
**LICENCE DE MATHÉMATIQUES**

**3ème année**

# Algèbre – 1ère Partie

# Théorie des Groupes

C.-A. PILLET

# Bibliographie


1. J.M. Arnaudiès, H. Fraysse : *Cours de Mathématiques I, Algèbre.* Dunod Université, Paris, 1990.
2. R. Godement : *Cours d'Algèbre.* Hermann, Paris, 1969.
3. B. Bigonnet : *Algèbre pour la licence.* Dunod, Paris, 2000.
4. L. Schwartz : *Mathématiques pour la licence, Algèbre.* Dunod, Paris, 1999.
5. B.L. van der Waerden : *Algebra.* Springer, New York, 1991.
6. S. Lang : *Undergraduate Algebra.* Springer, New York, 2004.
7. S. Lang : *Algebra.* Springer, New York, 2002.
8. P.R. Halmos : *Introduction à la théorie des ensembles.* Gauthier-Villars, Paris, 1988.

# Table des matières

# Chapitre 1

# Rappels et compléments

## 1.1 Applications

**1.1.1** Une *application* d'un ensemble non-vide $X$ dans un ensemble non-vide $Y$ est un sous-ensemble $f \subset X \times Y$ ayant la propriété suivante :

pour tout $x \in X$ il existe un seul $y \in Y$ tel que $(x, y) \in f$.

$X$ est l'*ensemble de départ* et $Y$ l'*ensemble d'arrivée* de l'application $f$, ce que l'on exprime par $f : X \to Y$. Si $(x, y) \in f$, on dit que $y$ est l'*image* de $x$ par $f$ et on écrit $y = f(x)$ ou encore $f : x \mapsto y$. L'ensemble des applications de $X$ dans $Y$ est noté $Y^X$.

**1.1.2** L'*image par* $f$ d'un sous-ensemble $A \subset X$ est le sous-ensemble de $Y$ défini par $f(A) = \{f(x) \,|\, x \in A\}$. La *pré-image par* $f$ d'un sous-ensemble $B \subset Y$ est le sous ensemble de $X$ défini par $f^{-1}(B) = \{x \in X \,|\, f(x) \in B\}$. En particulier, si $y \in Y$ et $x \in f^{-1}(\{y\})$ on dit que $x$ est *une pré-image* de $y$ par $f$. L'image de $X$ par $f$ est appelé *image de* $f$ et noté $\mathrm{Im} f$. Un élément $y \in Y$ admet une pré-image par $f$ si et seulement si $y \in \mathrm{Im} f$.

**1.1.3** Une application $f : X \to Y$ est dite *surjective* si $\mathrm{Im} f = Y$, elle est dite *injective* si tout $y \in Y$ admet au plus une pré-image par $f$, c'est-à-dire si tout élément $y \in \mathrm{Im} f$ admet exactement une pré-image $x \in X$. Dans ce cas on dit que $x$ est *la* pré-image de $y$ par $f$. L'application $f$ est dite *bijective* si elle est surjective et injective.

$f$ est surjective si et seulement si, pour tout $b \in Y$ l'équation $f(x) = b$ admet au moins une solution $x \in X$.

$f$ est injective si et seulement si, pour tout $b \in Y$ l'équation $f(x) = b$ admet au plus une solution $x \in X$.

$f$ est bijective si et seulement si, pour tout $b \in Y$ l'équation $f(x) = b$ admet une et une seule solution $x \in X$.

On appelle *permutation* d'un ensemble $X$ une application bijective de $X$ dans lui-même et on dénote par $\mathfrak{S}_X$ l'ensemble de toutes les permutations de $X$.

**1.1.4** Soit $f : X \to Y$ est une application. Pour tout $B_1, B_2 \subset Y$ on a

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2), \quad f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2).$$

Pour tout $A_1, A_2 \subset X$ on a

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2), \quad f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2),$$

et $f$ est injective si et seulement si

$$f(A_1 \cap A_2) = f(A_1) \cap f(A_2).$$

Si $A \subset X$ et $B \subset Y$ on a

$$f(f^{-1}(B)) \subset B, \qquad A \subset f^{-1}(f(A)).$$

$f$ est surjective si et seulement si $f(f^{-1}(B)) = B$ pour tout $B \subset Y$ et injective si et seulement si $A = f^{-1}(f(A))$ pour tout $A \subset X$.

Pour tout $B \subset Y$ on a

$$f^{-1}(Y \setminus B) = X \setminus f^{-1}(B).$$

$f$ est surjective si et seulement si, pour tout $A \subset X$

$$f(X \setminus A) \supset Y \setminus f(A).$$

$f$ est injective si et seulement si, pour tout $A \subset X$

$$f(X \setminus A) \subset Y \setminus f(A).$$

$f$ est bijective si et seulement si, pour tout $A \subset X$

$$f(X \setminus A) = Y \setminus f(A).$$

**1.1.5** La *composition* de deux applications $f : X \to Y$ et $g : Y \to Z$ est l'application $g \circ f : X \to Z$ définie par $g \circ f : x \mapsto g(f(x))$. Si $f$ et $g$ sont surjectives (resp. injectives), $g \circ f$ est surjective (resp. injective). Si $g \circ f$ est surjective (resp. injective), $g$ est surjective (resp. $f$ est injective).

De manière plus générale, on peut définir la composition $g \circ f$ de deux applications $f : X \to Y$ et $g : U \to V$ pour autant que $\operatorname{Im} f \subset U$. On a $(f \circ g)(A) = f(g(A))$ pour tout $A \subset X$ et $(f \circ g)^{-1}(B) = g^{-1}(f^{-1}(B))$ pour tout $B \subset Y$.

**1.1.6** Si $f \in Y^X$, $g \in V^U$, $j \in U^X$ et $k \in V^Y$, on dit que le diagramme

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle k} \\ U & \underset{g}{\to} & V \end{array}$$

commute si $k \circ f = g \circ j$.

**1.1.7** L'*application identique* ou *identité* d'un ensemble $X$ est l'application

$$\begin{array}{rcl} \mathrm{Id}_X : X & \to & X \\ x & \mapsto & x. \end{array}$$

Si $Y \subset X$, l'*injection canonique* de $Y$ dans $X$ est l'application

$$\begin{array}{rcl} i_Y : Y & \to & X \\ y & \mapsto & y. \end{array}$$

**1.1.8** Si $f \in Y^X$, l'application $f^\star : X \to \mathrm{Im} f$ définie par $f^\star : x \mapsto f(x)$ est surjective et le diagramme

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle f^\star}\searrow & & \nearrow{\scriptstyle i_{\mathrm{Im}f}} \\ & \mathrm{Im} f & \end{array}$$

commute, c'est à dire que $f = i_{\mathrm{Im}f} \circ f^\star$ est la composition d'une surjection et d'une injection. De plus, si $f$ est injective, $f^\star$ est bijective.

**1.1.9** Si $f : X \to Y$ est injective, il existe une et une seule application $g : \mathrm{Im} f \to X$ telle que $g \circ f = \mathrm{Id}_X$. C'est l'application qui, à chaque élément $y \in \mathrm{Im} f$ associe sa pré-image par $f$. De plus $g$ est bijective et $f \circ g = \mathrm{Id}_{\mathrm{Im}f}$. Si $f$ est bijective, l'ensemble de départ de $g$ est $Y$ tout entier, on appelle alors $g$ *application réciproque* ou *inverse* de $f$ et on la note $f^{-1}$.

**1.1.10** Si $f : X \to Y$ est surjective, il existe au moins une application $h : Y \to X$ telle que $f \circ h = \mathrm{Id}_Y$. Une telle application est nécessairement injective.

**1.1.11** Si $f : X \to Y$ et s'il existe deux applications $g : Y \to X$ et $h : Y \to X$ telles que $g \circ f = \mathrm{Id}_X$ et $f \circ h = \mathrm{Id}_Y$, alors $f$ est bijective et $g = h = f^{-1}$.

**1.1.12** Si $f : X \to Y$ et $g : Y \to Z$ sont des applications bijectives, alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. De plus $(f^{-1})^{-1} = f$.

## 1.2 Relations

**1.2.1** Une *relation* sur un ensemble non-vide $X$ est une partie $R \subset X \times X$. Si $R$ est une relation sur $X$ et $(x, y) \in R$, on dit que $x$ est en relation avec $y$ et on écrit $xRy$. Une relation est dite :

i. *Réflexive* si pour tout $x \in X$ on a $xRx$.

ii. *Symétrique* si pour tout $x, y \in X$ on a $xRy \Rightarrow yRx$.

iii. *Antisymétrique* si pour tout $x, y \in X$ on a $xRy$ et $yRx \Rightarrow x = y$.

iv. *Transitive* si pour tout $x, y, z \in X$ on a $xRy$ et $yRz \Rightarrow xRz$.

Une relation réflexive, symétrique et transitive est une *relation d'équivalence*. Une relation réflexive, antisymétrique et transitive est une *relation d'ordre*.

**Exemple 1** $R = \{(n, 2n) \mid n \in \mathbb{N}\}$ est une relation sur l'ensemble des entiers naturels $\mathbb{N} = \{0, 1, 2, \ldots\}$. Cette relation n'est ni réflexive, ni symétrique, ni antisymétrique, ni transitive.

**Exemple 2** $R = \{(x, x) \mid x \in X\}$ est une relation d'équivalence sur $X$, *l'identité* :

$$xRy \Leftrightarrow x = y.$$

**Exemple 3** $R = \{(k, k + n) \mid k \in \mathbb{Z}, n \in \mathbb{N}\}$ est une relation d'ordre sur l'ensemble des entiers relatifs $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. C'est la relation plus petit ou égal *à* habituellement notée $\leqslant$ :

$$xRy \Leftrightarrow x \leqslant y.$$

**Exemple 4** Soient $m, n \in \mathbb{Z}$. $q \in \mathbb{Z}$ est le quotient et $r \in \{0, 1, \ldots, n\}$ est le reste de la division euclidienne de $m$ par $n$ si $m = qn + r$. Soit $n$ un entier positif. La relation

$$aRb \quad \Leftrightarrow \quad a \text{ et } b \text{ ont le même reste lors de leur division par } n,$$

est une relation d'équivalence sur $\mathbb{Z}$ : la *congruence modulo* $n$. Lorsque $aRb$ on dit que $a$ et $b$ sont *congru modulo* $n$ et on écrit

$$a \equiv b \qquad (\mathrm{mod} n).$$

**Exemple 5** $\subset$est une relation d'ordre sur l'ensemble $2^X$ des sous-ensembles de $X$.

**1.2.2** Soit $R$ une relation d'équivalence sur l'ensemble $X$. Si $xRy$ on dit que $x$ et $y$ sont équivalents modulo $R$ et on écrit

$$x \equiv y \qquad (\mathrm{mod} R),$$

ou plus simplement $x \equiv y$ si aucune confusion n'est possible. Pour tout $x \in X$,

$$\pi(x) = \{y \in X \mid y \equiv x \,(\mathrm{mod}\, R)\},$$

est un sous-ensemble non-vide de $X$, car $x \in \pi(x)$ par réflexivité. $\pi(x)$ est la *classe d'équivalence* de $x$ modulo $R$. Pour $x, y \in X$ on a

$$\begin{array}{ccccc} y \in \pi(x) & \Leftrightarrow & x \equiv y & \Leftrightarrow & x \in \pi(y) \\ & & \Updownarrow & & \\ & & \pi(x) = \pi(y). & & \end{array}$$

L'ensemble de toutes les classes d'équivalence modulo R est un ensemble de sous-ensembles non-vides de X que l'on appelle *quotient* de X par R et que l'on note X/R. L'application

$$\begin{array}{rccc} \pi : & X & \to & X/R \\ & x & \mapsto & \pi(x), \end{array}$$

est clairement surjective, c'est la *surjection canonique* de X sur son quotient par R. On remarque que si $A \in X/R$ alors $a \in A$ si et seulement si $A = \pi(a)$.

**Exemple 6** Pour relation identité de l'exemple 2, la classe de chaque élément $x \in X$ est un singleton : $\pi(x) = \{x\}$. Le quotient X/R est donc le sous-ensemble de $2^X$ constitué de tous les singleton : $X/R = \{\{x\} \mid x \in X\}$. Dans ce cas et seulement dans ce cas, la projection canonique $\pi$ est injective : $\pi(x) = \pi(y) \Rightarrow x = y$. $\pi$ est donc une bijection de X dans X/R.

**Exemple 7** Pour la relation de congruence modulo $n$ de l'exemple 4, les classes d'équivalence sont des sous-ensembles infinis. Avec

$$\begin{array}{rcl} \bar{0} & = & \{\ldots, -2n, -n, 0, n, 2n, \ldots\}, \\ \bar{1} & = & \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\}, \\ \bar{2} & = & \{\ldots, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\}, \\ \vdots & \vdots & \\ \overline{q-1} & = & \{\ldots, -n-1, -1, n-1, 2n-1, \ldots\}, \end{array}$$

on a $\mathbb{Z}/R = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ et $\pi(a) = \bar{r}$ où r est le reste de la division de a par $n$.

**1.2.3** Une *partition* d'un ensemble X est un ensemble $\mathcal{P}$ de sous-ensembles de X tel que :

i. Pour tout $A \in \mathcal{P}$, $A \neq \varnothing$.

ii. Pour tout $A, B \in \mathcal{P}$, $A \neq B \Rightarrow A \cap B = \varnothing$.

iii. $\bigcup_{A \in \mathcal{P}} A = X$.

Si $\mathcal{P}$ est une partition de X et $x \in X$, il existe un et un seul élément de $\mathcal{P}$ contenant x. On note $\mathcal{P}_x$ cet élément (voir figure 1.1).

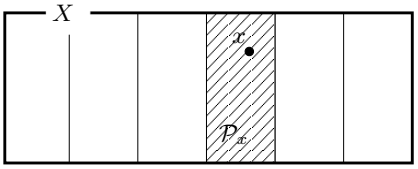


Fig. 1.1 – Une partition $\mathcal{P}$ et son élément $\mathcal{P}_x$.

**1.2.4** Si R est une relation d'équivalence sur X, le quotient X/R est une partition de X. En effet, nous avons déjà remarqué que si $A \in X/R$, alors $A \neq \varnothing$. De plus, si $A, B \in X/R$ sont tels que $A \cap B \neq \varnothing$, alors il existe $x \in A \cap B$ et $A = \pi(x)$, $B = \pi(x)$ montrent que $A = B$. Finalement, comme $x \in \pi(x)$, on a bien

$$\bigcup_{A \in X/R} A = \bigcup_{x \in X} \pi(x) \supset X.$$

Réciproquement, si $\mathcal{P}$ est une partition de X, la relation

$$x R y \quad \Leftrightarrow \quad \mathcal{P}_x = \mathcal{P}_y,$$

est une relation d'équivalence et $X/R = \mathcal{P}$. La surjection canonique est donnée par $\pi(x) = \mathcal{P}_x$.

**1.2.5** Si $a \in A \in X/R$ on dit que a est un *représentant* de la classe A. Un *système de représentants* de X/R est un sous-ensemble $\mathcal{X} \subset X$ tel que $A \cap \mathcal{X}$ ne contient qu'un seul élément pour tout $A \in X/R$. Par 1.1.9 il existe toujours au moins une application $\psi : X/R \to X$ telle que $\pi \circ \psi = \mathrm{Id}_{X/R}$. Une telle application est appelée *section de* X *par* R. Par 1.1.4 une section est toujours injective. De plus son image $\mathcal{X} = \mathrm{Im}\,\psi$ est un système de représentants de X/R.

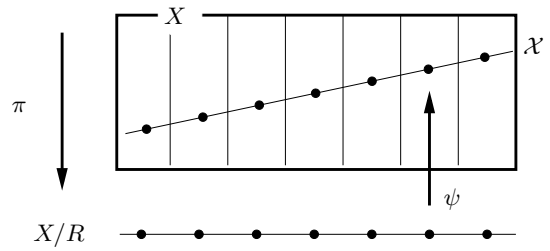


Fig. 1.2 – Une section $\psi$ et le système de représentants $\mathcal{X}$ associé.

