathbb{F}_2$ et (iii) $\mathbb{F} = \mathbb{F}_3$.

*Exercice* 3.11. (i) Énumérer *tous* les vecteurs de l'espace vectoriel $\mathbb{F}_2^3$ des vecteurs à trois composantes sur le corps $\mathbb{F}_2$. Attention : il y en a un nombre fini !
(ii) Soit $p$ un nombre premier. Combien de vecteurs contient l'espace vectoriel $\mathbb{F}_p^2$ sur le corps $\mathbb{F}_p$ ?
(iii) Quelle est la dimension de l'espace vectoriel $\mathbb{F}_p^2$ ? Attention : pour répondre à cette question, il est impératif de revoir les définitions de dimension et de base vues dans le cours d'algèbre linéaire.

*Exercice* 3.12. (i) Résoudre, sur $\mathbb{F}_2$, le système linéaire

$$x + y = 0 \qquad \text{et} \qquad y = 1.$$

(ii) Résoudre sur $\mathbb{F}_3$ le système

$$\begin{aligned} x \qquad\quad + z &= 0 \\ x + y \qquad\quad &= 1 \\ y + z &= 2. \end{aligned}$$

*Exercice* 3.13. (i) Montrer que le produit de matrices triangulaires supérieures et l'inverse d'une matrice triangulaire supérieure inversible sont triangulaire supérieures. Attention : pour l'inverse, se remémorer l'algorithme pour calculer l'inverse par équivalence-ligne : $(A \mid I) \sim (I \mid A^{-1})$.

(ii) L'ensemble $\mathrm{B}(n, \mathbb{F})$ des matrices triangulaires supérieures inversibles dont les éléments de matrices sont dans $\mathbb{F}$ forme un groupe.
(iii) Combien d'éléments contient $\mathrm{B}(3, \mathbb{F}_2)$ ? et $\mathrm{B}(2, \mathbb{F}_3)$ ? et $\mathrm{B}(n, \mathbb{F}_p)$ si $p$ est premier ?

## 4. Sous-groupes et théorème de Lagrange

4.1. **Sous-groupes.** Considérons le sous-ensemble des permutations

$$V_4 := \{(1), (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3)\}$$

de $S_4$. On voit que $V_4$ a la propriété remarquable que la composition de deux de ses éléments est encore un élément de $V_4$. De plus les inverses de chacun des éléments de $V_4$ appartiennent à $V_4$. Alors $(V_4, \circ)$ est soi-même un groupe ; on dit que $V_4$ est un sous-groupe de $S_4$ et on note $V_4 < S_4$. Ce groupe est appelé *le quatre-groupe de Klein*[5] (c'est un groupe isomorphe au groupe $(\mathbb{F}_4, +)$). (L'expression « $n$-groupe $G$ » signifie que le groupe $G$ possède $n$ éléments.)

En général, on dit qu'un groupe $(H, \circ)$ est un *sous-groupe* d'un groupe $(G, *)$ si $H \subseteq G$ et

$$h_1 \circ h_2 = h_1 * h_2$$

pour chaque $h_1$ et $h_2 \in H$. Ici $h_1 * h_2$ a un sens, parce que $H \subseteq G$. Une autre manière de dire la même chose est que $(H, \circ)$ est un sous-groupe de $(G, *)$ si et seulement si l'application induite par l'inclusion

$$H \subseteq G : \ h \mapsto h$$

est un homomorphisme de groupes.

Presque toujours on adopte les même symboles pour les deux opérations, celles sur $H$ et sur $G$, et on écrit

$$H < G.$$

Noter que $(\{1, -1\}, \cdot)$ est un sous-groupe de $(\mathbb{Q}^\times, \cdot)$, mais pas un sous-groupe de $(\mathbb{Z}, +)$.

*Exercice* 4.1. Existe-t-il un sous-groupe de $(\mathbb{Z}, +)$ isomorphe au sous-groupe $(\{+1, -1\}, \cdot)$ de $(\mathbb{Z}^\times, \cdot)$ ?

Soit $H < G$ un sous-groupe. A priori on a deux neutres ($\mathbf{1}_H$ et $\mathbf{1}_G$) et a priori chaque $h \in H$ a deux inverses (l'un dans le groupe $H$ et l'autre dans le groupe $G$). Heureusement, nous pouvons montrer que les deux neutres sont le même élément et les deux inverses sont égaux aussi. Alors il n'y a pas de confusion à parler du neutre ou de l'inverse d'un élément $h$.

**Lemme 4.1.** *Soit $(H, \circ)$ un sous-groupe de $(G, *)$. Alors les neutres $\mathbf{1}_H$ de $H$ et $\mathbf{1}_G$ de $G$ coïncident. Soit $h$ un élément de $H$, $k$ son inverse dans $H$ et $y$ son inverse dans $G$. Ces deux inverses $k$ et $y$ coïncident.*

*Démonstration.* On a $\mathbf{1}_H = \mathbf{1}_H \circ \mathbf{1}_H = \mathbf{1}_H * \mathbf{1}_H$, parce que $H < G$. Soit $x \in G$ l'inverse de $\mathbf{1}_H$ dans le groupe $G$, alors

$$\mathbf{1}_G = x * \mathbf{1}_H = x * (\mathbf{1}_H * \mathbf{1}_H) = (x * \mathbf{1}_H) * \mathbf{1}_H = \mathbf{1}_G * \mathbf{1}_H = \mathbf{1}_H,$$

parce que $\mathbf{1}_G$ est le neutre de $G$. Donc les neutres coïncident. Si $k \in H$ est l'inverse de $h \in H$, alors $h \circ k = k \circ h = \mathbf{1}_H$. Donc on a aussi que $h * k = k * h = \mathbf{1}_G$ et il suit que $k$ est l'inverse de $h$ dans $G$. □

5. Felix Klein, mathématicien allemand, 1849–1925.

Noter que lemme 1.3 donne aussi une preuve du lemme ci-dessus.

Supposons $H$ est un sous-ensemble d'un groupe $G$ avec l'opération interne $\circ$. Il est naturel de se demander si $H$ avec la même opération forme un sous-groupe. Pour cela, il faut au moins que $H \circ H \subseteq H$, c'est-à-dire $h_1 \circ h_2 \in H$ pour chaque $h_1, h_2 \in H$. Si ce n'est pas le cas, alors $\circ$ n'est pas une opération interne sur $H$ et $H$ n'est même pas un groupe. Cependant, si cela est le cas, l'associativité est immédiate et $(H, \circ)$ est alors un demi-groupe. Si la cardinalité de $H$ est finie et $H$ n'est pas vide, $(H, \circ)$ est automatiquement un groupe, comme l'exercice suivant le démontre.

*Exercice* 4.2. Supposons $H \subseteq G$ est un sous-ensemble non-vide de cardinalité finie d'un groupe quelconque $(G, \circ)$, tel que $H \circ H \subseteq H$. Alors $(H, \circ)$ est un sous-groupe de $(G, \circ)$.

Mais si la cardinalité de $H$ n'est pas finie, alors $(H, \circ)$ n'est pas nécessairement un sous-groupe même si $H \circ H \subseteq H$. Par exemple, si $(G, \circ) = (\mathbb{R}^\times, \cdot)$ est le groupe multiplicatif des nombres réels et $H$ est le sous-ensemble de tous les nombres dont la valeur absolue est plus grande que 1 :

$$H = \{x \in \mathbb{R};\ |x| > 1\}.$$

Dans ce cas $H \cdot H \subseteq H$, mais $(H, \cdot)$ n'est pas un groupe. Alors il faut supposer plus.