**1.2.6** Soit R une relation d'équivalence sur X. Une application $f : X \to Y$ est *compatible avec* R si

$$x \equiv y \pmod{R} \qquad \Rightarrow \qquad f(x) = f(y),$$

c'est à dire si f est constante sur les classes d'équivalence de R. Dans ce cas, si $A \in X/R$, la valeur de $f(x)$ ne dépend pas du choix de $x \in A$. On peut donc définir une application $f_R : X/R \to Y$ en posant $f_R(A) = f(x)$ pour un élément arbitraire $x \in A$. On dit que $f_R$ est déduite de f par *passage au quotient*. Par construction, le diagramme

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle\pi}\searrow & & \nearrow{\scriptstyle f_R} \\ & X/R & \end{array}$$

commute, c'est-à-dire que $f$ peut s'écrire comme la composition $f = f_R \circ \pi$.

**1.2.7** Soit $f : X \to Y$ une application. La relation $R_f$ définie par

$$x \equiv y \pmod{R_f} \qquad \Leftrightarrow \qquad f(x) = f(y), \tag{1.1}$$

est une relation d'équivalence sur $X$ et $f$ est compatible avec cette relation. $R_f$ est appellée *équivalence d'application de* $f$. Par passage au quotient $X/R_f$, on obtient donc une application ${}^*f : X/R_f \to Y$. Cette application est injective puisque ${}^*f(A) = {}^*f(B)$ implique $f(x) = f(y)$ pour $x \in A$ et $y \in B$ et donc $x \equiv y \pmod{R_f}$, c'est-à-dire $A = \pi(x) = \pi(y) = B$. Toute application $f$ peut donc s'écrire comme la composition $f = {}^*f \circ \pi$ d'une injection ${}^*f$ avec une surjection $\pi$. De plus, si $f$ est surjective ${}^*f$ est bijective.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle\pi}\searrow & & \nearrow{\scriptstyle {}^*f} \\ & X/R_f & \end{array}$$

**1.2.8** En appliquant la décomposition du paragraphe 1.1.1.1 à ${}^*f$ on obtient une application bijective $\bar{f} = ({}^*f)^*$ et le diagramme commutatif suivant

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i_{Imf}} \\ X/R_f & \underset{\bar{f}}{\longrightarrow} & Imf \end{array} \tag{1.2}$$

qui exprime la *décomposition canonique* de $f = i_{Imf} \circ \bar{f} \circ \pi$ en trois applications $i_{Imf}$ étant injective, $\bar{f}$ bijective et $\pi$ surjective.

## 1.3 Ensembles finis, cardinal

**1.3.1** Deux ensembles $X$ et $Y$ sont *équipotents* s'il existe une bijection $f : X \to Y$.

**1.3.2** Un ensemble non-vide $X$ est *fini* s'il existe un entier $n$ tel que $X$ soit équipotent à $\{1, 2, \ldots, n\}$, *infini* sinon. Un ensemble infini est *dénombrable* s'il est équipotent à $\mathbb{N}$, *non-dénombrable* sinon. L'ensemble vide est fini.

**1.3.3** Soit $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ une application. Si $f$ est injective, alors $f(1), f(2), \ldots f(n)$ sont des éléments distincts de $\{1, 2, \ldots m\}$. On en conclut que $n \leqslant m$. De plus, si $n = m$, alors $\{f(1), f(2), \ldots, f(n)\} = \{1, 2, \ldots, n\}$ et $f$ est surjective et par conséquent bijective.

Si $f$ est surjective, il existe des éléments distincts $x_1, x_2, \ldots x_m \in \{1, 2, \ldots n\}$ tels que $f(x_j) = j$. On conclut immédiatement que $n \geqslant m$. De plus, si $n = m$, on doit

avoir $\{x_1, x_2, \ldots, x_n\} = \{1, 2, \ldots, n\}$ et donc $\{f(1), f(2), \ldots, f(n)\} = \{1, 2, \ldots, n\}$. $f$ est donc injective et par conséquent bijective.

Si $f$ est bijective, on peut donc conclure que $n = m$.

**1.3.4** Si l'ensemble $X$ est équipotent à $\{1, 2, \ldots n\}$ et à $\{1, 2, \ldots m\}$, il existe des bijections $f$ et $g$ donnant lieu au diagramme

$$\begin{array}{ccc} X & \xrightarrow{f} & \{1, 2, \ldots, n\} \\ {\scriptstyle Id_X}\downarrow & & \downarrow{\scriptstyle h} \\ X & \xrightarrow{g} & \{1, 2, \ldots, m\} \end{array}$$

Ce diagramme définit une bijection $h = g \circ Id_X \circ f^{-1}$ qui permet de conclure que $n = m$. Si $X$ est fini il n'existe donc qu'un seul entier $n$ tel que $X$ soit équipotent à $\{1, 2, \ldots n\}$. On appelle *cardinal* de $X$ cet entier que l'on note $|X|$. Par convention, le cardinal de l'ensemble vide est $0$.

**1.3.5** Soient $X$ et $Y$ deux ensembles finis équipotents avec $|X| = n$ et $|Y| = m$. Il existe donc des bijection $f, g, k$ donnant lieu au diagramme

$$\begin{array}{ccc} X & \xrightarrow{f} & \{1, 2, \ldots, n\} \\ {\scriptstyle k}\downarrow & & \downarrow{\scriptstyle h} \\ Y & \xrightarrow{g} & \{1, 2, \ldots, m\} \end{array}$$

qui définit une bijection $h$. Le raisonnement du paragraphe 1.3.3 permet de conclure que $n = m$. Réciproquement, si $X$ et $Y$ sont deux ensembles finis de même cardinal $n$, le diagramme

$$\begin{array}{ccc} X & \xrightarrow{f} & \{1, 2, \ldots, n\} \\ {\scriptstyle k}\downarrow & & \downarrow{\scriptstyle Id} \\ Y & \xrightarrow{g} & \{1, 2, \ldots, m\} \end{array}$$

définit une bijection $k$ qui montre que $X$ et $Y$ sont équipotents.

Deux ensembles finis sont donc équipotents si et seulement si ils ont le même cardinal.

**1.3.6** En utilisant les résultats du paragraphe 1.3.3 on montre facilement que si $X$ et $Y$ sont des ensembles finis équipotents toute injection $f : X \to Y$ est une bijection. Il en est de même de toute surjection $f : X \to Y$.

On montre tout aussi facilement que si $X$ et $Y$ sont finis et qu'il existe une injection $f : X \to Y$ alors $|X| \leqslant |Y|$. De même s'il existe une surjection $f : X \to Y$ alors $|X| \geqslant |Y|$.

**1.3.7** Si $f : X \to Y$ est une injection et $A \subset X$, l'application $f_A : A \to f(A)$ définie par $f_A : x \to f(x)$ est bijective. $A$ et $f(A)$ sont donc équipotents.

**1.3.8** Soit $X$ un ensemble fini.

i. Si $A \subset X$, $A$ est fini et $|A| \leqslant |X|$ avec égalité si et seulement si $A = X$.

ii. Si $f \in Y^X$ est surjective, alors $Y$ est fini et $|Y| \leqslant |X|$.

iii. Si $f \in X^Y$ est injective, alors $Y$ est fini et $|Y| \leqslant |X|$.

iv. $2^X$ est fini et $|2^X| = 2^{|X|}$.

v. Si $0 \leqslant n \leqslant |X|$, on a $|\{A \in 2^X \,|\, |A| = n\}| = \begin{pmatrix} |X| \\ n \end{pmatrix}$.

vi. Si $Y$ est fini, $Y^X$ est fini et $|Y^X| = |Y|^{|X|}$.

vii. $\mathfrak{S}_X$ est fini et $|\mathfrak{S}_X| = |X|!$.

viii. $X \cap Y$ est fini et $|X \cap Y| \leqslant |X|$.

ix. Si $Y$ est fini alors $X \cup Y$ est fini et $|X \cup Y| = |X| + |Y| - |X \cap Y|$.

x. Si $Y$ est fini alors $X \times Y$ est fini et $|X \times Y| = |X| \cdot |Y|$.

xi. Si $R$ est une relation d'équivalence sur $X$, alors $X/R$ est fini et

$$|X| = \sum_{A \in X/R} |A|.$$

**1.3.9** Un ensemble $X$ est infini si et seulement si il admet un sous-ensemble $Y$ dénombrable.

**Démonstration** ($\Rightarrow$) Soit $X$ un ensemble infini. Il suffit de montrer qu'il existe une suite croissante de sous-ensembles $Y_n = \{y_0, y_1, \ldots, y_{n-1}\}$ de $X$, tels que $|Y_n| = n$. Dans ce cas $Y = \cup_n Y_n = \{y_j \,|\, j \in \mathbb{N}\} \subset X$ et l'application $f : \mathbb{N} \to Y$ définie par $f(j) = y_j$ étant bijective, $Y$ est donc un sous-ensemble dénombrable de $X$.

La suite $Y_n$ se construit par induction sur $n$. $X$ n'étant pas vide, il existe un $y_0 \in X$ et donc $Y_1 = \{y_0\} \subset X$ et $|Y_1| = 1$. Supposons que pour un entier $n$ il existe $Y_1 \subset Y_2 \subset \cdots \subset Y_n = \{y_0, y_1, \ldots, y_{n-1}\} \subset X$ avec $|Y_k| = k$ pour $k = 1, 2, \ldots n$. Comme $X$ est infini, on a $X \neq Y_n$ et il existe donc $y_n \in X \setminus Y_n$. Posons $Y_{n+1} = Y_n \cup \{y_n\}$, alors $Y_n \subset Y_{n+1}$ et $|Y_{n+1}| = |Y_n| + 1 = n + 1$, ce qui termine l'induction.

($\Leftarrow$) (Par l'absurde) Supposons que $X$ soit fini et admette un sous-ensemble $Y$ dénombrable. Il existe une bijection $f : \mathbb{N} \to Y$. Posons $Y_n = f(\{1, 2, \ldots n\})$, alors $Y_n \subset Y \subset X$ et, par (1.3.7), $Y_n$ est équipotent à $\{1, 2, \ldots n\}$, c'est-à-dire que $|Y_n| = n$. Par 1.3.8.i on a donc $n = |Y_n| \leqslant |X|$ pour tout $n$, ce qui contredit notre hypothèse. □

**1.3.10** Un ensemble $X$ est infini si et seulement si il existe un sous-ensemble $Y$ de $X$ distinct de $X$ et équipotent à $X$.

**Démonstration** ($\Leftarrow$) (Par contraposition) Si $X$ est fini et $Y \subset X$ est équipotent à $X$, alors $|Y| = |X|$ et donc $Y = X$ par 1.3.8.i.

($\Rightarrow$) Supposons maintenant que $X$ est infini. Par 1.3.9 il existe un sous-ensemble dénombrable $A \subset X$ et une bijection $f : \mathbb{N} \to A$. En posant $x_j = f(j)$, on a donc $A = \{x_j \mid j \in \mathbb{N}\}$. Si $B = X \setminus A$, l'application $\phi : X \to X$ définie par

$$\phi(x) = \begin{cases} x, & x \in B, \\ x_{j+1}, & x = x_j \in A, \end{cases}$$

est injective. Comme $\mathrm{Im}(\phi) = X \setminus \{x_1\}$, on en conclut donc que $X$ et $X \setminus \{x_1\}$ sont équipotents. □

**1.3.11** Soit $X$ un ensemble infini.

i. Si $X \subset Y$, $Y$ est infini.

ii. Si $Y$ est non-vide, $X^Y$ et $Y^X$ sont infinis.

iii. $2^X$ est infini.

iv. $\mathfrak{S}_X$ est infini.

v. Si $Y$ est non-vide, $X \times Y$ est infini.

vi. $X \cup Y$ est infini.

**1.3.12** (Théorème de Cantor-Bernstein) Soient $X$ et $Y$ deux ensembles tels qu'il existe une injection $f : X \to Y$ et une surjection $g : X \to Y$. Alors $X$ et $Y$ sont équipotents.

# Chapitre 2

# Groupes

## 2.1 Définition et exemples

Si $X$ est un ensemble, une application

$$\begin{array}{rcl} X \times X & \to & X \\ (a, b) & \rightarrowtail & a \cdot b \end{array}$$

est une *loi de composition interne* sur $X$. On dit que l'image $a \cdot b$ est le produit de $a$ par $b$ pour cette loi. Le symbole $\cdot$ peut être remplacé par $\star$, $\top$, $\circ \ldots$ et même être omis. Dans ce dernier cas, on écrit simplement $ab$.

Une loi est dite *associative* si

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

pour tout $a, b, c \in X$. Dans ce cas, l'usage de parenthèses est superflu et on peut définir $\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdots a_n$ sans aucune ambiguïté. Si

$$a \cdot b = b \cdot a,$$

pour tout $a, b \in X$, la loi de composition interne est dite *commutative*.

Un élément $e \in X$ est dit *neutre* pour une loi de composition interne si

$$a \cdot e = e \cdot a = a,$$

pour tout $a \in X$. Si un tel élément existe, il est nécessairement unique. En effet, si $e$ et $f$ sont tous deux neutres, on a $e = e \cdot f = f$.

Si une loi de composition interne admet un élément neutre $e$, elle est *symétrisable* si, pour tout $a \in X$, il existe un élément $a' \in X$ tel que

$$a \cdot a' = a' \cdot a = e.$$

On dit alors que $a'$ est un élément symétrique à $a$.

**Définition 1** *Un groupe est un ensemble* G *muni d'une loi de composition interne associative, admettant un élément neutre et symétrisable. Si cette loi est également commutative, on dit que* G *est un groupe abélien.*

*Un groupe est dit fini si l'ensemble* G *est fini. Dans ce cas on appelle ordre du groupe le cardinal* $|G|$.

Dans un groupe, le symétrique d'un élément $a$ est unique. En effet, si $a'$ et $a''$ sont des éléments symétriques à $a$ et si l'élément neutre est $e$, on a

$$a' = a' \cdot e = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = e \cdot a'' = a''.$$

De plus, l'élément neutre est son propre symétrique $e \cdot e = e$.

**Remarque 1** On dit qu'un groupe est *noté multiplicativement* si sa loi de composition interne est notée $a \cdot b$ ou $ab$. Dans ce cas on désigne souvent l'élément neutre par $e$ ou par 1 et le symétrique de $a$ par $a^{-1}$. Lorsque la loi de composition interne s'écrit $a + b$, on dit que le groupe est *noté additivement*. Dans ce cas $0$ désigne l'élément neutre et $-a$ le symétrique de $a$. On utilise également la notation $a - b = a + (-b)$. La notation additive est généralement réservée aux groupes abéliens. Dans ces notes, nous utiliserons toujours la notation multiplicative, sauf mention contraire.

Dans un groupe, on peut simplifier à droite

$$a \cdot c = b \cdot c \quad \Rightarrow \quad a \cdot c \cdot c^{-1} = b \cdot c \cdot c^{-1} \quad \Rightarrow \quad a = b,$$

et à gauche

$$c \cdot a = c \cdot b \quad \Rightarrow \quad c^{-1} \cdot c \cdot a = c^{-1} \cdot c \cdot b \quad \Rightarrow \quad a = b.$$

De plus on a $a \cdot (a^{-1}) = (a^{-1}) \cdot a = e \Rightarrow (a^{-1})^{-1} = a$. On vérifie tout aussi simplement que $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. L'équation $a \cdot x = b$ admet une et une seule solution $x = a^{-1} \cdot b$. De même, l'équation $x \cdot a = b$ admet l'unique solution $x = b \cdot a^{-1}$.

**Exemple 8** $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des groupes abéliens pour l'addition. L'élément neutre est $0$ et le symétrique de $a$ est son opposé $-a$. ♢

**Exemple 9** $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ sont des groupe abélien pour la multiplication. L'élément neutre est 1 et le symétrique de $a$ est son inverse $1/a$. ♢

**Exemple 10** Le plus petit groupe est $\{e\}$. Il ne contient que l'élément neutre. ♢

**Exemple 11** Si un groupe ne contient que deux éléments $e$ et $a \neq e$, et si $e$ est l'élément neutre, on doit avoir $a \cdot a = e$. En effet, si au contraire $a \cdot a = a$, on a

aussi $a \cdot a = e \cdot a$ et en simplifiant à droite $a = e$ ce qui est absurde. On peut décrire ce groupe par sa table de multiplication

| $\cdot$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

Ce groupe est abélien, sa table de multiplication étant symétrique par rapport à sa diagonale principale. ♢

**Exemple 12** Un espace vectoriel est un groupe abélien pour l'addition vectorielle. L'élément neutre est le vecteur nul et le symétrique d'un vecteur $a$ est son opposé $-a$. ♢

**Exemple 13** Soit $X$ un ensemble non-vide. L'ensemble $\mathfrak{S}_X$ des bijections de $X$ dans lui même est un groupe pour la composition des applications. Si $|X| > 2$, ce groupe n'est pas abélien.

Cas particulier : le groupe symétrique de degré $N$ est définit par $S_N = \mathfrak{S}_X$, avec $X = \{1, 2, \ldots, N\}$. (Voir la section 2.6) ♢

**Exemple 14** $GL(\mathbb{R}, n)$ est l'ensemble des matrices $n \times n$ réelles inversibles. C'est un groupe pour la multiplication matricielle. Si $n > 1$, il n'est pas abélien. ♢

**Exemple 15** Une matrice $n \times n$ réelle $u$ est orthogonale si $u^\top u = I$. L'ensemble $O(n)$ de ces matrices est un groupe pour la multiplication matricielle. Il n'est pas abélien si $n > 1$. ♢

Les *puissance* d'un élément $a$ du groupe $G$ sont définies inductivement de la manière suivante.

i. $a^0 = e$.

ii. $a^n = a \cdot a^{n-1}$ pour $n = 1, 2, \ldots$

iii. $a^{-n} = (a^n)^{-1}$ pour $n = 1, 2, \ldots$

On a alors $a^{n+k} = a^n \cdot a^k$ pour tout $n, k \in \mathbb{Z}$. Lorsque $G$ est noté additivement, on définit de manière analogue les *multiples* de $a$.

i. $0a = 0$ (le premier $0$ est un élément de $\mathbb{Z}$ alors que le second est dans $G$ !)

ii. $na = a + (n-1)a$ pour $n = 1, 2, \ldots$

iii. $(-n)a = -(na)$ pour $n = 1, 2, \ldots$

Dans ce cas on a $(n + k)a = na + ka$ pour tout $n, k \in \mathbb{Z}$.

## 2.2 Sous-groupes

Si G est un groupe noté multiplicativement, on définit le produit de deux sous-ensembles $A, B \subset G$ par

$$A \cdot B = \{a \cdot b \mid a \in A, b \in B\},$$

et si $a \in G$ et $B \subset G$, on pose

$$a \cdot B = \{a \cdot b \mid b \in B\}, \qquad B \cdot a = \{b \cdot a \mid b \in B\}.$$

De même si le groupe G est abélien et noté additivement, la somme de A et B est définie par

$$A + B = \{a + b \mid a \in A, b \in B\},$$

et celle de a et B par

$$a + B = \{a + b \mid b \in B\}.$$

### 2.2.1 Définition et caractérisation

**Définition 2** *Un sous-ensemble* H *d'un groupe* G *est un sous-groupe de* G *si c'est un groupe pour la loi de composition interne de* G.

Si H est un sous-groupe et $a \in H$, on a donc $a^k \in H$ (resp. $ka \in H$ en notation additive) pour tout $k \in \mathbb{Z}$.

Tout groupe $G \neq \{e\}$ admet au moins deux sous-groupes, $\{e\}$ et G.

**Définition 3** *Un sous-groupe de* G *est dit propre s'il est distinct de* $\{e\}$ *et de* G.

Soit G un groupe. Pour qu'un sous-ensemble H de G soit un sous-groupe, il est nécessaire que la restriction à $H \times H$ de la loi de composition interne de G soit une loi de composition interne sur H, c'est-à-dire que $H \cdot H \subset H$. Un sous-ensemble de G ayant cette propriété est dit *stable* (pour la loi de composition interne de G).

Si H est un sous-groupe de G, il doit contenir un élément neutre $e_H$ qui pourrait, a priori, être différent de l'élément neutre e de G. Cependant on a d'une part $e_H \cdot e_H = e_H$, puisque $e_H$ est un élément neutre de H, et d'autre part $e_H \cdot e = e_H$ puisque e est élément neutre de G. On obtient donc $e_H \cdot e_H = e_H \cdot e$. En simplifiant a gauche on obtient $e_H = e$ ce qui montre qu'en fait $e \in H$.

Si H est un sous-groupe de G tout élément $a \in H$ doit avoir un symétrique $a'_H \in H$ tel que $a \cdot a'_H = e$. Là encore, $a'_H$ pourrait être différent du symétrique $a^{-1}$ de a dans G. Comme on a aussi $a \cdot a^{-1} = e$, il suit que $a \cdot a'_H = a \cdot a^{-1}$. Par simplification à gauche on montre donc que $a^{-1} = a'_H \in H$.

Réciproquement, si H est un sous-ensemble stable de G contenant e et tel que $a^{-1} \in H$ pour tout $a \in H$, alors H est bien un groupe pour la loi de G. Nous avons donc montré :

**Lemme 1** *Un sous ensemble* $H$ *d'un groupe* $G$ *est un sous-groupe si et seulement si les conditions suivantes sont satisfaites :*

*i.* *H est stable.*

*ii.* $e \in H$.

*iii.* *Pour tout* $a \in H$, *on a aussi* $a^{-1} \in H$.

On obtient facilement le corollaire suivant.

**Corollaire 1** *Un sous ensemble* $H$ *d'un groupe* $G$ *est un sous-groupe si et seulement si les conditions suivantes sont satisfaites :*

*i.* $H \neq \varnothing$.

*ii.* *Pour tout* $a, b \in H$, *on a* $a \cdot b^{-1} \in H$.

**Démonstration** Si $H$ est un sous-groupe les conditions *i* et *ii* sont vérifiées à l'aide du Lemme 1. A l'inverse, *i* et *ii* étant vérifiées on en déduit qu'il existe $a \in H$ et que $e = a \cdot a^{-1} \in H$. Pour tout $a \in H$ on a donc $a^{-1} = e \cdot a^{-1} \in H$. Finalement pour tout $a, b \in H$ on a $b^{-1} \in H$ et donc $a \cdot b = a \cdot (b^{-1})^{-1} \in H$. Les trois conditions du Lemme 1 sont donc vérifiées. □

**Exemple 16** $\mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$, de $\mathbb{R}$ et de $\mathbb{C}$. ♢

**Exemple 17** $\{-1, 1\}$ est un sous-groupe de $\mathbb{R}^*$. Le cercle unité

$$S^1 = \{z \in \mathbb{C} \,|\, |z| = 1\},$$

est un sous-groupe de $\mathbb{C}^*$. ♢

**Exemple 18** Si $H$ est un sous-groupe de $\mathbb{Z}$ alors soit $H = \{0\}$ soit $H = n\mathbb{Z}$ avec $n = \min\{k \in H \,|\, k > 0\}$. Preuve : Si $H \neq \{0\}$ alors $\{k \in H \,|\, k > 0\} \neq \varnothing$ et donc $n = \min\{k \in H \,|\, k > 0\}$ existe. Comme $n \in H$ on a aussi $kn \in H$ pour tout $k \in \mathbb{Z}$ et donc $n\mathbb{Z} \subset H$. Si $a \in H$ il existe $q \in \mathbb{Z}$ et $r \in \{0, 1, \ldots, n-1\}$ tels que $a = nq + r$ (division euclidienne). Comme $(-q)n, a \in H$ on en conclut que $r = a + (-q)n \in H$ et comme $0 \leqslant r < n$ la minimalité de $n$ permet de conclure que $r = 0$ c'est-à-dire que $a \in n\mathbb{Z}$. ♢

**Exemple 19** Si $V$ est un espace vectoriel, tout sous-espace vectoriel de $V$ est un sous-groupe pour l'addition vectorielle. ♢

**Exemple 20** Soit $H \neq \{0\}$ un sous-groupe de $\mathbb{R}$ et $a = \inf\{x \in H \,|\, x > 0\}$. Si $a > 0$ alors $H = a\mathbb{Z}$, sinon $H$ est dense dans $\mathbb{R}$. Preuve : Montrons tout d'abord que $a \in H$. Si tel n'est pas le cas il existe une suite strictement décroissante $a_n$ dans $H^+ = \{x \in H \,|\, x > 0\}$ telle que $\lim_n a_n = a$. Comme $a_n$ est une suite de Cauchy la suite $b_n = a_n - a_{n+1} \in H^+$ converge vers $0$ et on arrive à la contradiction $a = \inf H^+ = 0 \in H$. On a donc $a \in H$ et par conséquent $a\mathbb{Z} \subset H$. Supposons

tout d'abord $a > 0$. Alors, pour tout $b \in H$ il existe $n \in \mathbb{Z}$ et $r \in [0, a[$ tels que $b = na + r$ (voir la figure 2.1). Si $r \neq 0$ on a $r \in H^+$ mais comme $r < a$ ceci contredit la minimalité de $a$. On a donc $r = 0$ et $b = na \in a\mathbb{Z}$ et on conclut que $H = a\mathbb{Z}$. Considérons maintenant le cas $a = 0$. Soient $b \in \mathbb{R}$ et $\varepsilon > 0$ donnés. Comme il existe une suite $a_n \in H^+$ telle que $\lim_n a_n = 0$, il existe $n$ tel que $a_n < \varepsilon$. Il existe aussi $k \in \mathbb{Z}$ et $r \in [0, a_n[$ tels que $b = ka_n + r$. On en conclut que $|b - ka_n| < \varepsilon$ ce qui montre que $H$ est dense dans $\mathbb{R}$. ♢

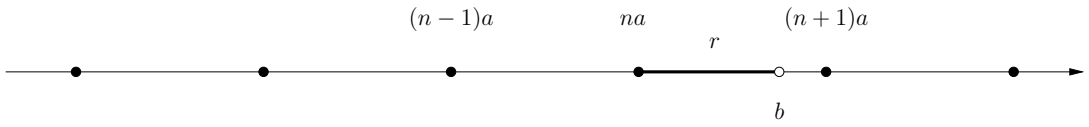


Fig. 2.1 –

Soit $H$ un sous-groupe de $G$. Il est clair que $K \subset H$ est un sous-groupe de $H$ si et seulement si c'est un sous-groupe de $G$.

**Exemple 21** $O(n)$ est un sous-groupe de $GL(\mathbb{R}, n)$. Une matrice orthogonale $u \in O(n)$ est une rotation si $\det u = 1$. L'ensemble $SO(n)$ de ces rotations est un sous-groupe de $O(n)$. ♢

**Exemple 22** Soit $n \neq 0$ et $H \neq \{0\}$ un sous-groupe de $n\mathbb{Z}$. Alors c'est un sous-groupe de $\mathbb{Z}$ et par conséquent $H = m\mathbb{Z}$ avec $m = \min\{k \in H \,|\, k > 0\}$. On en conclut que les sous-groupes de $n\mathbb{Z}$ sont tous les groupes $m\mathbb{Z}$ avec $n|m$. ♢

En utilisant le corollaire 1, on montre immédiatement que si $H$ et $K$ sont des sous-groupes du groupe $G$, alors $H \cap K$ est encore un sous-groupe. Plus généralement que si $(H_i)_{i\in I}$ est une famille de sous-groupes, alors $\cap_{i\in I} H_i$ est un sous-groupe.

Ainsi, si $A \subset G$ est un sous-ensemble non-vide du groupe $G$ l'intersection de tous les sous-groupes de $G$ contenant $A$

$$(A) = \bigcap_{\substack{H \supset A \\ H \text{ sous} - \text{groupe de } G}} H$$

est un sous-groupe. C'est évidemment le plus petit sous-groupe de $G$ contenant $A$. On dit aussi que c'est le sous-groupe de $G$ engendré par $A$.

**Exemple 23** Si $n, m \in \mathbb{Z}$ alors $(\{n, m\}) = n\mathbb{Z} \cap m\mathbb{Z} = \text{PPCM}(n, m)\mathbb{Z}$ est le sous-groupe de $\mathbb{Z}$ engendré par $n$ et $m$. ♢

### 2.2.2 Classes, quotients et indices

Soit H un sous-groupe du groupe G. On considère la relations sur G définie par

$$aRb \quad \Leftrightarrow \quad a^{-1} \cdot b \in H. \tag{2.1}$$

En utilisant le lemme 1, nous allons montrer que c'est une relation d'équivalence. R est réflexive puisque $a^{-1} \cdot a = e \in H$ implique aRa. Il suit de

$$aRb \quad \Rightarrow \quad a^{-1} \cdot b \in H \quad \Rightarrow \quad b^{-1} \cdot a = (a^{-1} \cdot b)^{-1} \in H \quad \Rightarrow \quad bRa,$$

que R est symétrique. Finalement R est transitive puisque si aRb et bRc, alors $a^{-1} \cdot b, b^{-1} \cdot c \in H$ et donc $a^{-1} \cdot c = (a^{-1} \cdot b) \cdot (b^{-1} \cdot c) \in H$, ce qui implique aRc.

La classe d'équivalence (mod R) d'un élément $a \in G$ est, par définition,

$$\pi(a) = \{x \in G \mid aRx\} = \{x \in G \mid a^{-1} \cdot x \in H\}.$$

Mais $a^{-1} \cdot x \in H$ si et seulement si il existe $h \in H$ tel que $a^{-1} \cdot x = h$, c'est-à-dire tel que $x = a \cdot h$. On a donc

$$\pi(a) = a \cdot H.$$

On appelle *classe (à gauche) de* a *suivant* H cette classe d'équivalence. On remarque que la classe de l'élément neutre e n'est autre que H lui-même, en effet $e \cdot H = H$. On notera cependant qu'en général une classe $a \cdot H$ n'est pas un sous-groupe de G.

Le quotient G/R est donc l'ensemble des classes (à gauche) suivant H. On l'appelle *quotient (à gauche) de* G *par* H et on le note G/H

$$G/H = \{a \cdot H \mid a \in G\}.$$

**Définition 4** *Soit* G *un groupe et* H *un sous-groupe. Si le quotient* G/H *est fini, l'entier*

$$[G : H] = |G/H|,$$

*est appelé indice de* H *dans* G.

**Remarque 2** En notation additive la relation (2.1) s'écrit

$$aRb \quad \Leftrightarrow \quad b - a \in H,$$

et on a $\pi(a) = a + H$ d'où il découle que $G/H = \{a + H \mid a \in G\}$.

**Exemple 24** Si l'on considère G comme sous-groupe de lui-même, on obtient le quotient $G/G = \{a \cdot G \mid a \in G\}$. Comme $a \cdot G = G$ pour tout $a \in G$, on a $G/G = \{G\}$, et donc $[G : G] = 1$.

L'autre extrême consiste à prendre le sous-groupe $H = \{e\}$. Dans ce cas la relation R est donnée par $aRb \Leftrightarrow a^{-1} \cdot b \in \{e\}$ c'est-à-dire $a = b$. R est donc la relation identité et ses classes sont $a \cdot \{e\} = \{a\}$. Le quotient est donc $G/\{e\} = \{\{a\} \mid a \in G\}$, il est fini si et seulement si G l'est et $[G : \{e\}] = |G|$ dans ce cas. ♢

**Exemple 25** On considère le groupe $G = O(n)$. Si $u \in O(n)$, alors $\det u = \pm 1$, c'est-à-dire que $G = G_+ \cup G_-$ où $G_\pm = \{u \in O(n) \mid \det u = \pm 1\}$ et $G_+ = SO(n)$ est un sous-groupe. Soit $u \in G$.

Si $\det u = 1$, alors $u \cdot G_+ = G_+$. En effet, pour tout $v \in G_+$ on a $u \cdot v \in G_+$ et $v = u \cdot w$ avec $w = u^\top v \in G_+$.

Si au contraire $\det u = -1$, alors $u \cdot G_+ = G_-$. En effet, pour tout $v \in G_+$, on a $u \cdot v \in G_-$ et pour tout $v \in G_-$, $v = u \cdot w$ avec $w = u^\top v \in G_+$.