**Proposition 4.1.** *Soit $H$ un sous-ensemble d'un groupe $(G, \circ)$. Alors $(H, \circ)$ est un sous-groupe de $(G, \circ)$ si et seulement si $H$ satisfait les trois propriétés suivantes.*

*(a) Pour chaque $h_1$ et $h_2$ de $H$ on a aussi $h_1 \circ h_2 \in H$.*

*(b) Le neutre $\mathbf{1}_G$ de $G$ est un élément de $H$, donc $\mathbf{1}_G \in H$.*

*(c) Pour chaque $h \in H$, l'inverse de $h$ dans $G$ est aussi dans $H$, donc $h^{-1} \in H$.*

*Démonstration.* Un sous-groupe satisfait les trois propriétés. Supposons que $H \subseteq G$ satisfait les propriétés. Alors $\circ$ définit une opération interne associative sur $H$, par (a) et parce que $\circ$ est une opération interne associative sur le groupe $G$. Le neutre $\mathbf{1}_G \in H$ est aussi un neutre pour $(H, \circ)$, parce que $\mathbf{1}_G \circ h = h \circ \mathbf{1}_G = h$ pour chaque $h \in H$ (par (b)). Et par (c) chaque $h^{-1} \in H$ et $h \circ h^{-1} = h^{-1} \circ h = \mathbf{1}_G$, donc chaque élément $h \in H$ a un inverse dans $(H, \circ)$. Ainsi $(H, \circ)$ est un groupe et donc un sous-groupe de $(G, \circ)$. $\square$

Il existe aussi un critère un peu plus court.

*Exercice* 4.3. Soit $H$ un sous-ensemble d'un groupe $(G, \circ)$. Alors $(H, \circ)$ est un sous-groupe de $(G, \circ)$ si et seulement si $H$ satisfait les deux propriétés suivantes.

(d) $H \neq \emptyset$ ($H$ n'est pas vide) et

(e) si $x, y \in H$, alors $x \circ y^{-1} \in H$.

*Exercice* 4.4. Énumérer tous les sous-groupes de $S_3$ et $D_4$ (les symétries d'un carré, ex. 1.7).

*Exemples* 4.1. Soit $\mathbb{K}$ un corps. L'ensemble de toutes les matrices $n \times n$ à coefficients dans $\mathbb{K}$, inversibles et triangulaires supérieures est noté $B(n, \mathbb{K})$. On dénote l'ensemble des matrices diagonales inversibles par $T(n, \mathbb{K})$ et l'ensemble des matrices triangulaires supérieures dont la seule valeur propre est $\mathbf{1} \in \mathbb{K}$ par $U(n, \mathbb{K})$. Ce groupe $U(n, \mathbb{K})$ est appelé le sous-groupe des matrices unipotentes. Alors

$$T(n, \mathbb{K}) < B(n, \mathbb{K}) < \mathrm{GL}(n, \mathbb{K}), \quad U(n, \mathbb{K}) < B(n, \mathbb{K}) \ \text{ et } \ U(n, \mathbb{K}) < \mathrm{SL}(n, \mathbb{K}) < \mathrm{GL}(n, \mathbb{K}).$$

Parfois on dit que $T(n,\mathbb{K})$ est le *sous-groupe (standard) de Cartan*[6] et $B(n,\mathbb{K})$ le *sous-groupe (standard) de Borel*[7] de $\mathrm{GL}(n,\mathbb{K})$.

L'ensemble $\mathrm{O}(n,\mathbb{K})$ de toutes les matrices $X$ $n\times n$ à coefficients dans $\mathbb{K}$ telles que $X\cdot X^t=\mathbf{1}$ est un sous-groupe de $\mathrm{GL}(n,\mathbb{K})$, appelé le *groupe orthogonal*.

L'ensemble $\mathbf{U}(n)$ de toutes les matrices complexes $X$ $n\times n$ telles que $X\cdot\overline{X}^t=\mathbf{1}$, c'est-à-dire de toutes les matrices unitaires, est un sous-groupe de $\mathrm{GL}(n,\mathbb{C})$, appelé le *groupe unitaire*. Ici, $\overline{X}$ est la matrice conjuguée complexe, c'est-à-dire $(\overline{X})_{ij}=\overline{X_{ij}}$.

*Exercice* 4.5. (i) Soit le sous-ensemble du groupe $GL(n+1,\mathbb{K})$ constitué des matrices de la forme $A=\left(\begin{smallmatrix} a & b\\ 0^t & c\end{smallmatrix}\right)$ où $a\in GL(n,\mathbb{K})$, $b\in\mathbb{K}^n$, $c\in\mathbb{K}^\times$ et $0$ dénote le vecteur nul de $\mathbb{K}^n$. Montrer que $A$ est un sous-groupe de $GL(n+1,\mathbb{K})$.
(ii) On considère maintenant le sous-groupe des matrices de la forme ci-dessus avec $c=1$. On dénote alors la matrice $A$ par la paire $(a,b)$. Montrer que la multiplication pour ce sous-groupe est $(a_2,b_2)\cdot(a_1,b_1)=(a_2a_1,a_2b_1+b_2)$.
(iii) Soit le sous-ensemble $G_{n,m}\subset GL(n+m,\mathbb{K})$ des matrices de la forme $B=\left(\begin{smallmatrix} a & b\\ 0^t & c\end{smallmatrix}\right)$ où $a\in GL(n,\mathbb{K})$, $b\in\mathbb{K}^{n\times m}$, $c\in GL(m,\mathbb{K})$ et où $0$ dénote maintenant la matrice nulle dans $\mathbb{K}^{m\times n}$. Est-ce que $G_{n,m}$ est un sous-groupe de $GL(n+m,\mathbb{K})$ pour tout $m,n>0$ ?

Un autre critère utile est que $H\subseteq G$ est un sous-groupe si et seulement si $H$ est l'image d'un homomorphisme dans $G$. Ceci suit de la proposition suivante.

**Proposition 4.2.** *L'image* $\operatorname{Im}\phi$ *d'un homomorphisme de groupes* $\phi:K\to G$ *est un sous-groupe de* $G$ *et le noyau* $\operatorname{Ker}\phi$ *est un sous-groupe de* $K$.

*Un sous-ensemble* $H\subseteq G$ *d'un groupe* $G$ *est un sous-groupe de* $G$ si et seulement si *il existe un homomorphisme de groupes* $\phi:K\to G$ *telle que* $H=\operatorname{Im}\phi$.

*Démonstration.* Nous allons utiliser le critère précédent. Clairement $\operatorname{Im}\phi$ n'est pas vide. Supposons $x,y\in\operatorname{Im}\phi$, alors il existe $a,b\in K$ tels que $\phi(a)=x$ et $\phi(b)=y$, alors

$$xy^{-1}=\phi(a)\phi(b)^{-1}=\phi(a)\phi(b^{-1})=\phi(a\circ b^{-1})\in\operatorname{Im}\phi.$$

(on a utilisé Lemme 1.3.) Donc $\operatorname{Im}\phi$ est un sous-groupe de $G$. La preuve que $\operatorname{Ker}\phi<K$ est analogue. La deuxième partie est évidente (n'est-ce pas ?). □

*Exercice* 4.6. Chaque monomorphisme $\phi:H\to G$ induit un isomorphisme entre $H$ et le sous-groupe $\operatorname{Im}\phi$ de $G$.

*Exemples* 4.2. L'ensemble de matrices $n\times n$ de permutation est un sous-groupe de $GL(n,\mathbb{R})$, parce que c'est l'image de $L:S_n\to\mathrm{GL}(n,\mathbb{R})$.