Nous pouvons donc conclure que $O(n)/SO(n) = G/G_+ = \{G_+, G_-\}$ alors que $[O(n) : SO(n)] = 2$. ♢

**Exemple 26** (Notation additive) Soient $a, b \in \mathbb{Z}$ tels que $a|b$. D'après l'exemple 22 $b\mathbb{Z}$ est un sous-groupe de $a\mathbb{Z}$. La classe de $na \in a\mathbb{Z}$ suivant $b\mathbb{Z}$ est $\pi(na) = na + b\mathbb{Z}$. Pour déterminer le nombre de classes distinctes posons $k = b/a$ et remarquons que la condition $\pi(na) = \pi(ma)$ est équivalente à $(m - n)a \in b\mathbb{Z}$ c'est-à-dire à $m - n \in k\mathbb{Z}$. Le quotient de $a\mathbb{Z}$ par $b\mathbb{Z}$ est donc

$$a\mathbb{Z}/b\mathbb{Z} = \{b\mathbb{Z}, a + b\mathbb{Z}, 2a + b\mathbb{Z}, \ldots, (k-1)a + b\mathbb{Z}\},$$

et l'indice de $b\mathbb{Z}$ dans $a\mathbb{Z}$ est $[a\mathbb{Z} : b\mathbb{Z}] = k = b/a$.

**Théorème 1** *Soit $G$ un groupe et $H$, $K$ des sous-groupes tels que $K \subset H$. Alors $[G : K]$ est fini si et seulement si $[G : H]$ et $[H : K]$ le sont. Dans ce cas, on a $[G : K] = [G : H][H : K]$.*

**Démonstration** Nous allons montrer que $G/H \times H/K$ et $G/K$ sont équipotents en construisant une bijection $\psi$ entre ces deux ensembles. Le résultat suivra alors de 1.3.8.x et 1.3.11.v. En effet, $G/H \times H/K$ est fini si et seulement si $G/H$ et $H/K$ le sont et dans ce cas $|G/K| = |G/H \times H/K| = |G/H| \cdot |H/K|$.

Soient $\pi_1 : G \to G/H$ et $\pi_2 : H \to H/K$ les surjections canoniques. Il existe des sections (*c.f.* 1.2.5) $\phi_1 : G/H \to G$ et $\phi_2 : H/K \to H$ telles que $\pi_1 \circ \phi_1 = \mathrm{Id}_{G/H}$ et $\pi_2 \circ \phi_2 = \mathrm{Id}_{H/K}$. Considérons l'application

$$\begin{aligned} \psi : G/H \times H/K &\to G/K, \\ (p, q) &\mapsto \pi(\phi_1(p) \cdot \phi_2(q)), \end{aligned}$$

où $\pi : G \to G/K$ est la surjection canonique.

$\pi$ étant surjective, pour montrer que $\psi$ est bijective, nous devons montrer que pour tout $g \in G$ il existe une et une seule paire $(p, q) \in G/H \times H/K$ solution de l'équation

$$\psi(p, q) = \pi(g). \tag{2.2}$$

Cette dernière est équivalente à la condition $\phi_1(p) \cdot \phi_2(q) \in g \cdot K$, ou encore à $\phi_1(p) \in g \cdot K \cdot \phi_2(q)^{-1}$. Puisque $K \subset H$ et $\phi_2(q) \in H$, nous obtenons donc une condition nécessaire

$$\phi_1(p) \in g \cdot H. \tag{2.3}$$

Cette dernière détermine complètement $p$ puisque $p = \pi_1 \circ \phi_1(p) = g \cdot H = \pi_1(g)$. Pour déterminer $q$, notons que (2.3) implique $g^{-1} \cdot \phi_1(p) \in H$ et écrivons (2.2) comme $\phi_2(q) \in (\phi_1(p)^{-1} \cdot g) \cdot K = h \cdot K$, où nous avons posé $h = (g^{-1} \cdot \phi_1(p))^{-1} \in H$. En conséquence, $q = \pi_2 \circ \phi_2(q) = h \cdot K = \pi_2(h)$ est lui aussi complètement déterminé. □

Pour $a \in G$, l'application $g_a : G \to G$ définie par $g_a(x) = a \cdot x$ est appelée *translation à gauche par* $a$. On vérifie immédiatement que $g_a \circ g_b = g_{a \cdot b}$ et que $g_e = \mathrm{Id}_G$. On a donc $g_a \circ g_{a^{-1}} = g_{a^{-1}} \circ g_a = g_e = \mathrm{Id}_G$ qui montre que $g_a$ est une bijection de $G$ dans lui même et que $g_a^{-1} = g_{a^{-1}}$. $\mathcal{G}(G) = \{g_a \mid a \in G\}$ est donc un groupe pour la composition des applications. C'est un sous-groupe du groupe $\mathfrak{S}_G$ des permutations de $G$.

L'image par la bijection $g_a$de la classe $e \cdot H = H$ est

$$g_a(H) = \{g_a(h) \mid h \in H\} = \{a \cdot h \mid h \in H\} = a \cdot H.$$

En invoquant 1.3.7, nous pouvons conclure que toutes les classes selon $H$ sont équipotentes à $H$.

Supposons que $G$ soit un groupe fini et $H$ un sous-groupe. Alors $H$ est fini et donc $|q| = |H| < \infty$ pour tout $q \in G/H$. Comme $G/H$ est une partition de $G$ on a, d'après 1.3.8.xi,

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

**Théorème 2** *Soit $G$ un groupe fini. Si $H$ est un sous-groupe, alors*

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

*En particulier, l'ordre de $H$ est un diviseur de l'ordre de $G$.*

## 2.3 Morphismes

### 2.3.1 Définition et propriétés élémentaires

**Définition 5** *1. Soient $G$ et $H$ des groupes. On appelle morphisme de $G$ dans $H$ une application $\phi : G \to H$ telle que $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ pour tout $a, b \in G$. On note $\mathrm{Hom}(G, H)$ l'ensemble des morphismes de $G$ dans $H$.*

*2. Un morphisme bijectif est appelé isomorphisme.*

*3. S'il existe un isomorphisme $\phi : G \to H$, on dit que les groupes $G$ et $H$ sont isomorphes et on écrit $G \simeq H$. ($\simeq$ est une relation d'équivalence).*

*4. Un isomorphisme $\phi : G \to G$ est appelé automorphisme. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de $G$.*

Soit $\phi \in \mathrm{Hom}(G, H)$. Pour $a \in G$, on a

$$\phi(a) \cdot \phi(e) = \phi(a \cdot e) = \phi(a) = \phi(a) \cdot e.$$

En simplifiant à gauche, on obtient donc[1]

$$\phi(e) = e. \tag{2.4}$$

De plus,

$$\phi(a^{-1}) \cdot \phi(a) = \phi(a^{-1} \cdot a) = \phi(e) = e,$$

permet de conclure que $\phi(a^{-1}) = \phi(a)^{-1}$. On démontre alors aisément que, pour tout $n \in \mathbb{Z}$, $\phi(a^n) = \phi(a)^n$.

Soit $\phi : G \to H$ un isomorphisme et $a, b \in H$. Si $a' = \phi^{-1}(a)$ et $b' = \phi^{-1}(b)$ on a

$$\phi^{-1}(a \cdot b) = \phi^{-1}(\phi(a') \cdot \phi(b')) = \phi^{-1}(\phi(a' \cdot b')) = a' \cdot b' = \phi^{-1}(a) \cdot \phi^{-1}(b).$$

L'application réciproque $\phi^{-1}$ d'un isomorphisme est donc un isomorphisme. En particulier, comme $\mathrm{Id}_G$ est clairement un automorphisme de $G$, $\mathrm{Aut}(G)$ est un groupe pour la composition des applications.

Soit $K$ un sous-groupe de $G$. $\phi(K)$ n'est pas vide puisque $e = \phi(e) \in \phi(K)$. De plus, si $a, b \in \phi(K)$, il existe $a', b' \in K$ tels que $a = \phi(a')$ et $b = \phi(b')$. On a alors

$$a \cdot b^{-1} = \phi(a') \cdot \phi(b')^{-1} = \phi(a' \cdot b'^{-1}) \in \phi(K),$$

et le corollaire 1 permet de conclure que $\phi(K)$ est un sous groupe de $H$. En particulier, $\mathrm{Im}\,\phi = \phi(G)$ est un sous-groupe de $H$.

Si $K$ est un sous-groupe de $H$, $\phi^{-1}(K)$ n'est pas vide puisque $\phi(e) \in K$. Si $a$ et $b$ sont dans $\phi^{-1}(K)$ alors $\phi(a), \phi(b) \in K$ et $\phi(a \cdot b^{-1}) = \phi(a) \cdot \phi(b)^{-1} \in K$. On a donc $a \cdot b^{-1} \in \phi^{-1}(K)$ et nous concluons à nouveau que $\phi^{-1}(K)$ est un sous-groupe.

**Définition 6** *Soit $\phi \in \mathrm{Hom}(G, H)$. On appelle noyau de $\phi$ le sous-ensemble* $\mathrm{Ker}\,\phi = \phi^{-1}(\{e\})$.

Comme $\{e\}$ est un sous-groupe, le noyau d'un morphisme est un sous-groupe.

**Théorème 3** *Soit $\phi \in \mathrm{Hom}(G, H)$.*

*i. L'image par $\phi$ d'un sous-groupe est un sous-groupe.*

*ii. La pré-image par $\phi$ d'un sous-groupe est un sous-groupe.*

*iii. $\phi$ est injectif si et seulement si* $\mathrm{Ker}\,\phi = \{e\}$.

*iv. $\phi$ est surjectif si et seulement si* $\mathrm{Im}\,\phi = H$.

[1] Attention, $e$ a deux significations dans cette formule. A gauche c'est l'élément neutre de $G$ et à droite celui de $H$ !

**Démonstration** Nous avons déjà démontré *i* et *ii* alors que *iv* est la définition même de la surjectivité. Pour démontrer *iii*, soit $a \in G$. Alors $\phi(b) = \phi(a)$ est équivalent à

$$\phi(a^{-1} \cdot b) = \phi(a)^{-1} \cdot \phi(b) = e,$$

c'est-à-dire à $a^{-1} \cdot b \in \operatorname{Ker}\phi$ où encore à $b \in a \cdot \operatorname{Ker}\phi$. Le morphisme $\phi$ est donc injective si et seulement si $\operatorname{Ker}\phi = \{e\}$. □

Pour $a \in G$ on définit l'application $j_a : G \to G$ par $j_a(x) = a \cdot x \cdot a^{-1}$. On vérifie immédiatement que $j_a$ est un morphisme, que $j_e = \mathrm{Id}_G$ et $j_a \circ j_b = j_{a\cdot b}$. En particulier, on a $j_a \circ j_{a^{-1}} = j_{a^{-1}} \circ j_a = \mathrm{Id}_G$. $j_a$ est donc un automorphisme de G et $j_a^{-1} = j_{a^{-1}}$. On appelle $j_a$ *automorphisme intérieur* de G associé à l'élément $a \in G$.

L'application $j : G \to \mathrm{Aut}(G)$, définie par $j : a \mapsto j_a$ est un morphisme. L'image de j est le *groupe des automorphismes intérieurs* de G que l'on dénote par $\mathrm{Int}(G)$. Le noyau de j est appelé *centre* du groupe G et noté $Z(G)$. Notons que $a \in Z(G)$ si et seulement si $j_a = \mathrm{Id}_G$, c'est-à-dire si, pour tout $x \in G$, $a \cdot x \cdot a^{-1} = x$, ou encore $a \cdot x = x \cdot a$. Le centre d'un groupe est donc l'ensemble de ses éléments qui commutent avec tous ses éléments. En particulier, $Z(G)$ est un groupe abélien. De plus, un groupe G est abélien si et seulement si $Z(G) = G$.

**Exemple 27** Le centre du groupe $GL(\mathbb{R}, n)$ est constitué de toutes les matrices $T \in GL(\mathbb{R}, n)$ telles que $TA = AT$ pour tout $A \in GL(\mathbb{R}, n)$. Soit T une telle matrice et supposons qu'il existe $u \in \mathbb{R}^n$ tel que u et $v = Tu$ soient linéairement indépendants. A l'aide du théorème de la base incomplète on construit facilement une matrice $A \in GL(\mathbb{R}, n)$ telle que $Au = u$ et $Av = -v$. Comme $ATu = Av = -v$ et $TAu = Tu = v$ on en déduit que $v = 0$ ce qui est absurde. Pour tout $u \in \mathbb{R}^n$ il existe donc $\lambda(u) \in \mathbb{R}$ tel que $Tu = \lambda(u)u$. Si u et v sont linéairement indépendant on a $T(u+v) = \lambda(u+v)(u+v) = Tu + Tv = \lambda(u)u + \lambda(v)v$ d'où nous pouvons conclure que $\lambda(u+v) = \lambda(u) = \lambda(v)$. $\lambda(u)$ est donc indépendant de u et $T = \lambda I$. $Z(GL(\mathbb{R}, n)) = \{\lambda I \,|\, \lambda \in \mathbb{R}^*\}$ est le groupe des homothéthies de $\mathbb{R}^n$.

## 2.3.2 Sous-groupes distingués

Nous avons établi au paragraphe précédent que l'image et le noyau d'un morphisme sont des sous-groupes. La question suivante se pose donc naturellement : tous les sous-groupes d'un groupe G sont-ils l'image ou le noyau d'un morphisme ? Si H est un sous-groupe de G, l'injection canonique $i_H : H \to G$ est un morphisme. Comme $H = \operatorname{Im} i_H$ la réponse est positive pour l'image d'un morphisme. Dans le cas du noyau la question est plus délicate et va nous amener à une construction importante, celle du groupe quotient.

Si $\phi \in \mathrm{Hom}(G, K)$ on a, pour tout $a \in G$,

$$\phi(a \cdot \operatorname{Ker}\phi \cdot a^{-1}) = \phi(a) \cdot e \cdot \phi(a)^{-1} = e,$$

c'est à dire $a \cdot \mathrm{Ker}\,\phi \cdot a^{-1} \subset \mathrm{Ker}\,\phi$. Si $b = a^{-1}$, on a donc aussi $b \cdot \mathrm{Ker}\,\phi \cdot b^{-1} \subset \mathrm{Ker}\,\phi$ et par conséquent $\mathrm{Ker}\,\phi \subset a \cdot \mathrm{Ker}\,\phi \cdot a^{-1}$. On en conclut que

$$a \cdot \mathrm{Ker}\,\phi \cdot a^{-1} = \mathrm{Ker}\,\phi,$$

pour tout $a \in G$. Pour qu'un sous-groupe $H$ de $G$ soit le noyau d'un morphisme, il est donc nécessaire que la condition $a \cdot H \cdot a^{-1} = H$ soit satisfaite pour tout $a \in G$.

**Définition 7** *Un sous-groupe* $N$ *du groupe* $G$ *est dit distingué (ou normal) si, pour tout* $a \in G$, *on a*

$$j_a(N) = a \cdot N \cdot a^{-1} \subset N.$$

*On a alors* $a \cdot N \cdot a^{-1} = N$ *pour tout* $a \in G$ *et on écrit* $N \lhd G$.

*Un groupe* $G$ *est dit simple si* $|G| > 1$ *et si ses seuls sous-groupes distingués sont* $\{e\}$ *et* $G$.

Si $N \lhd G$, le produit de deux classes à gauche suivant $N$ est encore une telle classe. En effet, si $\pi : G \to G/N$ est la surjection canonique et $a, b \in G$, on a

$$\begin{aligned} \pi(a) \cdot \pi(b) &= (a \cdot N) \cdot (b \cdot N) = (a \cdot (b \cdot N \cdot b^{-1})) \cdot (b \cdot N) \\ &= (a \cdot b) \cdot N \cdot e \cdot N = (a \cdot b) \cdot N = \pi(a \cdot b). \end{aligned}$$

Cette formule définit une loi de composition interne sur le quotient $G/N$. Cette loi est clairement associative. Elle admet l'élément neutre $e \cdot N$, et le symétrique de la classe $a \cdot N$ est la classe $a^{-1} \cdot N$. De plus, $\pi$ est un morphisme dont le noyau est $N$. Nous avons donc montré qu'un sous-groupe $N$ est le noyau d'un morphisme si et seulement si il est distingué.

**Théorème 4** *Si* $N \lhd G$, *le quotient* $G/N$ *est un groupe pour le produit des classes. On l'appelle groupe quotient de* $G$ *par* $N$. *La surjection canonique*

$$\pi : G \to G/N$$

*est un morphisme et* $\mathrm{Ker}\,\pi = N$.

**Exemple 28** L'addition dans le groupe quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ est donnée par

$$\bar{k} + \bar{j} = \bar{l},$$

où $l$ est le reste de la division de $k + j$ par $n$. En effet

$$\begin{aligned} \bar{k} + \bar{j} &= \pi(k) + \pi(j) \\ &= \pi(k + j) \\ &= (k + j) + n\mathbb{Z} \\ &= l + n\mathbb{Z} \\ &= \bar{l}. \end{aligned}$$

♢

Le groupe quotient $G/N$ est fini si et seulement si l'indice de $N$ dans $G$ est fini, on a en effet $|G/N| = [G : N]$.

Si $G$ est un groupe abélien, il est clair que tous ses sous-groupes sont distingués : $a \cdot H \cdot a^{-1} = a \cdot a^{-1} \cdot H = e \cdot H = H$. Dans ce cas, le groupe quotient est lui aussi abélien.

Si $N \lhd G$ et $\phi \in \mathrm{Hom}(G, K)$, alors $\phi(N) \lhd \phi(G)$. En effet, $\phi(N)$ est un sous-groupe de $\phi(G)$ et pour tout $a \in \phi(G)$, on vérifie bien

$$a \cdot \phi(N) \cdot a^{-1} = \phi(b) \cdot \phi(N) \cdot \phi(b)^{-1} = \phi(b \cdot N \cdot b^{-1}) = \phi(N),$$

pour $b \in \phi^{-1}(\{a\}) \in G$.

Si $N \lhd K$ et $\phi \in \mathrm{Hom}(G, K)$, alors $\phi^{-1}(N) \lhd G$. On a en effet

$$\phi(a \cdot \phi^{-1}(N) \cdot a^{-1}) \subset \phi(a) \cdot N \cdot \phi(a)^{-1} = N,$$

pour tout $a \in G$ et donc $a \cdot \phi^{-1}(N) \cdot a^{-1} \subset \phi^{-1}(N)$.

Si $N \lhd G$ et si $H$ est un sous-groupe de $G$ tel que $N \subset H$ alors $N \lhd H$.

Soit $N \lhd G$ et $H$ un sous-groupe de $G$. Alors $N \cdot H = H \cdot N$ est le plus petit sous-groupe de $G$ contenant $N$ et $H$, et $N \lhd N \cdot H$. En effet, si $n \in N$ et $h \in H$ on peut écrire

$$n \cdot h = h \cdot (h^{-1} \cdot n \cdot h) = h \cdot n' \in H \cdot N,$$

et

$$h \cdot n = (h \cdot n \cdot h^{-1}) \cdot h = n'' \cdot h \in N \cdot H,$$

puisque $n' = h^{-1} \cdot n \cdot h \in N$ et $n'' = h \cdot n \cdot h^{-1} \in N$. De plus $e = e \cdot e \in N \cdot H$ et si $n, n' \in N$ et $h, h' \in H$ on a

$$(n \cdot h) \cdot (n' \cdot h') = [n \cdot (h \cdot n' \cdot h^{-1})] \cdot [h \cdot h'] = n'' \cdot h'' \in N \cdot H,$$

puisque $n'' = n \cdot (h \cdot n' \cdot h^{-1}) \in N$ et $h'' = h \cdot h' \in H$. Finalement, si $n \cdot h \in N \cdot H$, on a aussi

$$(n \cdot h)^{-1} = h^{-1} \cdot n^{-1} = (h^{-1} \cdot n^{-1} \cdot h) \cdot h^{-1} \in N \cdot H.$$

$N \cdot H$ est donc bien un sous-groupe. Il contient clairement $N$ et $H$. Comme tout sous groupe de $G$ contenant $N$ et $H$ doit aussi contenir $N \cdot H$, ce dernier est bien le plus petit sous-groupe contenant $N$ et $H$. Pour voir que $N$ est distingué dans $H \cdot N$, on remarque que pour $h \in H$ et $n \in N$ on a bien

$$(h \cdot n) \cdot N \cdot (h \cdot n)^{-1} = h \cdot (n \cdot N \cdot n^{-1}) \cdot h^{-1} = h \cdot N \cdot h^{-1} = N.$$

**Exemple 29** (En notation additive $N \cdot H$ devient $N + H$.) $a\mathbb{Z} + b\mathbb{Z}$ est le plus petit sous-groupe de $\mathbb{Z}$ contenant $a\mathbb{Z}$ et $b\mathbb{Z}$. On a $a\mathbb{Z} + b\mathbb{Z} = \mathrm{PGCD}(a, b)\mathbb{Z}$.

Si $G$ est simple et $\phi \in \mathrm{Hom}(G, H)$ alors soit $\mathrm{Ker}\,\phi = G$, ce qui est equivalent à $\mathrm{Im}\,\phi = \{e\}$, soit $\mathrm{Ker}\,\phi = \{e\}$ et $\phi$ est injectif. Si en plus $H$ est simple et $\mathrm{Im}\,\phi \neq \{e\}$, alors $\phi$ est un isomorphisme.

### 2.3.3 Les théorèmes d'isomorphisme

On considère $\phi \in \mathrm{Hom}(G, H)$. Il apparaît clairement de la démonstration du théorème 3 que les classes d'équivalence de $R_\phi$, l'équivalence d'application de $\phi$ (c.f. équ. (1.1)), sont les classes à gauche suivant $\mathrm{Ker}\,\phi$ de $G$ et que par conséquent, on a $G/R_\phi = G/\mathrm{Ker}\,\phi$. Nous pouvons donc écrire la décomposition canonique (1.2) de $\phi$ comme

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i_{\mathrm{Im}\phi}} \\ G/\mathrm{Ker}\,\phi & \xrightarrow[\bar{\phi}]{} & \mathrm{Im}\phi \end{array} \tag{2.5}$$

L'application $\bar{\phi} : G/\mathrm{Ker}\,\phi \to \mathrm{Im}\,\phi$ est donnée par $\bar{\phi} : \pi(a) \mapsto \phi(a)$. On a donc

$$\begin{aligned} \bar{\phi}(\pi(a)) \cdot \bar{\phi}(\pi(b)) &= \phi(a) \cdot \phi(b) = \phi(a \cdot b) \\ &= \bar{\phi}(\pi(a \cdot b)) \\ &= \bar{\phi}(\pi(a) \cdot \pi(b)), \end{aligned}$$

qui montre que $\bar{\phi}$ est un morphisme. $\bar{\phi}$ étant bijective, c'est un isomorphisme. On remarquera que toutes les flèches du diagramme (2.5) sont des morphismes.

**Théorème 5** *(Premier théorème d'isomorphisme) Soit* $\phi \in \mathrm{Hom}(G, H)$, *alors* $\mathrm{Im}\,\phi \simeq G/\mathrm{Ker}\,\phi$. *En particulier, si* $\phi$ *est surjectif,* $H \simeq G/\mathrm{Ker}\,\phi$.

**Exemple 30** (Comparer avec l'exemple 24) Le morphisme $\mathrm{Id}_G : G \to G$ à le noyau $\{e\}$ et l'image $G$. On obtient donc $G/\{e\} \simeq G$.

Le morphisme $\phi : G \to G$ définit par $\phi(a) = e$ pour tout $a \in G$ a pour noyau $G$ et pour image $\{e\}$. On a donc $G/G \simeq \{e\}$. ♢

**Exemple 31** Soient $a > 0$ et $\phi : \mathbb{R} \to \mathbb{C}^*$ le morphisme défini par $\phi(x) = e^{i2\pi x/a}$. L'image de $\phi$ est le cercle unité $S^1 = \{z \in \mathbb{C} \,|\, |z| = 1\}$ et son noyau est

$$\mathrm{Ker}\,\phi = \{x \in \mathbb{R} \,|\, e^{i2\pi x/a} = 1\} = a\mathbb{Z}.$$

On a donc l'isomorphisme $\mathbb{R}/a\mathbb{Z} \simeq S^1$. ♢

**Exemple 32** Pour un autre exemple, revenons sur la définition du centre $Z(G)$ (*c.f.* la fin du paragraphe 2.3.1) comme noyau du morphisme $j : G \to \mathrm{Aut}(G)$. L'image de ce morphisme est le groupe $\mathrm{Int}(G)$ des automorphismes intérieurs de $G$. Le centre $Z(G)$ est donc un sous-groupe distingué de $G$ et

$$\mathrm{Int}(G) \simeq G/Z(G).$$

Si $G$ est abélien, $Z(G) = G$ et donc $\mathrm{Int}(G) = \{\mathrm{Id}_G\} \simeq G/G = \{G\}$. Dans le cas extrême opposé où $Z(G) = \{e\}$, on a $\mathrm{Int}(G) \simeq G/\{e\} \simeq G$. ♢

**Exemple 33** L'application $\phi : O(n) \to \mathbb{R}^*$ définie par $\phi(u) = \det u$ est un morphisme : $\phi(u\cdot v) = \det(u\cdot v) = \det u \cdot \det v = \phi(u)\cdot\phi(v)$. Son noyau est l'ensemble des transformations orthogonales de déterminant 1, c'est-à-dire $SO(n)$. Son image est $\{-1, 1\}$. On a donc $SO(n) \lhd O(n)$ et

$$O(n)/SO(n) \simeq \{-1, 1\}.$$

$\diamondsuit$

**Exemple 34** L'application $g : G \to \mathfrak{S}_G$ qui à $a \in G$ associe la translation à gauche $g_a : x \mapsto a \cdot x$ est un morphisme. Son image est le sous-groupe $\mathcal{G}(G)$. Son noyau est $\{e\}$. En effet, si $a \neq e$, $g_a \neq \mathrm{Id}_G$ puisque $g_a(e) = a \cdot e = a \neq e$. On a donc

$$G \simeq G/\{e\} \simeq \mathcal{G}(G).$$

Tout groupe est donc isomorphe au groupe de ses translations à gauche. $\diamondsuit$

**Théorème 6** *(Second théorème d'isomorphisme) Soient* $N$ *et* $H$ *des sous-groupes de* $G$. *Si* $N$ *est distingué alors*

$$H/H \cap N \simeq H \cdot N/N. \tag{2.6}$$

**Démonstration** Comme nous l'avons vu au paragraphe précédent, $N \lhd H \cdot N$ et donc $H \cdot N/N$ est un groupe. Soit $\pi : H \cdot N \to H \cdot N/N$ la surjection canonique et $\phi : H \to H \cdot N/N$ sa restriction à $H \subset H \cdot N$. Comme $\pi$ est un morphisme, $\phi$ en est également un. D'une part, l'élément neutre de $H \cdot N/N$ étant la classe $e \cdot N = N$, le noyau de $\phi$ est l'ensemble des $h \in H$ tels que $\phi(h) = \pi(h) = h \cdot N = N$ c'est donc $H \cap N$. On en conclut $\operatorname{Ker}\phi = H \cap N \lhd H$. D'autre part, pour tout $h \in H$, $n \in N$ on a $\pi(h \cdot n) = h \cdot n \cdot N = h \cdot N = \phi(h)$ et donc $\operatorname{Im}\phi = \operatorname{Im}\pi = H \cdot N/N$. La relation (2.6) suit du premier théorème s'isomorphisme. $\square$

**Exemple 35** Soient $a, b \in \mathbb{Z}$ et $d = \mathrm{PGCD}(a, b)$, $M = \mathrm{PPCM}(a, b)$. Comme

$$\begin{aligned} a\mathbb{Z} \cap b\mathbb{Z} &= M\mathbb{Z}, \\ a\mathbb{Z} + b\mathbb{Z} &= d\mathbb{Z}, \end{aligned}$$

le second théorème d'isomorphisme donne

$$a\mathbb{Z}/M\mathbb{Z} = a\mathbb{Z}/(a\mathbb{Z} \cap b\mathbb{Z}) \simeq (a\mathbb{Z} + b\mathbb{Z})/b\mathbb{Z} = d\mathbb{Z}/b\mathbb{Z}.$$

Comme d'autre part on a (*c.f.* exemple 26)

$$|a\mathbb{Z}/M\mathbb{Z}| = [a\mathbb{Z} : M\mathbb{Z}] = M/a,$$

et

$$|d\mathbb{Z}/b\mathbb{Z}| = [d\mathbb{Z} : b\mathbb{Z}] = b/d,$$

on peut en conclure que $M/a = b/d$, c'est-à-dire

$$ab = \mathrm{PGCD}(a, b)\,\mathrm{PPCM}(a, b).$$

**Théorème 7** *(Troisième théorème d'isomorphisme) Si* $\phi \in \mathrm{Hom}(G,H)$ *et* $K \lhd H$ *alors l'application*

$$\begin{array}{rccc} \psi: & G/\phi^{-1}(K) & \to & H/K \\ & g\cdot\phi^{-1}(K) & \mapsto & \phi(g)\cdot K, \end{array}$$

*est un morphisme injectif. De plus si* $\phi$ *est surjectif* $\psi$ *est un isomorphisme, c'est-à-dire que*

$$G/\phi^{-1}(K) \simeq \phi(G)/K.$$

**Démonstration** Soit $\pi : H \to H/K$ la surjection canonique. $\phi_K = \pi\circ\phi$ est un morphisme (surjectif si $\phi$ est surjectif) dont le noyau est

$$\mathrm{Ker}\,\phi_K = \{a\in G \mid \phi(a)\cdot K = e\cdot K\} = \{a\in G\mid \phi(a)\in K\} = \phi^{-1}(K).$$

On a donc $G/\phi^{-1}(K) \simeq \mathrm{Im}\,\phi_K$. La décomposition canonique

$$\begin{array}{ccc} G & \stackrel{\phi_K}{\to} & H/K \\ \pi\downarrow & & \uparrow i_{\mathrm{Im}\,\phi_K} \\ G/\phi^{-1}(K) & \stackrel{\bar\phi_K}{\to} & \mathrm{Im}\,\phi_K \end{array}$$

définit donc un morphisme injectif $\psi = i_{\mathrm{Im}\,\phi_K}\circ\bar\phi_K : G/\phi^{-1}(K)\to H/K$. Si $\phi$ est surjectif, ce morphisme est bijectif et on a alors $G/\phi^{-1}(K)\simeq\phi(G)/K$. □

### 2.3.4 Groupes cycliques

Si G est un groupe et $a\in G$ l'application $\phi_a : \mathbb{Z}\to G$ définie par $\phi_a(n) = a^n$ est un morphisme du groupe additif $\mathbb{Z}$ dans G puisque $\phi_a(n)\cdot\phi_a(m) = \phi_a(n+m)$. Son image $\mathrm{Im}\,\phi_a = \{a^n \mid n\in\mathbb{Z}\}$ est donc un sous-groupe de G. De plus, si H est un sous-groupe de G contenant a, il doit aussi contenir $a^{-1}$ et donc $a^n$ pour tout les $n\in\mathbb{Z}$. $\mathrm{Im}\,\phi_a$ est donc le plus petit sous-groupe de G contenant a.

**Définition 8** *1. Soit* G *un groupe et* $a\in G$. *On appelle sous-groupe de* G *engendré par* a *et on note* $(a)$ *le plus petit sous-groupe de* G *contenant* a

$$(a) = \{a^n \mid n\in\mathbb{Z}\}.$$

*2. Si le groupe* $(a)$ *est fini on appelle ordre de* $a\in G$ *et on note* $\omega(a)$ *l'ordre de* $(a)$. *Sinon on dit que* a *est d'ordre infini.*

*3. Un groupe* G *est cyclique s'il est engendré par un de ses éléments, c'est-à-dire s'il existe* $a\in G$ *tel que* $G = (a)$.

$L_a = \mathrm{Ker}\,\phi_a = \{n\in\mathbb{Z}\mid a^n = e\}$ est un sous-groupe de $\mathbb{Z}$. Si $L_a = \{0\}$, $\phi_a : \mathbb{Z}\to(a)$ est un isomorphisme et a est d'ordre infini. Dans le cas contraire, $L_a = n\mathbb{Z}$ pour

un entier $n = \min\{k \in \mathbb{Z} \mid k > 0, a^k = e\} > 0$ et $(a) \simeq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. On en conclut que $a$ est d'ordre fini $\omega(a) = |(a)| = |\mathbb{Z}_n| = n$ et donc $L_a = \omega(a)\mathbb{Z}$,

$$(a) = \{e, a, \ldots, a^{\omega(a)-1}\},$$

et $a^{\omega(a)} = e$. On en conclut :

**Théorème 8** *Si* $G$ *est un groupe cyclique alors soit* $G$ *est infini et isomorphe à* $\mathbb{Z}$ *soit* $|G| = n$ *et* $G$ *est isomorphe à* $\mathbb{Z}_n$ *pour un entier* $n > 0$.