L'ensemble $\mathrm{SL}(n,K)$ de toutes les matrices de coefficients dans un corps $K$ et de déterminant $\mathbf{1}$ est un sous-groupe de $\mathrm{GL}(n,K)$, parce que c'est le noyau de l'homomorphisme $\det:GL(n,K)\to K^\times$.

Le groupe alterné $\mathrm{Alt}_n$ est un sous-groupe de $S_n$ parce que c'est le noyau de l'homomorphisme signe sg.

6. Élie Cartan, mathématicien français, 1869–1951.
7. Armand Borel, mathématicien suisse, 1923–2003.

*Exercice* 4.7. Montrer que le *centre*

$$Z(G) := \{g \in G;\ \forall x \in G : gx = xg\}$$

est un sous-groupe de $G$. (Utiliser le morphisme conjugaison $c : G \to \operatorname{Aut} G$. Voir l'exercice 1.16.)

**Lemme 4.2.** *Soit $G$ un groupe. Alors l'intersection d'une famille quelconque de sous-groupes de $G$ est aussi un sous-groupe de $G$.*

*Démonstration.* Cette intersection n'est pas vide, parce que $\mathbf{1}_G$ est dans chaque sous-groupe de $G$. Soient $x$ et $y$ dans l'intersection, donc $xy^{-1} \in H$ pour chaque sous-groupe $H$ de la famille de sous-groupes. Donc $xy^{-1}$ est dans l'intersection. Il suit que l'intersection est un sous-groupe de $G$. □

*Exemples* 4.3. En particulier, si $H < G$ et $K < G$ aussi $(H \cap K) < G$. On a aussi que si $H < K$ et $K < G$ alors $H < G$.

Alors $\mathrm{SO}(n, K) := \mathrm{SL}(n, K) \cap \mathrm{O}(n, K)$ est un sous-groupe de $\mathrm{GL}(n, K)$, de $\mathrm{SL}(n, K)$ et de $\mathrm{O}(n, K)$. Et $\mathrm{S}\mathbf{U}(n) := \mathrm{SL}(n, \mathbb{C}) \cap \mathbf{U}(n)$ est un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$, de $\mathrm{SL}(n, \mathbb{C})$ et de $\mathbf{U}(n)$.

*Exercice* 4.8. Montrer que

$$\mathrm{SO}(2, \mathbb{R}) = \left\{ \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} ; \phi \in \mathbb{R} \right\}$$

et

$$\mathrm{S}\mathbf{U}(2) = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} ;\ z, w \in \mathbb{C}, |z|^2 + |w|^2 = 1 \right\}.$$

Calculer $\mathrm{S}\mathbf{U}(n) \cap U(n, \mathbb{C})$ et $\mathrm{SO}(n, \mathbb{R}) \cap B(n, \mathbb{R})$. Calculer les centres de $\mathrm{GL}(n, \mathbb{C})$, $\mathrm{S}\mathbf{U}(n)$, $U(n, \mathbb{C})$, $C_n$ et $D_n$.

Il existe une manière facile de produire des sous-groupes du groupe orthogonal. Soit $F \subseteq \mathbb{R}^n$, par exemple un cube ou un tétraèdre dans $\mathbb{R}^3$. Alors

$$\{g \in \mathrm{O}(n, \mathbb{R});\ g(F) = F\}$$

est un sous-groupe de $\mathrm{O}(3, \mathbb{R})$. Ce sont des exemples de groupes de symétrie.

*Exercice* 4.9. Est-ce que les sous-ensembles suivants sont des sous-groupes de $\mathrm{GL}(n, \mathbb{R})$ ? (Attention : il faudra vérifier que *(a)* le neutre, *(b)* le produit de deux éléments du sous-ensemble et *(c)* l'inverse d'un élément du sous-ensemble appartiennent tous au sous-ensemble.)

(i) Les matrices de la forme $\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ dans $\mathrm{GL}(4, \mathbb{R})$.

(ii) Les matrices de la forme $\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \\ e & f & 1 & 0 \\ g & h & 0 & 1 \end{pmatrix}$ dans $\mathrm{GL}(4, \mathbb{R})$.

(iii) Les matrices de $\mathrm{GL}(n, \mathbb{R})$ dont les élément $m_{ij}$ sont nuls lorsque $i - j$ est un nombre impair. (Les diagonales non nulles alternent avec les nulles, la diagonale principale pouvant être non nulle.)

(iv) L'union des ensembles des matrices triangulaires supérieures et des triangulaires inférieures.

(v) Les rotations $\{\mathbf{1}, \rho, \rho^2, \ldots, \rho^{n-1}\}$ du groupe diédral $D_n$.

(vi) Les réflexions $\{\mathbf{1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}$ du groupe diédral $D_n$.

(vii) Le sous-ensemble des entiers pairs de $(\mathbb{Z}, +)$.

*Exercice* 4.10. À la section 2, deux homomorphismes ont été construits dont le domaine est le groupe symétrique : $L : S_n \to \mathrm{GL}(n, \mathbb{R})$ et $\mathrm{sg} : S_n \to \mathbb{R}^\times$. Identifier, pour ces deux homomorphismes, leurs noyau et image en précisant de quel groupe ils sont des sous-groupes.

*Exercice* 4.11. VRAI ou FAUX. Soit $H$ un sous-groupe de $G$.
(i) Si $G$ est abélien, $H$ est abélien.
(ii) Si $G$ est non abélien, $H$ est non abélien.
(iii) L'ordre d'un élément $h \in H$ (vu comme élément de $H$) est égal à son ordre comme élément de $G$.
(iv) Si $\phi : G \to K$ est un isomorphisme, alors $H$ et le sous-ensemble $\phi(H) < K$ sont isomorphes.
(v) L'ordre d'un sous-groupe d'un groupe infini est infini.
(vi) L'ordre d'un sous-groupe d'un groupe fini est fini.

*Exercice* 4.12. (i) Soit $a \in G$ et soit le sous-ensemble $\mathbb{C}_G(a) = \{g \in G\,;\, ga = ag\}$. Montrer que $C_G(a)$ est un sous-groupe de $G$. (Ce groupe est appelé le centralisateur de $a$ dans $G$.)
(ii) Soit $A$ un sous-ensemble de $G$ (pas nécessairement un sous-groupe de $G$). Montrer que $\mathrm{N}_G(A) = \{g \in G \,|\, gag^{-1} \in A, \text{ pour tout } a \in A\}$ est un sous-groupe de $G$. (Ce sous-groupe est appelé le normalisateur de $A$ dans $G$.)
Solution de (i) : cet exercice ressemble beaucoup à la vérification qu'un sous-ensemble est un sous-espace vectoriel. Vous avez fait de nombreux exercices du genre dans le cours d'algèbre linéaire. Pour le cas présent, $\mathbf{1}$ est dans $C_G(a)$ puisque la condition $ga = ag$ est vérifiée pour $g = \mathbf{1} : \mathbf{1}a = a = a\mathbf{1}$. La seconde étape consiste à vérifier que l'ensemble proposé est fermé sous la multiplication. Si $g$ et $h$ sont dans $C_G(a)$, c'est donc que $ga = ag$ et $ha = ah$. Alors leur produit $gh$ satisfait $(gh)a = g(ha) = g(ah) = (ga)h = a(gh)$. Donc $gh \in G_C(a)$. Reste à vérifier que l'inverse d'un élément $g \in C_G(a)$ est aussi dans $C_G(a)$. Mais si $g$ satisfait $ga = ag$, il suffit de multiplier à gauche et à droite par $g^{-1} \in G$ pour obtenir $g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1}$ et donc, après simplification, $ag^{-1} = g^{-1}a$ et donc $g^{-1} \in C_G(a)$. Ainsi $C_G(a)$ est un sous-groupe de $G$.