**Exemple 36** Dans le groupe multiplicatif $\mathbb{C}^*$ considérons l'élément $a = e^{2\pi i/n}$. On a $a^k = 1$ si et seulement si $k \in n\mathbb{Z}$ et donc $L_a = n\mathbb{Z}$, $\omega(a) = n$ et

$$(a) = \{1, a, a^2, \ldots, a^{n-1}\}.$$

Comme $(a^k)^n = 1$ le groupe $(a)$ coincide avec l'ensemble $C_n$ des $n$ racines $n$-èmes de l'unité. $C_n$ est donc un groupe cyclique d'ordre $n$ et tout groupe cyclique d'ordre $n$ lui est isomorphe.

Une racine $n$-ème de l'unité $\xi$ est dite *primitive* si $C_n = (\xi)$. Par exemple $i$ et $-i$ sont des racines 4-ème primitives de l'unité. ♢

**Théorème 9** *Si* $G$ *est un groupe fini et* $a \in G$ *alors* $a^{|G|} = e$.

**Démonstration** Le théorème 2 permet de conclure que $\omega(a) = |(a)|$ est un diviseur de $|G|$. En particulier, $a^{|G|} = (a^{\omega(a)})^{|G|/\omega(a)} = e$. □

**Exemple 37** Si $H \subset \mathbb{C}^*$ est un sous-groupe fini d'ordre $n$ alors $H = C_n$. Preuve : par le résultat précédent on doit avoir $a^n = 1$ pour tout $a \in H$ et donc $H \subset C_n$. Comme $|C_n| = |H| = n$ on peut conclure que $H = C_n$. ♢

**Théorème 10** *Si l'ordre d'un groupe fini est un nombre premier ce groupe est cyclique.*

**Démonstration** Il existe $a \in G$ tel que $a \neq e$ et donc $|(a)| > 1$. Comme $|(a)|$ divise $p$, on doit donc avoir $|(a)| = p$ et par conséquent $(a) = G$. □

Soient $a, b \in G$ des éléments d'ordre fini qui commutent, $a \cdot b = b \cdot a$. Alors $a \cdot b$ est d'ordre fini et $\omega(a \cdot b)$ divise $\omega(a)\omega(b)$. En effet,

$$(a \cdot b)^{\omega(a)\omega(b)} = (a^{\omega(a)})^{\omega(b)} \cdot (b^{\omega(b)})^{\omega(a)} = e,$$

montre que $\omega(a)\omega(b) \in L_{a\cdot b} = \omega(a \cdot b) \cdot \mathbb{Z}$. On peut conclure que $\omega(a)\omega(b)$ est un multiple de $\omega(a \cdot b)$.

Comme $e = ((a \cdot b)^{\omega(a\cdot b)})^{\omega(a)} = (a^{\omega(a)})^{\omega(a\cdot b)} \cdot b^{\omega(a\cdot b)\omega(a)} = b^{\omega(a\cdot b)\omega(a)}$ on conclut que $\omega(b)$ divise $\omega(a \cdot b)\omega(a)$. Si $\omega(a)$ et $\omega(b)$ sont premiers entre eux, on peut conclure que $\omega(b)$ divise $\omega(a \cdot b)$. En interchangeant les rôles de $a$ et $b$ on montre aussi que $\omega(a)$ divise $\omega(a \cdot b)$ et donc que $\omega(a)\omega(b)$ divise $\omega(a \cdot b)$. Comme nous savons déjà que $\omega(a)\omega(b)$ est un multiple de $\omega(a \cdot b)$ nous pouvons conclure que $\omega(a)\omega(b)$ est égal à $\omega(a \cdot b)$. Nous avons donc démontré le lemme suivant.

**Lemme 2** *Si* $a, b \in G$ *sont des éléments d'ordre fini tels que* $a \cdot b = b \cdot a$ *on a :*

*i.* $a \cdot b$ *est d'ordre fini et* $\omega(a \cdot b)$ *divise* $\omega(a)\omega(b)$.

*ii. Si* $\omega(a)$ *et* $\omega(b)$ *sont premiers entre eux, alors* $\omega(a \cdot b) = \omega(a)\omega(b)$.

Lorsque $\omega(a)$ et $\omega(b)$ ne sont pas premiers entre eux il est possible que $\omega(a \cdot b)$ soit strictement plus petit que $\omega(a)\omega(b)$, comme le montre l'exemple $b = a^{-1}$.

### 2.3.5 Groupes diédraux

L'application $\phi : \mathbb{R} \to O(2)$ qui à $x$ associe la rotation d'angle $x$

$$\phi(x) = \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix},$$

est un morphisme dont l'image est l'ensemble de toutes les rotations du plan, c'est-à-dire le sous-groupe $SO(2)$. Son noyau $\operatorname{Ker}\phi$ est l'ensemble des $x$ tels que $\cos x = 1$ et $\sin x = 0$, c'est-à-dire $\operatorname{Ker}\phi = 2\pi\mathbb{Z}$. On a donc, compte tenu de l'exemple 31

$$SO(2) \simeq \mathbb{R}/2\pi\mathbb{Z} \simeq S^1.$$

L'isomorphisme $\mu : S^1 \to SO(2)$ est donné explicitement par

$$\mu(x + iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

Par cet isomorphisme, tout sous-groupe fini de $S^1$ se transforme en un sous-groupe fini de $SO(2)$ et réciproquement, tout sous-groupe fini de $S^1$ est l'image par l'isomorphisme réciproque $\mu^{-1}$ d'un sous-groupe fini de $SO(2)$. Comme nous savons (exemple 37) que le seul sous-groupe d'ordre $m$ de $S^1$ est le groupe cyclique $C_m$ engendré par $e^{2\pi i/m}$, nous pouvons conclure que le seul sous-groupe d'ordre $m$ de $SO(2)$ est le groupe $\mathcal{R}_m = \mu(C_m)$ et que ce dernier est cyclique, engendré par la rotation $\rho_m = \mu(e^{2\pi i/m})$ d'angle $2\pi/m$. On a donc $\mathcal{R}_m = \{I, \rho_m, \ldots, \rho_m^{m-1}\}$, avec

$$\rho_m = \begin{pmatrix} \cos 2\pi/m & -\sin 2\pi/m \\ \sin 2\pi/m & \cos 2\pi/m \end{pmatrix}.$$

Le groupe $O(2)$ admet-il d'autres sous-groupes fini ? Pour répondre à cette question, supposons que $H$ soit un sous-groupe d'ordre $m$ de $O(2)$ distinct de $\mathcal{R}_m$ et posons $H^{\pm} = \{u \in H \mid \det u = \pm 1\}$. Alors $H^+ = H \cap SO(2)$ est un sous-groupe fini de $SO(2)$, et donc $H^+ = \mathcal{R}_n$ pour un entier $n > 0$. On note que $n = m$ est exclu puisque dans ce cas on aurait $H = H^+ = \mathcal{R}_m$ contrairement à notre hypothèse. On a donc $n < m$ et par conséquent il existe $\sigma \in H^- = H \setminus H^+$. $\sigma$ est une transformation orthogonale de plan de déterminant $-1$, c'est-à-dire une réflexion. La translation à gauche de $H$ associée $g_\sigma : a \mapsto \sigma a$ est une bijection de $H$ dans lui-même. De plus la relation

$$\det g_\sigma(a) = \det(\sigma a) = \det\sigma \det a = -\det a,$$

implique que $g_\sigma(H^+) \subset H^-$ et donc $|H^+| \leqslant |H^-|$ ainsi que $g_\sigma(H^-) \subset H^+$ et donc $|H^-| \leqslant |H^+|$. On conclut que $|H^+| = |H^-|$, que $m$ doit être pair, que $n = m/2$ et que $H^- = g_\sigma(H^+) = \{\sigma, \sigma\rho_n, \ldots, \sigma\rho_n^{n-1}\}$. $H$ est engendré par les deux éléments $\rho_n$ et $\sigma$, $H = \{\rho_n^k, \sigma\rho_n^k \mid k = 0, \ldots, n-1\}$, on l'appelle *groupe diédral de degré* $n$ *déterminé par* $\sigma$ et on le note $D_n(\sigma)$.

$\sigma$ est une réflexion, et donc $\sigma^2 = I$. Il en est de même de $\rho_n\sigma$ et $\rho_n\sigma\rho_n\sigma = I$ est équivalent à $\sigma\rho_n\sigma = \rho_n^{-1}$ ou encore à $\sigma\rho_n = \rho_n^{-1}\sigma$. Notons que $\rho_n = \rho_n^{-1}$ si et seulement si $n = 1, 2$. Le groupe $D_n(\sigma)$ est donc abélien si $n = 1, 2$ et non-abélien si $n \geqslant 3$. Les trois relations

$$\rho_n^n = I, \quad \sigma^2 = I, \quad \sigma\rho_n\sigma = \rho_n^{-1}, \tag{2.7}$$

déterminent complètement la structure algébrique du groupe $D_n(\sigma)$. En effet, elles permettent de calculer tous les produits

$$\begin{aligned}
\rho_n^k\rho_n^l &= \rho_n^{k+l},\\
\rho_n^k(\sigma\rho_n^l) &= \sigma(\sigma\rho_n^k\sigma)\rho_n^l = \sigma(\sigma\rho_n\sigma)^k\rho_n^l = \sigma\rho_n^{-k+l},\\
(\sigma\rho_n^k)\rho_n^l &= \sigma\rho_n^{k+l},\\
(\sigma\rho_n^k)(\sigma\rho_n^l) &= (\sigma\rho_n^k\sigma)\rho_n^l = (\sigma\rho_n\sigma)^k\rho_n^l = \rho_n^{-k+l}.
\end{aligned}$$

En particulier, les groupes diédraux de degré $n$ sont tous isomorphes, un isomorphisme $\phi : D_n(\sigma) \to D_n(\sigma')$ étant déterminé par $\phi(\rho_n^k) = \rho_n^k$ et $\phi(\sigma\rho_n^k) = \sigma'\rho_n^k$. Si

$$\sigma = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

nous dirons que $D_n(\sigma)$ est *le groupe diédral de degré* $n$ que nous noterons simplement $D_n$.

**Théorème 11** *Les seuls sous-groupe d'ordre* $m$ *du groupe* $O(2)$ *sont :*

*i.* $\mathcal{R}_m = \{\rho_m^k \mid k = 0, \ldots, m-1\}$, *le groupe cyclique engendré par la rotation* $\rho_m$ *d'angle* $2\pi/m$.

*ii. Si* $m$ *est pair,* $D_{m/2}(\sigma) = \{\rho_{m/2}^k, \sigma\rho_{m/2}^k \mid k = 0, \ldots, m/2-1\}$ *les groupes diédraux de degré* $m/2$ *déterminés par une réflexion* $\sigma$.

### 2.3.6 Produit direct

Soient $G_1, \ldots, G_n$ des groupes. Le produit cartésien

$$G = G_1 \times \cdots \times G_n,$$

est un groupe pour la loi de composition

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

L'élément neutre est $e = (e, \cdots, e)$ et l'élément symétrique de $(a_1, \ldots, a_n)$ est $(a_1^{-1}, \ldots, a_n^{-1})$.

Les applications $J_i : G_i \to G$ définies par $J_i : a \mapsto (e, \ldots, a, \ldots, e)$ sont des morphisme injectifs. Les images $\hat{G}_i = J_i(G_i)$ sont donc des sous-groupes de G, tels que $\hat{G}_i \simeq G_i$. On vérifie facilement que si $a \in G$ et $b_i \in G_i$ on a

$$j_a \circ J_i(b_i) = a \cdot J_i(b_i) \cdot a^{-1} = J_i \circ j_{a_i}(b_i),$$

d'où l'on conclut que $a \cdot \widehat{G}_i \cdot a^{-1} = \hat{G}_i$, c'est-à-dire que $\hat{G}_i \lhd G$.

Soit $\hat{G} = \widehat{G}_1 \times \cdots \times \hat{G}_n$ le produit cartésien des sous-groupes $\hat{G}_i$. L'application $\phi : \hat{G} \to G$ donnée par

$$\phi(\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_n) = \hat{a}_1 \cdot \hat{a}_2 \cdots \hat{a}_n,$$

est un morphisme. On a $\phi(J_1(a_1), \ldots, J_n(a_n)) = (a_1, \ldots, a_n)$ et donc $\phi$ est surjectif. D'autre part $\operatorname{Ker}\phi = \{(e, \ldots, e)\}$ implique que $\phi$ est injectif. C'est donc un isomorphisme. La représentation d'un élément $a \in G$ comme produit

$$a = \hat{a}_1 \cdot \hat{a}_2 \cdots \hat{a}_n,$$

d'éléments des sous-groupes $\hat{G}_i$ est donc unique. Ces observations motivent la définition suivante.

**Définition 9** *Soient* G *un groupe et* $G_1, G_2, \ldots, G_n$ *des sous-groupes. On dit que* G *est le produit direct des* $G_i$*, et on écrit*

$$G = \bigotimes_{i=1}^{n} G_i$$

*si l'application* $\phi : G_1 \times \cdots \times G_n \to G$ *définie par* $\phi(a_1, \ldots, a_n) = a_1 \cdots a_n$ *est un isomorphisme.*

Si G est le produit direct des sous-groupes $G_i$ et si $G \simeq H$, il existe un isomorphisme $\psi : G \to H$ et les images $H_i = \psi(G_i)$ sont des sous-groupes de H. L'application $\check{\psi} : H_1 \times \cdots \times H_n \to G_1 \times \cdots \times G_n$ définie par

$$\check{\psi}(a_1, \ldots, a_n) = (\psi^{-1}(a_1), \ldots, \psi^{-1}(a_n)),$$

est un isomorphisme. Le diagramme

$$\begin{array}{ccc} G_1 \times \cdots \times G_n & \xrightarrow{\phi} & G \\ \uparrow \check{\psi} & & \downarrow \psi \\ H_1 \times \cdots \times H_n & \to & H \end{array}$$

définit un isomorphisme $H_1 \times \cdots \times H_n \to H$ qui montre que H est le produit direct des sous-groupes $H_i$.

**Théorème 12** *Soient* $G$ *un groupe et* $G_1, G_2, \ldots, G_n$ *des sous-groupes.* $G$ *est le produit direct des sous-groupes* $G_i$ *si et seulement si les trois conditions suivantes sont satisfaites :*

*i.* $G_i \lhd G$ *pour* $i = 1, \ldots, n$.

*ii.* $G = G_1 \cdot G_2 \cdots G_n$.

*iii.* $G_i \cap G_1 \cdots G_{i-1} \cdot G_{i+1} \cdots G_n = \{e\}$ *pour* $i = 1, \ldots, n$.

**Démonstration** Supposons que $G$ soit le produit direct des $G_i$ et posons

$$\tilde{G} = G_1 \times \cdots \times G_n, \quad \tilde{G}_i = J_i(G_i).$$

Soit $\phi$ soit l'isomorphisme de la définition 9. Comme remarqué précédemment, $\tilde{G}_i \lhd \tilde{G}$ et donc $G_i = \phi(\tilde{G}_i) \lhd \phi(\tilde{G}) = G$. On vérifie facilement que

$$\tilde{G} = \tilde{G}_1 \cdot \widetilde{G}_2 \cdots \tilde{G}_n, \tilde{G}_i \cap \tilde{G}_1 \cdots \tilde{G}_{i-1} \cdot \tilde{G}_{i+1} \cdots \tilde{G}_n = \{e\}.$$

Ces deux propriétés se transportent par $\phi$ pour donner les conditions *i* et *ii*.