4.2. **Sous-groupe engendré par un sous-ensemble.** On peut définir des sous-groupes de $G$ à l'aide de générateurs. Soit $S \subseteq G$ un sous-ensemble d'un groupe. Le sous-groupe de $G$ *engendré par* $S$ est défini comme étant le plus petit sous-groupe de $G$ contenant $S$. Plus précisément, c'est l'intersection de tous les sous-groupes $K < G$ contenant $S$ comme sous-ensemble. On écrit $\langle S \rangle$ pour ce sous-groupe. Les éléments de $S$ sont des *générateurs* de $H$ dans le sens suivant. Chaque élément $x$ de $\langle S \rangle$ s'écrit comme

$$x = s_1 s_2 \cdots s_n,$$

où $n \in \mathbb{Z}_{\geq 0}$ et $s_i$ ou $s_i^{-1} \in S$ pour chaque $i$. Le produit vide est par définition le neutre de $G$.

*Démonstration.* Soit

$$K := \{s_1 s_2 \cdots s_n \in G;\ n \in \mathbb{Z}_{\geq 0} \text{ et } \forall_{1 \leq i \leq n} : s_i \text{ ou } s_i^{-1} \in S\}.$$

On a que $K$ est un sous-groupe de $G$, parce que $\mathbf{1}_G \in K$ (le produit vide), $K \cdot K \subseteq K$ et l'inverse $s_n^{-1} \cdots s_2^{-1} s_1^{-1}$ de $s_1 s_2 \cdots s_n$ est aussi dans $K$. Évidemment $S \subseteq K$. Soit $H$ un sous-groupe de $G$

contenant $S$. Alors chaque expression $s_1 s_2 \cdots s_n$ est dans $H$ et donc $K \subseteq H$. Il suit que $K$ est exactement l'intersection de tous les sous-groupes de $G$ contenant $S$ et le plus petit sous-groupe de $G$ contenant $S$. $\square$

*Exemples* 4.4. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\{\overline{1}\}$.

Soit $S = \{(1,2),(2,3),(3,4),\ldots,(n-1,n)\} \subset S_n$. Alors $\langle\, S \,\rangle = S_n$, parce que chaque permutation est un produit de 2-cycles de la forme $(i, i+1)$. On a que

$$\langle\, \{(12)(34),(13)(24)\} \,\rangle = V_4$$

dans $S_4$.

Le sous-ensemble $\{\rho, \sigma\}$ engendre le groupe diédral $D_n$ de l'exercise 1.9.

*Exercice* 4.13. Soit $S$ l'ensemble des produits de pairs de 2-cycles (pas nécessairement disjoints) dans $S_n$. Montrer que $\langle\, S \,\rangle = \mathrm{Alt}_n$. Montrer que $\mathrm{Alt}_n$ est aussi le sous-groupe engendré par l'ensemble de tous les 3-cycles.

*Exercice* 4.14. Soit $\mathbb{K}$ un corps. Pour $k \in \mathbb{K}$ et $0 \leq i, j \leq n$, $i \neq j$, soit $E_{ij}(k)$ la matrice $n \times n$ élémentaire définie par $E_{ij}(k)_{rr} := \mathbf{1}$ (si $1 \leq r \leq n$), $E_{ij}(k)_{ij} := k$ et $E_{ij}(k)_{rs} := \mathbf{0}$ si $r \neq s$ et $(r,s) \neq (i,j)$. Montrer que $\mathrm{SL}(n,\mathbb{K})$ est le sous-groupe de $\mathrm{GL}(n,\mathbb{K})$ engendré par toutes les matrices élémentaires $E_{ij}(k)$. (Utiliser l'algorithme de Gauss de l'algèbre linéaire.)

*Exercice* 4.15. Soit $H$ le sous-groupe de $\mathrm{GL}(2,\mathbb{R})$ engendré par les deux matrices

$$A := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};\ B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

c'est-à-dire $H = \langle\, A, B \,\rangle$. Montrer que $H = \mathrm{SL}(2,\mathbb{Z})$, la collection des matrices à coefficients entiers et de déterminant 1.

*Exercice* 4.16. Le sous-groupe engendré par $S \subseteq G$ est abélien si et seulement si $st = ts$ pour chaque $s, t \in S$.

*Exemple* 4.5. Les sous-groupes de $(\mathbb{Z}, +)$ sont les

$$n\mathbb{Z} := \{nm;\ m \in \mathbb{Z}\}$$

pour $n \in \mathbb{Z}_{\geq 0}$. Par exemple $15\mathbb{Z} \cap 18\mathbb{Z} \cap 10\mathbb{Z} = 90\mathbb{Z}$.

*Démonstration.* Ce sont vraiment des sous-groupes. Soit $H \neq \{0\}$ un sous-groupe. Soit $n$ le plus petit entier positif dans $H$, et supposons que $n\mathbb{Z} \neq H$, alors il existe un $m \in H$ qui n'est pas divisible par $n$. Par division avec reste il existe des entiers $r, s$ tels que $m = sn + r$, où $0 < r < n$. Mais $-sn \in H$ (pourquoi ?), donc $r \in H$ qui est plus petit que $n$. Contradiction. Donc $n\mathbb{Z} = H$. $\square$

*Exercice* 4.17. Montrer que $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{ppcm}(a,b)\mathbb{Z}$ et $\langle\, a\mathbb{Z} \cup b\mathbb{Z} \,\rangle = \mathrm{pgcd}(a,b)\mathbb{Z}$.

*Exercice* 4.18. Soit $a \in G$, alors le sous-groupe $\langle\, a \,\rangle := \langle\, \{a\} \,\rangle$ est isomorphe à $(\mathbb{Z}, +)$ si $|\langle\, a \,\rangle| = \infty$ et isomorphe à $C_n$ (le groupe cyclique d'ordre $n$) si $|\langle\, a \,\rangle| = n < \infty$. Montrer que si $|\langle\, a \,\rangle| = n < \infty$ alors $n$ est le plus petit entier $n$ tel que $a^n = \mathbf{1}$.

*Exercice* 4.19. Soit $G$ un groupe et soient deux éléments $s, t \in G$ d'ordre respectif 2 et 3 qui commutent $st = ts$. Alors $\langle \{s, t\} \rangle$ contient nécessairement un élément d'ordre 6.

*Exercice* 4.20. VRAI ou FAUX.
(i) Le sous-groupe de $S_n$ engendré par $\{(1,2),(2,3),\ldots,(k-1,k)\}$ avec $k \leq n$ est isomorphe à $S_k$.
(ii) Le sous-groupe $\langle \{1\} \rangle$ du groupe $(\mathbb{Z}, +)$ est $\mathbb{Z}$ lui-même.
(iii) Le groupe $(\mathbb{Q} \setminus \{0\}, \times)$ peut être engendré par un ensemble fini de générateurs.
(v) Si $H$ est un sous-groupe de $G$, alors $\langle H \rangle = H$.

*Exercice* 4.21. (i) Soit $G$ un groupe abélien et $G_{\text{fini}} = \{g \in G\,;\, |g| < \infty\}$. Alors $G_{\text{fini}}$ est un sous-groupe de $G$.
(ii) Soit $\mathbb{Q}/\mathbb{Z}$ l'ensemble des classes d'équivalence sous la relation $\sim$ suivante : $\frac{p}{q} \sim \frac{r}{s}$ s'il existe $n \in \mathbb{Z}$ tel que $\frac{p}{q} = \frac{r}{s} + n$. Montrer que $\frac{\overline{p}}{q} \hat{+} \frac{\overline{r}}{s} = \overline{\frac{p}{q} + \frac{r}{s}}$ est une opération bien définie sur $\mathbb{Q}/\mathbb{Z}$ et que $(\mathbb{Q}/\mathbb{Z}, \hat{+})$ est un groupe.
(iii) Soit $\mathrm{SO}(2, \mathbb{R})$ le groupe des matrices orthogonales $2 \times 2$ de déterminant 1. Montrer que $\mathrm{SO}(2, \mathbb{R})_{\text{fini}}$ et $(\mathbb{Q}/\mathbb{Z}, \hat{+})$ sont isomorphes.