Réciproquement, supposons les conditions *i*, *ii* et *iii* satisfaites. Si $a_i \in G_i$ et $b_j \in G_j$ on a

$$a_i \cdot b_j \cdot a_i^{-1} \cdot b_j^{-1} = (a_i \cdot b_j \cdot a_i^{-1}) \cdot b_j^{-1} = a_i \cdot (b_j \cdot a_i^{-1} \cdot b_j^{-1}),$$

et comme $G_i$ et $G_j$ sont distingués on peut conclure que $a_i \cdot b_j \cdot a_i^{-1} \cdot b_j^{-1} \in G_i \cap G_j$. Si $i \neq j$, alors $G_j \subset G_1 \cdots G_{i-1} \cdot G_{i+1} \cdots G_n$ et la condition *ii* permet de conclure que

$$a_i \cdot b_j \cdot a_i^{-1} \cdot b_j^{-1} \in G_i \cap G_j \subset G_i \cap G_1 \cdots G_{i-1} \cdot G_{i+1} \cdots G_n = \{e\}$$

c'est-à-dire que les éléments de deux sous-groupes distincts $G_i \neq G_j$ commutent

$$a_i \cdot b_j = b_j \cdot a_i. \tag{2.8}$$

Soit $\phi : G_1 \times \cdots \times G_n \to G$ donnée par $\phi(a_1, \ldots, a_n) = a_1 \cdots a_n$. Si $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in G_1 \times \cdots \times G_n$ on a $a \cdot b = (a_1 \cdot b_1, \ldots, a_n \cdot b_n)$ et donc

$$\begin{aligned} \phi(a \cdot b) &= (a_1 \cdot b_1) \cdots (a_n \cdot b_n) \\ &= (a_1 \cdots a_n) \cdot (b_1 \cdots b_n) \\ &= \phi(a) \cdot \phi(b), \end{aligned}$$

grâce à la propriété (2.8). $\phi$ est donc un morphisme.

$\phi$ est surjectif par la propriété *i*. Si $a = (a_1, \ldots, a_n) \in \operatorname{Ker} \phi$, la propriété (2.8) permet d'écrire, pour tout $i = 1, \ldots n$,

$$\begin{aligned} a_1 \cdots a_n &= e, \\ a_i \cdot (a_1 \cdots a_{i-1} \cdot a_{i+1} \cdots a_n) &= e, \\ a_1 \cdots a_{i-1} \cdot a_{i+1} \cdots a_n &= a_i^{-1} \in G_1 \cdots G_{i-1} \cdot G_{i+1} \cdots G_n \cap G_i, \end{aligned}$$

et donc $a_i = e$ par la propriété *ii*. On a donc $\operatorname{Ker} \phi = \{e\}$ et $\phi$ est injective. C'est donc un isomorphisme. □

**Remarque 3** Il est évident de la preuve précédente que le produit direct est commutatif, c'est-à-dire que si $G = G_1 \otimes G_2$ alors on a aussi $G = G_2 \otimes G_1$.

**Définition 10** *Un groupe* $G$ *est dit décomposable s'il existe des groupes* $H_1, H_2$ *d'ordres supérieurs à 1 et tels que*

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

*Dans le cas contraire, on dit que* $G$ *est indécomposable.*

Comme nous l'avons vu au début de ce paragraphe, $H_1 \times H_2$ est le produit direct des sous-groupes $\hat{H}_1$ et $\hat{H}_2$. D'autre part si $G = G_1 \otimes G_2$ il est par définition isomorphe a $G_1 \times G_2$. Un groupe est donc décomposable si et seulement si c'est un produit direct de deux de ses sous-groupes d'ordres supérieurs à 1.

Si $G = G_1 \otimes G_2$, on a $G = G_1 \cdot G_2$ et $G_1, G_2$ sont distingués. Le second théorème d'isomorphisme permet d'écrire

$$G/G_2 \simeq G_1/(G_1 \cap G_2),$$

et comme $G_1 \cap G_2 = \{e\}$, on conclut

$$(G_1 \otimes G_2)/G_2 \simeq G_1. \tag{2.9}$$

**Exemple 38** Soit $G = C_6 = \{e, a, \ldots, a^5\}$ le groupe cyclique d'ordre 6. Les sous-groupes $G_1 = \{e, a^2, a^4\}$ et $G_2 = \{e, a^3\}$ sont cycliques d'ordre 3 et 2 respectivement. $G$ étant abélien, ces sous-groupes sont distingués.

On a $G_1 \cdot G_2 = \{e \cdot e, e \cdot a^3, a^2 \cdot e, a^2 \cdot a^3, a^4 \cdot e, a^4 \cdot a^3\} = G$, et donc la propriété *i* du théorème 12. La propriété *ii* est évidente, $G_1 \cap G_2 = \{e\}$.

On a donc $G = G_1 \otimes G_2$ et comme $G_1 \simeq C_3$ et $G_2 \simeq C_2$ on a aussi $C_6 \simeq C_3 \times C_2$. Le groupe $C_6$ est donc décomposable. ♢

**Exemple 39** Soit $G = \{e, a, b, c\}$ le petit groupe de Klein dont la table est donnée par

| · | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

On note que tous ses éléments distincts de l'élément neutre sont d'ordre 2. $G$ n'est donc pas cyclique.

Considérons les sous-groupes engendrés par $a$ et $b$, $G_1 = \{e, a\}$, $G_2 = \{e, b\}$. On a $G_1 \cdot G_2 = \{e \cdot e, e \cdot b, a \cdot e, a \cdot b\} = G$ et $G_1 \cap G_2 = \{e\}$. $G$ étant abélien on a donc $G = G_1 \otimes G_2$. Comme $G_1 \simeq G_2 \simeq C_2$, on a aussi $G \simeq C_2 \times C_2$. Le petit groupe de Klein est donc décomposable.

Si $G_3 = \{e, c\}$, il est clair que nous pouvons montrer de manière analogue que $G = G_1 \otimes G_3 = G_2 \otimes G_3$. La décomposition d'un groupe en produit direct de sous-groupes n'est donc généralement pas unique ♢

Un groupe simple est nécessairement indécomposable. La réciproque est fausse comme le montre l'exemple suivant.

**Exemple 40** Soit $C_4 = \{e, a, a^2, a^3\}$ le groupe cyclique d'ordre 4. Son unique sous-groupe propre est $\{e, a^2\} \simeq C_2$. $C_4$ n'est donc pas simple mais il est indécomposable.♢

## 2.4 Actions de groupe

Si X est un ensemble, $\mathfrak{S}_X$ dénote l'ensemble des bijections de X dans lui-même. Les éléments de $\mathfrak{S}_X$ sont appelés *permutations* de X. $\mathfrak{S}_X$ est un groupe pour la composition des applications. Son élément neutre est l'identité $Id_X$. Le symétrique d'une permutation f est l'application réciproque $f^{-1}$. Si $f \in \mathfrak{S}_X$, on écrit son action sur $x \in X$ comme $f : x \mapsto fx$.

### 2.4.1 Groupes de transformations

Soit X un ensemble. Un groupe de transformations de X est un sous-groupe de $\mathfrak{S}_X$. Un ensemble G d'applications de X dans lui-même est un groupe de transformations de X si et seulement si :

i. $Id_X \in G$.

ii. Pour tout $f, g \in G$, on a $f \cdot g \in G$.

iii. Pour tout $f \in G$, on a $f^{-1} \in G$.

Si G est un groupe de transformations de X, il en est de même de tout sous-groupe de G.

**Exemple 41** Le groupe $\mathcal{G}(G)$ des translations à gauche du groupe G est un groupe de transformations de G lui-même. Il en est de même du groupe des translations à droites $\mathcal{D}(G) = \{d_a \mid a \in G\}$ où $d_a : x \mapsto x \cdot a^{-1}$. On vérifie aisément que $d_a \circ d_b = d_{a\cdot b}$, $d_e = Id_G$ et $d_{a^{-1}} = d_a^{-1}$. ♢

**Exemple 42** Le groupe $Aut(G)$ et son sous-groupe $Int(G)$ sont eux aussi des groupes de transformations du groupe G. ♢

**Exemple 43** Si $x \in X$, $\mathfrak{S}_x = \{f \in \mathfrak{S}_X \mid fx = x\}$ est un groupe de transformations de X.

i. $Id_X(x) = x$, et donc $Id_X \in \mathfrak{S}_x$.

ii. $fgx = fx = x$ pour $f, g \in \mathfrak{S}_x$.

iii. $f^{-1}x = x$ pour $f \in \mathfrak{S}_x$.

$\mathfrak{S}_x$ est le *groupe d'isotropie* de $x$. ♢

**Exemple 44** Soit $P : X \to Y$ une application. L'ensemble

$$\mathfrak{S}^P = \{f \in \mathfrak{S}_X \mid P(fx) = P(x) \text{ pour tout } x \in X\},$$

est un groupe de transformations de $X$.

i. $P(\mathrm{Id}_X(x)) = P(x)$.

ii. $P(fgx) = P(gx) = P(x)$.

iii. $y = fx$ et $P(x) = P(fx) \Rightarrow P(f^{-1}y) = P(y)$.

$\mathfrak{S}^P$ est le *groupe d'invariance* de $P$. ♢

**Exemple 45** Dans l'espace vectoriel $\mathbb{R}^{p+n}$ on considère la forme quadratique non-dégénérée

$$Q[x] = (x_1^2 + \cdots + x_p^2) - (x_{p+1}^2 + \cdots + x_{p+n}^2).$$

L'ensemble $O(p,n)$ des applications linéaires $a : \mathbb{R}^{p+n} \to \mathbb{R}^{p+n}$ telles que

$$Q[Ax] = Q[x],$$

pour tout $x$ est un groupe de transformations.

i. $\mathrm{Id}_{\mathbb{R}^n} \in O(p,n)$.

ii. $Q[abx] = Q[bx] = Q[x]$.

iii. $a \in O(p,n)$ est non-singulière. En effet, si on dénote par $q$ la matrice symétrique associée à $Q$, on doit avoir $a^\top q a = q$ et comme $\det q = (-1)^n \neq 0$, $\det a = \pm 1$. On vérifie donc $a^{-1} \in O(p,n)$ comme dans l'exemple précédent.

$SO(p,n) = \{a \in O(p,n) \mid \det a = 1\}$ est un sous-groupe. C'est donc aussi un groupe de transformations de $\mathbb{R}^{p+n}$.

Cas particuliers.

1. Si $n = 0$ on a $q = \mathrm{Id}_{\mathbb{R}^p}$ et on retrouve le groupe orthogonal $O(p)$.
2. Si $p = 3$ et $n = 1$, on obtient le *groupe de Lorentz* $L$.
3. Soit $\mathbb{R}^4_+ = \{(x_1,x_2,x_3,x_4) \in \mathbb{R}^4 \mid x_1^2 + x_2^2 + x_3^2 - x_4^2 < 0, x_4 \geqslant 0\}$. L'ensemble des $a \in L$ tels que
$$a\mathbb{R}^4_+ \subset \mathbb{R}^4_+,$$
est un sous-groupe $L_+$ de $L$, le *groupe de Lorentz orthochrone.* ♢

**Exemple 46** Dans le plan affine $\mathbb{R}^2$, soit $P_n$ un polygone régulier à $n$ sommets centré à l'origine. L'ensemble des transformations affines qui laissent $P_n$ invariant est un sous-groupe du groupe orthogonal $O(2)$. C'est donc un groupe de transformation du plan. Il est formé des rotations et des réflexions orthogonales qui transforment $P_n$ dans lui-même.

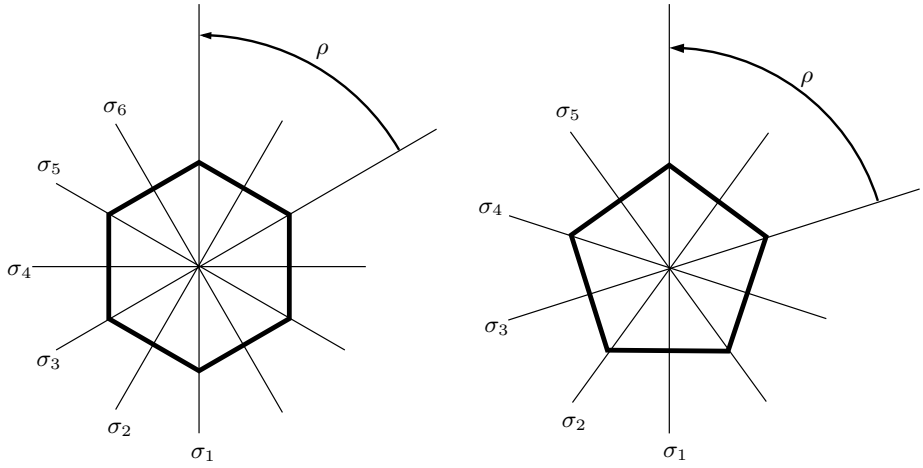


Fig. 2.2 – Transformations laissant l'hexagone et le pentagone invariant.

Il apparaît clairement dans la figure 2.2 que les rotations qui laissent invariant $P_n$ doivent avoir des angles de rotations multiples de $2\pi/n$. On note également la présence de $n$ axes de symétrie $\sigma_1, \ldots, \sigma_n$. Le groupe d'invariance de $P_n$ est donc un sous-groupe d'ordre $2n$ du groupe orthogonal $O(2)$. Comme il ne contient pas uniquement des rotations, c'est le groupe diédral $D_n$ de la section 2.3.5.

### 2.4.2 Action d'un groupe sur un ensemble

On dit qu'un groupe $G$ *opère* sur l'ensemble $X$ s'il existe une application

$$\begin{aligned} G \times X &\to X \\ (a, x) &\mapsto ax, \end{aligned}$$

appelée *action de* $G$ *dans* $X$, telle que :

i. $a(bx) = (a \cdot b)x$ pour tout $a, b \in G$ et pour tout $x \in X$.

ii. $ex = x$ pour tout $x \in X$.

La restriction d'une action de $G$ dans $X$ à un sous-groupe $H$ de $G$ définit évidement une action de $H$ dans $X$. Si $G$ opère sur $X$, il en va donc de même pour tous ses sous-groupes.

Etant donnée une action de $G$ dans $X$, pour tout $a \in G$, on peut définir une application $\theta_a : X \mapsto X$ par $\theta_a(x) = ax$. On a donc

$$\theta_a \circ \theta_b(x) = \theta_a(\theta_b(x)) = a\theta_b(x) = a(bx) = (a \cdot b)x = \theta_{a \cdot b}(x),$$

pour tout $x \in X$ et $\theta_e = \mathrm{Id}_X$. Comme $\theta_a \circ \theta_{a^{-1}} = \theta_{a^{-1}} \circ \theta_a = \theta_e = \mathrm{Id}_X$, $\theta_a$ est bijective pour tout $a \in G$. L'application $\theta : a \mapsto \theta_a$ est donc un morphisme de $G$ dans $\mathfrak{S}_X$ et et son image $\mathrm{Im}\,\theta$ est un groupe de transformations de $X$. Ce groupe est isomorphe au groupe quotient $G/\mathrm{Ker}\,\theta$.

**Exemple 47** L'espace vectoriel $\mathbb{R}^n$ opère (comme groupe abélien) sur l'espace affine $\mathbb{R}^n$ par l'action $(a, x) \mapsto x + a$. Le morphisme $\theta$ es défini par $\theta_a(x) = x + a$. Son image est le groupe $T(\mathbb{R}^n)$ des translations de l'espace affine $\mathbb{R}^n$. Son noyau est trivial $\operatorname{Ker}\theta = \{0\}$ c'est-à-dire que $T(\mathbb{R}^n) \simeq \mathbb{R}^n$. ♢

**Exemple 48** Soient $X$ et $Y$ des ensembles et $G$ un groupe de transformations de $X$. $G$ opère sur $Y^X$ par l'action $(af)(x) = f(a^{-1}x)$. Dans ce cas on a donc $\theta_a(f) = f \circ a^{-1}$. ♢

**Exemple 49** Un groupe $G$ opère sur lui-même par ses translations à gauches

$$\begin{array}{rcl} G \times G & \to & G \\ (a, x) & \mapsto & g_a(x) = a \cdot x. \end{array}$$

Dans ce cas $\theta_a = g_a$ et nous avons déjà remarqué que $\theta : a \mapsto g_a$ est un isomorphisme de $G$ dans $\mathcal{G}(G)$(*c.f.* exemple 34). ♢

**Exemple 50** Un groupe $G$ opère également sur lui-même par ses translations à droite

$$\begin{array}{rcl} G \times G & \to & G \\ (a, x) & \mapsto & d_a(x) = x \cdot a^{-1}. \end{array}$$

Dans ce cas $\theta_a = d_a$ et $\theta : a \mapsto d_a$ est un isomorphisme de $G$ dans $\mathcal{D}(G)$. ♢

**Exemple 51** Le groupe $\operatorname{Aut}(G)$ opère naturellement sur $G$

$$\begin{array}{rcl} \operatorname{Aut}(G) \times G & \to & G \\ (\phi, x) & \mapsto & \phi(x). \end{array}$$

Dans ce cas, $\theta = i_{\operatorname{Aut}(G)}$ est l'injection canonique de $\operatorname{Aut}(G)$ dans $\mathfrak{S}_G$.