4.3. **Sous-groupe dérivé.** Soit $G$ un groupe et soient $x, y \in G$ deux éléments. Le *commutateur* de la paire $(x, y)$ est l'élément

$$[x, y] := xyx^{-1}y^{-1} \in G.$$

Alors $xy = [x, y]yx$ et $[x, y][y, x] = \mathbf{1}$. Soit $S$ l'ensemble de tous les commutateurs

$$S := \{[x, y];\ x, y \in G\}.$$

En général $S$ n'est pas un sous-groupe de $G$. Le sous-groupe de $G$ engendré par $S$ est dénoté par $[G, G]$, ou par $G'$, et appelé le *sous-groupe dérivé* de $G$. Puis on peut définir $G'' := (G')'$ (le sous-groupe dérivé du sous-groupe dérivé de $G$), $G^{(3)} := G'''$, etc.

On dit qu'un groupe est *résoluble* si $G^{(n)} = \mathbf{1}$ pour $n$ assez grand.

$$G \supseteq G' \supseteq G'' \supseteq G^{(3)} \supseteq G^{(n)} = \mathbf{1}.$$

*Exercice* 4.22. Soit $\mathbb{K}$ un corps. Montrer que chaque sous-groupe $H$ de $B(n, \mathbb{K})$ est résoluble. Indice : Calculer $B(n, \mathbb{K})'$ et $B(n, \mathbb{K})''$.

On va montrer plus loin que le sous-groupe dérivé est l'intersection des noyaux de tous les homomorphismes de $G$ vers un groupe abélien. On montre déjà

**Lemme 4.3.** *Pour chaque homomorphisme $\phi : G \to A$, où $A$ est abélien, on a que $G' \subseteq \operatorname{Ker} \phi$.*

*Démonstration.* On a $\phi([x, y]) = \phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = \mathbf{1}_A$, parce que l'opération interne de $A$ est commutative. Donc $S \subseteq \operatorname{Ker} \phi$, impliquant que $G' = \langle S \rangle \subseteq \operatorname{Ker} \phi$, parce que $\operatorname{Ker} \phi$ est un sous-groupe de $G$. □

*Exercice* 4.23. Soit $G = \mathrm{Alt}_4$ et $A = C_3 = \langle \rho := e^{2\pi i/3} \rangle$. Soit l'application $\phi : G \to A$ définie par $\phi(x) = 1$ si $x \in V_4$ ; et

$$\phi((1,2,3)) = \phi((1,3,4)) = \phi((2,4,3)) = \phi((1,4,2)) = \rho;$$

$$\phi((1,3,2)) = \phi((2,3,4)) = \phi((1,2,4)) = \phi((1,4,3)) = \rho^2.$$

Vérifier que $\phi$ est un homomorphisme. Conclure que $V_4 \supseteq [\mathrm{Alt}_4, \mathrm{Alt}_4]$.

Maintenant un résultat classique de Galois.

**Proposition 4.3.** *On a (i)* $[S_n, S_n] = \mathrm{Alt}_n$*, (ii)* $[\mathrm{Alt}_n, \mathrm{Alt}_n] = \{\mathbf{1}\}$ *si* $1 \leq n \leq 3$ *;* $[\mathrm{Alt}_4, \mathrm{Alt}_4] = V_4$ *et* $[\mathrm{Alt}_n, \mathrm{Alt}_n] = \mathrm{Alt}_n$ *si* $n \geq 5$.

*Démonstration.* Pour (i), on a que $[S_n, S_n] \subseteq \mathrm{Alt}_n$ parce que $\mathrm{Alt}_n$ est le noyau de l'homomorphisme $\mathrm{sg} : S_n \to \{+1, -1\}$ et le lemme précédent s'applique. Si $n = 2$ la proposition est claire, alors on peut supposer que $n \geq 3$. Soient $1 \leq i, j, k \leq n$ trois entiers différents. Alors le 3-cycle $(i, j, k) \in [S_n, S_n]$ est un commutateur, parce que

$$[(i,j),(i,k)] = (i,j) \circ (i,k) \circ (i,j) \circ (i,k) = (i,j,k).$$

Donc le sous-groupe engendré par tous les 3-cycles est contenu dans $[S_n, S_n]$. Mais ce sous-groupe est $\mathrm{Alt}_n$ par l'exercice 4.13. Donc $\mathrm{Alt}_n < S_n'$ et (i) suit.

(ii) Pour $n = 3$ c'est clair, parce que $\mathrm{Alt}_3$ est cyclique d'ordre 3 donc abélien.

Pour $n = 4$. On a

$$[(1,2,3),(1,2,4)] = (1,2) \circ (3,4)$$

et de façon analogue pour les deux autres produits disjoints de deux 2-cycles. Donc $V_4 \subseteq [\mathrm{Alt}_4, \mathrm{Alt}_4]$. Dans le dernier exercice on a vu que $V_4$ est le noyau d'un homomorphisme vers un groupe abélien, d'où l'égalité.

Pour $n \geq 5$ on a

$$(1,2,3) = [(1,2,4),(1,3,5)]$$

et de façon analogue tous les autres 3-cycles sont des commutateurs dans $\mathrm{Alt}_n$. Mais $\mathrm{Alt}_n$ est engendré par les 3-cycles, donc $[\mathrm{Alt}_n, \mathrm{Alt}_n] = \mathrm{Alt}_n$ . □

**Corollaire 4.1.** *Le groupe* $S_n$ *est résoluble si et seulement si* $n \leq 4$.

*Remarque.* Les solutions de l'équation quadratique $x^2 + bx + c = 0$ sont données par la formule

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Des formules pour obtenir les solutions des équations du 3e et 4e degré ont été trouvées au 16e siècle. Mais plusieurs siècles d'efforts n'ont pas permis de trouver des formules semblables pour des degrés plus élevés. C'est Abel[8] et Ruffini qui montrèrent les premiers qu'il n'en existe pas (Abel quand il avait 19 ans, la preuve de Ruffini était douteuse) ! Un peu plus tard Galois[9] montra aussi qu'il est impossible de trouver de telles formules. Il établit une relation profonde entre la théorie des équations et la théorie des groupes. Le point-clé est que l'équation générale de degré $n$ est résoluble par des radicaux si et seulement si $S_n$ est résoluble (donc par le corollaire si et seulement si $n \leq 4$).

Les coefficients du polynôme $x^n + b_1 x^{n-1} + \ldots + b_n$ sont des combinaisons des racines $x_1, x_2, \ldots, x_n$ comme on voit quand on fait le développement de $\prod_{i=1}^{n}(x - x_i)$ et on compare les coefficients. Par

8. Niels Henrik Abel, mathématicien norvégien, 1802–1829.

9. Évariste Galois, étudiant de l'école normale, 1811–1832.

exemple, $b_n = \prod_{i=1}^n(-x_i)$ et $b_1 = \sum_{i=1}^n(-x_i)$. Ces combinaisons ne dépendent pas de l'ordre des racines choisi et sont donc invariantes sous toute permutation de ces racines. Ainsi apparaît le groupe des permutations dans la théorie des équations !

*Exercice* 4.24. (i) Calculer le sous-groupe dérivé de $D_3$.
(ii) Même exercice pour $D_n$. (Si vous n'avez pas utilisé les relations entre $\rho$ et $\sigma$ (voir l'exercice 1.9), alors il est temps de le faire !)

*Exercice* 4.25. Le groupe $G$ est abélien si et seulement $G' = \{\mathbf{1}\}$.

*Exercice* 4.26. Soit $k \in G'$ un élément du groupe dérivé de $G$ et soit $g \in G$ un élement quelconque de $g$. Alors $gkg^{-1} \in G'$.

*Exercice* 4.27. VRAI ou FAUX.
(i) $G' = \{\mathbf{1}\}$ si $G$ est abélien.
(ii) Les sous-groupes dérivés de deux groupes isomorphes sont isomorphes.
(iii) Si $\phi : G \to H$ est un morphisme, alors $(\operatorname{Im}\phi)' = \operatorname{Im}(\phi|_{G'})$.

4.4. **Théorème de Cayley.** On peut interpréter chaque groupe comme un sous-groupe d'un groupe de permutations. C'est un résultat classique de Cayley [10].

**Proposition 4.4.** *Chaque groupe $(G, *)$ est isomorphe à un sous-groupe du groupe symétrique $S_G$.*

*Démonstration.* A chaque $g \in G$ on associe la bijection $T_g : G \to G$ (pas un homomorphisme de groupes !) définie par

$$T_g(x) := g * x$$

pour $x \in G$. On a $T_g \circ T_h = T_{g*h}$, parce que

$$(T_g \circ T_h)(x) = T_g(T_h(x)) = T_g(h * x) = g * (h * x) = (g * h) * x = T_{g*h}(x)$$

pour chaque $x \in G$. L'application inverse de $T_g$ est $T_{g^{-1}}$. Donc l'application

$$T : G \to S_G \text{ avec } T(g) := T_g$$

est un homomorphisme de groupes. Pour montrer que $T$ est un monomorphisme, il suffit de montrer que le noyau est trivial. Supposons donc que $g \in \operatorname{Ker} T$, alors $T_g = \mathbf{1}$, donc

$$g * x = T_g(x) = \mathbf{1}(x) = x,$$

pour chaque $x \in G$. Donc $g = \mathbf{1}_G$ et le noyau est trivial. Donc $T$ est un monomorphisme et $G$ est isomorphe au sous-groupe

$$\{T_g; g \in G\} < S_G.$$

□

10. Arthur Cayley, mathématicien anglais, 1821–1895.

4.5. **Théorème de Lagrange.** Soit $H < G$ un sous-groupe d'un groupe $(G, \circ)$. Pour $g \in G$ on définit le sous-ensemble $g \circ H$, le *translaté à gauche* de $H$ par $g$, comme

$$g \circ H := \{g \circ h;\ h \in H\},$$

et de façon analogue $H \circ g$, le translaté à droite de $H$ par $g$. Évidemment $g \circ H = (g \circ h) \circ H$ comme sous-ensembles de $G$, pour chaque $h \in H$.

Pour $H < G$ un sous-groupe d'un groupe $(G, \circ)$, on désigne par $G/H$ (« $G$ modulo $H$ ») l'ensemble des translatés à gauche de $H$ par les éléments de $G$. Alors on peut interpréter $g \circ H$ soit comme *sous-ensemble* de $G$, soit comme *élément* de $G/H$. Il faut bien comprendre la différence ! !

Il y a une application surjective *naturelle*

$$\nu_H :\ G \to G/H;\ \nu_H(g) := g \circ H.$$

Bien sûr, ici $g \circ H$ est vu comme un élément de $G/H$, pas comme un sous-ensemble de $G$.

Cette application n'est pas un homomorphisme de groupes, pour la simple raison qu'on n'a pas défini une opération interne sur l'ensemble $G/H$. Si $g \circ H$ et $k \circ H$ sont considérés comme sous-ensembles de $G$, on peut définir un autre sous-ensemble de $G$ :

$$g \circ H \circ k \circ H := \{g \circ h_1 \circ k \circ h_2;\ h_1, h_2 \in H\}.$$

Mais, en général cet ensemble est la réunion de plusieurs translatés à gauche par des éléments de $G$ (montrer ça).

**Lemme 4.4.** *Soit $H < G$ un sous-groupe d'un groupe $(G, \circ)$. Alors chaque élément de $G$ est contenu dans un seul translaté à gauche de $H$, et dans un seul translaté à droite. Si deux translatés à gauche de $H$ sont différents, alors leur intersection est vide. Il y a une bijection entre $H$ et le translaté $g \circ H$.*

*Démonstration.* Soit $g \in G$, alors $g = g \circ \mathbf{1}_G \in g \circ H$, donc $g$ est contenu dans le translaté $g \circ H$. Supposons que $g$ est aussi contenu dans $x \circ H$ pour $x \in G$. Alors il existe un $h \in H$ tel que $g = x \circ h$, alors $g \circ H = (x \circ h) \circ H = x \circ H$, donc les deux translatés coïncident. La bijection est $h \mapsto g \circ h$ avec l'inverse $x \in g \circ H \mapsto g^{-1} \circ x$. □

Le nombre d'éléments $O(G)$ dans un groupe $G$ s'appelle *l'ordre de $G$*. *L'ordre* $O(g)$ d'un élément $g \in G$ est l'ordre du sous-groupe engendré par $g$, ou

$$O(g) := O(\langle\, g \,\rangle).$$

Si $H < G$, le nombre de translatés à gauche de $H$ s'appelle *l'indice de $H$ dans $G$* et se dénote $(G : H)$ ou $O(G/H)$.

**Théorème 4.1** (Théorème de Lagrange)**.** [11] *Soient $H < K$ et $K < G$ des sous-groupes. Alors*

$$(G : H) = (G : K)(K : H).$$

*En particulier*

$$O(G) = (G : K) \cdot O(K)$$

11. Joseph Louis Lagrange, mathématicien français, 1736–1813.

*et si $O(G) < \infty$, alors $O(K)$ est un diviseur de $O(G)$.*

*Si $g \in G$, alors $O(g)$ est un diviseur de $O(G)$.*

*Démonstration.* On a que $H$ est aussi un sous-groupe de $G$ et le groupe $G$ est la réunion disjointe de ses différents translatés à gauche de $H$, par le lemme précédent. Chaque translaté à gauche $gH$ est en bijection avec $H$, donc a la même cardinalité que $H$ et on voit que $O(G) = (G : H) \cdot O(H)$.

Soient $xH$ et $yK$ deux translatés. Si l'intersection n'est pas vide, alors $xH \subseteq yK$ et il y a une bijection entre $K/H$ (les translatés à gauche de $H$ contenus dans $K$) et les translatés à gauche de $H$ contenus dans $yK$ par l'application $kH \mapsto ykH$. Donc chaque translaté à gauche de $K$ contient $(K : H)$ translatés à gauche de $H$. Alors $(G : H) = (G : K)(K : H)$.

Les autres affirmations suivent de cette formule. □

*Remarque.* On pourrait définir un sous-monoïde $N$ d'un monoïde $(M, \circ)$ (d'une façon évidente), et le translaté à gauche $m \circ N$. Mais l'analogue du théorème ne serait plus valide. C'est ça peut-être la plus grande différence entre la théorie des monoïdes et la théorie des groupes !

*Exercice* 4.28. Soit $G$ un groupe tel que $O(G)$ est un nombre premier $p$. Alors $G$ est isomorphe à $C_p$ et est engendré par chaque élément qui n'est pas le neutre.

*Exercice* 4.29. On dit que $1 \leq n_1 \leq n_2 \leq \cdots \leq n_\ell$ est une partition de $n$ si $n = n_1 + n_2 + \cdots + n_\ell$. Soit une telle partition de $n$. Alors $n!$ est divisible par $n_1! n_2! \cdots n_\ell!$.

*Exercice* 4.30. Soit $G$ un groupe fini et soit $g \in G$. On a que $O(g)$ est le plus petit nombre entier $m$ tel que $g^m = \mathbf{1}$. Si $g^r = \mathbf{1}$, alors $r$ est divisible par $O(g)$. On a que $g^{O(G)} = \mathbf{1}$. Pour chaque $i$ on a que $O(g^i)$ divise $O(g)$. Si $i \geq 0$ est un diviseur de $O(g)$ alors $O(g^i) = O(g)/i$.

**Lemme 4.5.** *Soit $G$ un groupe et $x, y \in G$ d'ordre fini tels que $xy = yx$. Soit $m$ le plus petit commun multiple de $O(x)$ et $O(y)$ ; $n$ le plus grand commun diviseur de $O(x)$ et $O(y)$ et $a := m/n$. Alors*

$$a | O(xy) \text{ et } O(xy) | m.$$

*En particulier, si $O(x)$ et $O(y)$ sont relativement premiers et $xy = yx$ alors $O(xy) = O(x)O(y)$.*

*Démonstration.* Il existe $q$ et $r$ relativement premiers tels que $O(x) = nq$, $O(y) = nr$. Remarquons que $a = qr$. Puisque $x$ et $y$ commutent, on a que

$$(xy)^m = x^m y^m = x^{nqr} y^{nqr} = \mathbf{1}$$

et donc par l'exercice précédent $O(xy)|m$.

On va montrer que $O((xy)^n) = a$. D'abord $O((xy)^n)$ divise $a$, car

$$((xy)^n)^a = (xy)^{na} = (xy)^m = \mathbf{1}.$$

Supposons que $O((xy)^n) \neq a$, alors il existe un premier $p$ tel que $p|a$ et $O((xy)^n)$ divise l'entier $a/p$. On peut supposer que $p$ divise $q$ (sinon on change $x$ et $y$). Donc $p$ ne divise pas $r$ et il existe un entier $q'$ tel que $q = q'p$ . Alors

$$1 = ((xy)^n)^{a/p} = x^{nq'r} y^{nq'r} = x^{nq'r}$$

et il suit que $O(x) = nq$ divise $nq'r$ et donc $q$ divise $q'r$ et $q = q'p$ divise $q'$ (car $q$ et $r$ sont relativement premiers), ce qui est une contradiction. Donc $O((xy)^n) = a$. Par l'exercice précédent on obtient que $a|O(xy)$. □

**Proposition 4.5.** *Soit $A$ un groupe abélien fini. Soit $m$ le plus grand ordre d'un élément de $A$ (appelé l'exposant de $A$). Pour chaque $a \in A$ on a que $O(a)$ divise $m$.*

*Démonstration.* Choisissons un élément $g \in A$ tel que $O(g) = m$. Soit $a \in A$ et supposons que $O(a)$ ne divise pas $m$. Alors il existe un nombre premier $p$ tel que la multiplicité de $p$ dans $O(a)$ est plus élevée que dans $m$, disons $m = p^r m'$, $O(a) = p^s n'$, $s > r$ et $p$ ne divise ni $m'$ ni $n'$. Posons $x = g^{p^r}$ et $y = a^{n'}$, alors $O(x) = m'$ et $O(y) = p^s$. Par le lemme précédent on aura $O(xy) = m'p^s > m'p^r = m$. Une contradiction. Alors $O(a)$ divise $m$ après tout. □

Nous utilisons la proposition pour montrer que chaque sous-groupe fini du groupe multiplicatif d'un corps est nécessairement cyclique.

**Proposition 4.6.** *Chaque sous-groupe fini $H$ du groupe multiplicatif $\mathbb{K}^\times$ d'un corps $\mathbb{K}$ est cyclique, c'est-à-dire il existe un élément $h \in H$ tel que $H = \langle h \rangle$. Donc pour chaque élément $k$ de $H$ il existe un $n \in \mathbb{Z}_{\geq 0}$ tel que $k = h^n$.*

*Démonstration.* Soit $m \leq O(H)$ le plus grand ordre d'un élément de $H$. Alors par la proposition précédente l'ordre de chacun des éléments de $H$ est un diviseur de $m$. Donc chaque $h \in H$ est une solution de l'équation $T^m - \mathbf{1} = \mathbf{0}$ et cette équation de degré $m$ a au moins $O(H)$ solutions. Mais, par la Proposition 3.1, une équation de degré $m$ a au maximum $m$ solutions dans $\mathbb{K}$. On conclut que $m = O(H)$. Ceci veut dire qu'il existe un élément $k \in H$ d'ordre $O(H)$, alors $H = \langle k \rangle$ est isomorphe au groupe cyclique d'ordre $O(H)$. □

*Exercice* 4.31. Soit $H$ le sous-groupe de $\mathbb{C}^\times$ engendré par $\{i, e^{2\pi i/5}, -1\}$. Montrer que $O(H) = 20$, que $H$ est cyclique et trouver un générateur.

*Exercice* 4.32. Soit $n$ un nombre naturel, alors $\mathbb{Z}/n\mathbb{Z}$ est un monoïde pour la multiplication définie dans le petit cours arithmétique. Posons $(\mathbb{Z}/n\mathbb{Z})^\times$ pour le groupe des classes inversibles. Si $\phi(n)$ dénote le nombre d'entiers entre 0 et $n$ qui sont relativement premiers avec $n$, montrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ a $\phi(n)$ éléments. Par le théorème de Lagrange on a donc que $m^{\phi(n)} = 1$ dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Montrer maintenant :

**Théorème 4.2** (Fermat-Euler [12])**.** *Pour chaque paire de nombres entiers relativement premiers $n$ et $m$, le reste de $m^{\phi(n)}$ après division par $n$ est* 1.

En particulier, soit $n = 1000000$. On a que $m > 0$ est relativement premier avec $n$ si et seulement si son dernier chiffre est $1, 3, 7$ ou 9, donc $\phi(n) = 400000$. Le théorème dit dans ce cas que si $m > 0$ a comme dernier chiffre $1, 3, 7$ or 9, alors les six derniers chiffres de $m^{400000} - 1$ sont tous 0.

12. Pierre de Fermat, avocat et conseiller municipal français et mathématicien amateur, 1601–1665. Leonhard Euler, mathématicien suisse, 1707–1783.

*Exercice* 4.33. Soit $p$ un nombre premier. Montrer que $(\mathbb{Z}/p\mathbb{Z}^\times, .)$ est un groupe cyclique d'ordre $p-1$. Donc il existe un nombre $m$ tel que, pour chaque $0 < r < p$, il existe un exposant $a$ tel que le reste de $m^a$ par division par $p$ est $r$. (Indice : $(\mathbb{Z}/p\mathbb{Z}, +, .)$ est un corps.)

*Exercice* 4.34. VRAI ou FAUX. Soit $H < G$.
(i) Si $G$ est abélien, alors $g \circ H = H \circ g$ pour $g \in G$.
(ii) Si $H$ est abélien, alors $g \circ H = H \circ g$ pour $g \in G$.
(iii) Soit $C_p$ le groupe cyclique d'ordre $p$ premier, $G$ un groupe et $\phi : C_p \to G$ un morphisme. Alors $\ker \phi = C_p$ ou $\phi$ est injectif.

*Exercice* 4.35. Énumérer les translatés à gauche de $S_n/\operatorname{Alt}_n$ et ceux de $D_n/\langle \sigma \rangle$ où $D_n$ est le groupe diédral à $2n$ élements et $\sigma$ est la réflexion $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

*Exercice* 4.36. Montrer que $\phi : \mathbb{C}^\times \to \mathbb{R}^\times$ défini par $\phi(a+ib) = a^2 + b^2$ est un morphisme et décrire l'ensemble des translatés $\mathbb{C}^\times / \ker \phi$.

*Exercice* 4.37. Soient $H$ et $K$ deux sous-groupes de $G$ et soit, pour $g \in G$, l'ensemble $H \circ g \circ K$ défini par $\{h \circ g \circ k \in G \mid h \in H \text{ et } k \in K\}$. Cet ensemble est appelé le double translaté de $g$. Soit la relation $g_1 \sim g_2$ si $g_1$ appartient au double translaté $H \circ g_2 \circ K$ . Est-ce que $\sim$ est une relation d'équivalence ?

*Exercice* 4.38. Soient $H$ et $K$ deux sous-groupes finis de $G$ dont les ordres sont relativement premiers. Alors $H \cap K = 1$.

*Exercice* 4.39. Soit $H < G$ et soit la relation entre éléments de $G$ définie par $a \sim b$ si $b^{-1}a \in H$.
(i) $\sim$ est une relation d'équivalence.
(ii) Décrire les éléments de $G/\sim$ en termes du matériel introduit dans la présente section.

*Exercice* 4.40. Appliquer le résultat de l'exercice 4.28 au groupe $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ pour démontrer le petit théorème de Fermat : si $p$ est premier, alors $a^p \equiv a \bmod p$ pour tout $a \in \mathbb{Z}$.

4.6. **Le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$.** [13] Soit $p$ un nombre premier. Si $n \geq 2$, alors $\mathbb{Z}/p^n\mathbb{Z}$ n'est plus un corps et on ne peut plus conclure que le groupe multiplicatif $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est cyclique. En effet le groupe

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

n'est pas cyclique. Mais

$$(\mathbb{Z}/9\mathbb{Z})^\times = \langle \overline{2} \rangle = \{\overline{2}^0 = \overline{1},\ \overline{2}^1 = \overline{2},\ \overline{2}^2 = \overline{4},\ \overline{2}^3 = \overline{8},\ \overline{2}^4 = \overline{7},\ \overline{2}^5 = \overline{5}\}.$$

**Proposition 4.7.** *(i) Soit $p$ un nombre premier impair et $k \geq 1$. Alors le groupe multiplicatif $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique d'ordre $p^k - p^{k-1}$.*

*En plus, si la classe de $b \in \mathbb{Z}$ est un générateur de $(\mathbb{Z}/p^2\mathbb{Z})^\times$, alors sa classe modulo $p^k$ est aussi un générateur de $(\mathbb{Z}/p^k\mathbb{Z})^\times$ pour chaque $k \geq 2$.*

*(ii) Le groupe $(\mathbb{Z}/2^k\mathbb{Z})^\times$ d'ordre $2^{k-1}$ est engendré par les classes de $-1$ (d'ordre 2) et de 5 (d'ordre $2^{k-2}$). Ici $k \geq 3$.*

13. **Ne sera pas matière à examen !**

On ne donne pas la preuve ici.

*Remarque.* En utilisant ces résultats on montre que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si $n$ n'est pas divisible par 8 et engendré par exactement deux générateurs si $n$ est un multiple de 8.

Ce sont des résultats utilisés en théorie des nombres.

## Références

[1] M.A. Armstrong, *Groups and symmetry*, U.T.M., Springer-Verlag, New York, 1988.

[2] J.D. Dixon, *Problems in group theory*, Dover reprint, New York, 1973.

[3] D.S. Dummit et R.M. Foote, *Abstract Algebra, third edition*, John Wiley and Sons, Hoboken (NJ) , 2004.

[4] N. Jacobson, *Basic algebra I*, W.H. Freeman, San Francisco 1974.

[5] D.J.S. Robinson, *A course in the theory of groups*, GTM **80**, Springer-Verlag, New York, 1996.

[6] W.R. Scott, *Group theory*, Dover reprint, New York, 1987.

# Index


élément
  inverse, 16
  neutre, 16
épimophisme, 20
équivalence
  classe d', 9
  relation de, 9
*field*, *voir* corps 29

algorithme
  d'Euclide, 7
  de Bézout, 7
$\mathrm{Alt}_n$, 28
associativité, 15
$Aut(G)$, 20
automophisme, 20

Bézout, algorithme de, 7
bien définie
  opération, 11

Cayley
  théorème de, 42
centralisateur, 38
commutateur, 40
commutativité, 15
complexes $\mathbb{C}$, 29
congruence, 11
corps, 29
coupure de Dedekind, 13
cycle(s), 24
  disjoints, 24

demi-groupe, 15
division avec reste, 6

endomophisme, 20
Euclide, algorithme d', 7
Euler
  théorème de Fermat-Euler, 45

$\mathbb{F}_2$, 29
$\mathbb{F}_3$, 30
$\mathbb{F}_4$, 30
factorisation unique, 8
Fermat
  petit théorème de Fermat, 46
  théorème de Fermat-Euler, 45

groupe, **15–19**
  abélien, 17
  alterné, 28, 36
  centre, 37
  d'automorphismes, 20
  exposant d'un, 45
  fini, 17
  infini, 17
  ordre, 17, 43
  orthogonal, 31
  orthogonal sur $\mathbb{K}$, 36
  résoluble, 40
  symétrique, *voir* permutation 23
  unitaire, 36
$\mathrm{GL}(n, \mathbb{F}_q)$, groupe général linéaire sur un corps fini, 31
$\mathrm{GL}(n, \mathbb{K})$, groupe général linéaire sur un corps quelconque, 35
$\mathrm{GL}(n, \mathbb{R})$, groupe général linéaire réel, 14
groupe symétrique, *voir* permutation 23

homomorphisme, *voir* morphisme 20

image, 22, 36
$\mathrm{Im}\,\phi$, 22
indice d'un sous-groupe, 43
inverse, 16
inversion, 27
isomophisme, 20

$\mathrm{Ker}\,\phi$, 22

Lagrange
  théorème de, 43

monoïde, 16
monomophisme, 20
morphisme, **20–22**
  épimorphisme, 20
  automorphisme, 20
  endomorphisme, 20
  isomorphisme, 20
  monomorphisme, 20

neutre, 16
nombres
  complexes, 29
  congruents modulo $n$, 11
  naturels $\mathbb{N}$, 4

p-adiques $\mathbb{Q}_p$, 13
premiers, 8
réels, 13, 29
rationnels, 10, 29
relativement premiers, 8
normalisateur, 38
noyau, 22, 36

$\mathrm{O}(4, \mathbb{F}_2)$, 31
opération
associative, 15
binaire ou interne, 15
commutative, 15
ordre
d'un élément, 43

p-adiques $\mathbb{Q}_p$, 13
parité d'une permutation, 27
permutation
cyclique, 24
groupe de, **23–28**, 36
impaire, 27
inversion, 27
matrice de, 26
ordre du groupe de, 23
paire, 27
résolubilité du groupe de, 41
signe d'une, 27
premier (nombre), 8

$\mathbb{Q}(\sqrt{N})$, 29

relation
binaire, 9
d'équivalence, 9
de congruence modulo $n$, 11

$\mathrm{sg}(\sigma)$, 27
$S_n$, *voir* permutation 23
sous-groupe, **34–47**
centralisateur, 38
dérivé, 40
de Borel, 36
de Cartan, 36
engendré par un sous-ensemble, 38
indice, 43
normalisateur, 38
suite de Cauchy, 13

translaté (à gauche ou à droite), 43

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

*E-mail address*: broera@DMS.UMontreal.CA