Cette action permet, via le morphisme $j : G \to \operatorname{Aut}(G)$, de définir une autre action de $G$ dans lui-même

$$\begin{array}{rcccl} G \times G & \to & \operatorname{Aut}(G) \times G & \to & G \\ (a, x) & \mapsto & (j_a, x) & \mapsto & j_a(x) = a \cdot x \cdot a^{-1} \end{array} \tag{2.10}$$

Dans ce cas $\theta_a = j_a$ et, comme nous l'avons vu dans l'exemple 32, $\theta$ est un isomorphisme de $G/Z(G)$ dans $\operatorname{Int}(G)$. ♢

Si le groupe $G$ opère sur $X$, la relation définie par

$$x R_G y \Leftrightarrow \text{il existe } a \in G \text{ tel que } y = ax,$$

est une relation d'équivalence :

i. $x = ex \Rightarrow x R_G x$.

ii. $x R_G y \Rightarrow y = ax \Rightarrow a^{-1}y = a^{-1}(ax) = ex = x \Rightarrow y R_G x$.

iii. $xR_G y$ et $yR_G z \Rightarrow y = ax$ et $z = by \Rightarrow z = bax = (b \cdot a)x \Rightarrow xR_G z$.

La classe d'équivalence de $x \in X$ pour $R_G$ est

$$Gx = \{ax \mid a \in G\},$$

qu'on appelle G-*orbite* de $x$. Le quotient $X/R_G$ est donc l'ensemble des G-orbites que l'on note

$$\Omega(X|G) = \{Gx \mid x \in X\}.$$

Un ensemble sur lequel opère un groupe G est donc naturellement partitionné en G-orbites. On dit que G opère *transitivement* sur X si cette partition ne contient qu'une seule orbite, c'est-à-dire si $|\Omega(X|G)| = 1$.

Le *stabilisateur* de $x \in X$ est $G_x = \{a \in G \mid ax = x\}$. C'est un sous-groupe de G :

i. $a, b \in G_x \Rightarrow ax = x$ et $bx = x \Rightarrow (a \cdot b)x = a(bx) = ax = x \Rightarrow a \cdot b \in G_x$.

ii. $ex = x \Rightarrow e \in G_x$.

iii. $a \in G_x \Rightarrow ax = x \Rightarrow x = a^{-1}x \Rightarrow a^{-1} \in G_x$.

Deux éléments $x$ et $y$ d'une G-orbite ont des stabilisateurs isomorphes. En effet, supposons que $y = ax$. Alors $b \in G_y$ si et seulement si $b(ax) = ax$ c'est à dire $(a^{-1} \cdot b \cdot a)x = x$ ou encore $a^{-1} \cdot b \cdot a \in G_x$. On peut donc conclure que $G_y = j_a(G_x)$. En particulier, si $G_x$ est fini, on a $|G_x| = |G_y|$.

Un *point fixe* de $a \in G$ est un élément $x \in X$ tel que $ax = x$. On dénote par Fix $a$ l'ensemble des points fixes de $a$.

**Théorème 13** *La* G*-orbite d'un point* $x$ *est équipotente au quotient* $G/G_x$. *En particulier, elle est finie si et seulement si l'indice de* $G_x$ *dans G l'est et on a alors*

$$|Gx| = [G : G_x]. \tag{2.11}$$

**Démonstration** Soient $a, b \in G$, alors

$$ax = bx \Leftrightarrow (a^{-1} \cdot b)x = x \Leftrightarrow a^{-1} \cdot b \in G_x \Leftrightarrow b \in aG_x \Leftrightarrow aG_x = bG_x,$$

et l'application $\varphi : Gx \to G/G_x$ donnée par $\varphi(ax) = aG_x$ est donc bijective. □

Un système de représentants de $\Omega(X|G)$ est un ensemble $\mathcal{X} \subset X$ contenant un et un seul élément de chaque G-orbite.

**Corollaire 2** *Si le groupe fini* G *opère sur l'ensemble* X *et si* $\mathcal{X}$ *est un système de représentants de* $\Omega(X|G)$, *alors*

$$|X| = \sum_{x \in \mathcal{X}} [G : G_x], \tag{2.12}$$

*si* X *est fini et*

$$\sum_{x \in \mathcal{X}} \left(1 - \frac{1}{|G_x|}\right) = \frac{1}{|G|} \sum_{a \in G \setminus \{e\}} |\operatorname{Fix} a|. \tag{2.13}$$

**Démonstration** $\Omega(X|G)$ étant une partition de X, la première assertion est une conséquence directe de la formule 1.3.8.xi et du théorème 13.

Pour démontrer la seconde assertion, considérons l'ensemble

$$M = \{(a, x) \in G \setminus \{e\} \times X \,|\, ax = x\}.$$

On a d'une part

$$M = \bigcup_{a \in G\setminus\{e\}} \{a\} \times \operatorname{Fix} a,$$

et donc $|M| = \sum_{a\in G\setminus\{e\}} |\operatorname{Fix} a|$ et d'autre part

$$M = \bigcup_{x\in X} (G_x \setminus \{e\}) \times \{x\},$$

et $|M| = \sum_{x\in X}(|G_x| - 1) = \sum_{\omega\in\Omega(X|G)} \sum_{y\in\omega}(|G_y| - 1)$. Comme $\omega \in \Omega(X|G)$ et $x, y \in \omega$ impliquent que $G_x \simeq G_y$ et donc $|G_x| = |G_y|$ et $|\omega| = [G : G_x] = |G|/|G_x|$ on obtient bien

$$\sum_{a\in G\setminus\{e\}} |\operatorname{Fix} a| = |M| = \sum_{x\in X} |G|(1 - \frac{1}{|G_x|}).$$

□

**Exemple 52** Considérons l'action naturelle du groupe diédral $G = D_4$ sur l'ensemble $X = \{1, 2, 3, 4\}$ des sommets d'un carré. Si on note $\rho$ la rotation d'angle $\pi/2$ autour de l'origine $\mathcal{O}$ du plan affine (voir figure 2.3) et $\sigma$ la réflexion à l'axe de symétrie parallèle au coté $\overline{12}$ on a $G = \{I, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$.

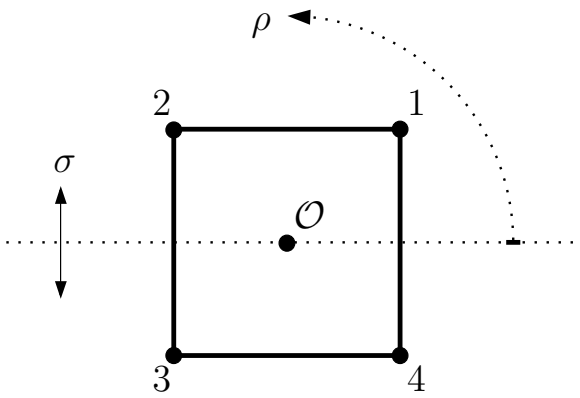


Fig. 2.3 – Le groupe $D_4$ agit naturellement sur l'ensemble des sommet d'un carré.

L'action de $\rho$ et $\sigma$ sur X est décrite par les permutations

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

On a par exemple $\rho 3 = 4$, $\sigma 2 = 3$ et $\sigma\rho^3 1 = \sigma\rho^2 2 = \sigma\rho 3 = \sigma 4 = 1$. On remarque que sous l'action répétée de $\rho$ on a $1 \mapsto 2 \mapsto 3 \mapsto 4$. On a donc $G1 = X$, il n'y a qu'une seule G-orbite et G agit transitivement sur X.

La seule rotation laissant le sommet 1 fixé est I. La seule réflexion est celle d'axe $\overline{13}$, c'est-à-dire $\sigma\rho^3$. Le stabilisateur du sommet 1 est donc $G_1 = \{I, \sigma\rho^3\}$. Les classes à gauche de $G_1$ sont

$$\begin{array}{rcccl} IG_1 & = & \sigma\rho^3 G_1 & = & \{I, \sigma\rho^3\}, \\ \rho G_1 & = & \sigma\rho^2 G_1 & = & \{\rho, \sigma\rho^2\}, \\ \rho^2 G_1 & = & \sigma\rho G_1 & = & \{\rho^2, \sigma\rho\}, \\ \rho^3 G_1 & = & \sigma G_1 & = & \{\rho^3, \sigma\}. \end{array}$$

En particulier on vérifie la formule (2.12) : $4 = |G1| = [G : G_1] = |G|/|G_1| = 8/2$. On note finalement que $\operatorname{Fix} I = 4$, $\operatorname{Fix} a = 2$ si $a$ est une réflexion par rapport à une des diagonales du carré et $\operatorname{Fix} a = 0$ dans tous les autres cas. On a donc

$$\frac{1}{2} = 1 - \frac{1}{|G_1|} = \frac{1}{|G|} \sum_{a \in G \setminus \{e\}} |\operatorname{Fix} a| = \frac{1}{8}(3 \cdot 0 + 2 \cdot 2 + 2 \cdot 0),$$

conformément à la formule (2.13). ♢

### 2.4.3 Classes de conjugaison

Soit G un groupe. Deux éléments $a, b \in G$ sont *conjugués* s'il existe $u \in G$ tel que $a \cdot u = u \cdot b$, c'est-à-dire $a = j_u(b)$. Similairement, deux sous-ensembles $A, B \subset G$ sont dits conjugués si $A = j_u(B)$ pour un élément $u \in G$.

Nous avons vu dans l'exemple 51 que G opère sur lui-même par l'action (2.10). La G-orbite de $a \in G$ pour cette action, $\{u \cdot a \cdot u^{-1} \mid u \in G\}$, est appelée *classe de conjugaison* de $a$. G est donc partitionné en classes de conjugaison. La classe de conjugaison de $e$ est $\{e\}$. Plus généralement, la classe de conjugaison d'un élément $a \in G$ est réduite à $\{a\}$ si et seulement si $a \cdot u = u \cdot a$ pour tous les $u \in G$, c'est-à-dire si $a \in Z(G)$. Si G est abélien, $Z(G) = G$ et toutes les classes de conjugaison sont réduites à un élément.

Le stabilisateur de $a \in G$ pour l'action (2.10) est appelé *centralisateur* de $a$ et est noté $N_a$. C'est l'ensemble des éléments de G qui commutent avec $a$

$$N_a = \{x \in G \mid xa = ax\},$$

et donc $Z(G) \subset N_a$. Si G est abélien on a donc $N_a = G$ pour tout $a \in G$. Le théorème 13 et son corollaire 2 donnent dans ce contexte

**Théorème 14** *Soit* G *un groupe fini et* $\mathcal{X}$ *un ensemble de représentants de ses classes de conjugaison. On a alors l'équation des classes de* G

$$|G| = \sum_{x \in \mathcal{X}} [G : N_x] = |Z(G)| + \sum_{x \in \mathcal{X} \setminus Z(G)} [G : N_x],$$

*où* $|Z(G)|$ *et* $|[G : N_x]|$ *sont des diviseurs de* $|G|$ *et* $|[G : N_x]| > 1$ *pour tous les représentants* $x \in \mathcal{X} \setminus Z(G)$.

L'équation des classes d'un groupe abélien est triviale. Par contre, comme nous le verrons au paragraphe suivant, elle fournit des informations intéressantes lorsque G n'est pas abélien.

**Exemple 53** Considérons le groupe diédral $D_n = \{\rho^k, \sigma\rho^k \,|\, k = 0, \dots n-1\}$. On calcule aisément, à l'aide des relations (2.7) les classes de conjugaison de $D_n$,

$$\begin{aligned} j_{\rho^k}(\rho^l) &= \rho^k\rho^l\rho^{-k} = \rho^l, \\ j_{\rho^k}(\sigma\rho^l) &= \rho^k(\sigma\rho^l)\rho^{-k} = \sigma(\sigma\rho^k\sigma)\rho^{l-k} = \sigma\rho^{l-2k}, \\ j_{\sigma\rho^k}(\rho^l) &= \sigma\rho^k\rho^l\rho^{-k}\sigma = \rho^{-l}, \\ j_{\sigma\rho^k}(\sigma\rho^l) &= \sigma\rho^k(\sigma\rho^l)\rho^{-k}\sigma = \sigma\rho^k(\sigma\rho^{l-k}\sigma) = \sigma\rho^{2k-l}. \end{aligned}$$

Si $n = 2N$ est pair, les rotations se groupent en $N-1$ classes contenant chacune 2 éléments mutuellement réciproques et deux classe contenant un seul élément, l'identité I et la rotation d'angle $\pi$, $\rho^N = -I$ (symétrie centrale),

$$\{I\}, \{\rho, \rho^{-1}\}, \{\rho^2, \rho^{-2}\}, \dots, \{\rho^{N-1}, \rho^{-(N-1)}\}, \{\rho^N\}.$$

Les réflexions forment 2 classes de N éléments

$$\{\sigma\rho^{2k} \,|\, k = 0, \dots, N-1\}, \{\sigma\rho^{2k+1} \,|\, k = 0, \dots, N-1\}.$$

Le centre du groupe est dans ce cas formé de deux éléments

$$Z(D_{2N}) = \{I, -I\}.$$

L'équation des classes est donc

$$n = 4N = 2 + (N-1) \cdot 2 + 2 \cdot N.$$

Lorsque $n = 2N + 1$ est impair, les rotations forment N classes de deux éléments et une seule classe d'un élément,

$$\{I\}, \{\rho, \rho^{-1}\}, \{\rho^2, \rho^{-2}\}, \dots, \{\rho^N, \rho^{-N}\}.$$

Les réflexions ne forment alors plus qu'une classe de 2N éléments

$$\{\sigma\rho^k \,|\, k = 0, \dots, n-1\}.$$

Dans ce cas le centre se réduit à l'identité

$$Z(D_{2N+1}) = \{I\},$$

et l'équation des classes est

$$n = 2N + 1 = 1 + N \cdot 2 + 1 \cdot 2N.$$

♢

## 2.5 Groupes finis

### 2.5.1 Exposant d'un groupe fini

Soient G un groupe fini, $a \in G$ et $\omega(a)$ son ordre. $L_a = \{n \in \mathbb{Z} \mid a^n = e\}$ est un sous-groupe du groupe additif $\mathbb{Z}$. Il est engendré par $\omega(a)$ et comme $\omega(a)$ divise $|G|$ on a $L_a = \omega(a)\mathbb{Z} \supset |G|\mathbb{Z}$. L'intersection de la famille $(L_a)_{a\in G}$ est donc un sous-groupe non-trivial de $\mathbb{Z}$ et il existe un diviseur M de $|G|$ tel que

$$L = \bigcap_{a\in G} L_a = \{n \in \mathbb{Z} \mid a^n = e \text{ pour tout } a \in G\} = M\mathbb{Z} \supset |G|\mathbb{Z}.$$

L'entier M peut donc s'exprimer comme

$$M = \min\{n \in L \mid n > 0\} = \min\{n > 0 \mid a^n = e \text{ pour tout } a \in G\}, \tag{2.14}$$

c'est le plus petit entier positif tel que $a^M = e$ pour tout $a \in G$. D'autre part,

$$M\mathbb{Z} = \bigcap_{a\in G} \omega(a)\mathbb{Z},$$

permet de conclure que

$$M = \text{PPCM}\{\omega(a) \mid a \in G\}. \tag{2.15}$$

L'entier M est appelé *exposant du groupe* G et noté exp G.

**Exemple 54** Si G est cyclique d'ordre n, et a un générateur, on a $x^n = e$ pour tout $x \in G$, mais $a^l \neq e$ pour $1 \leqslant l < n$. Il suit de (2.14) que $\exp G = n$. ♢

Si H est un sous-groupe de G, alors

$$\exp H\mathbb{Z} = \bigcap_{a\in H} \omega(a)\mathbb{Z} \supset \bigcap_{a\in G} \omega(a)\mathbb{Z} = \exp G\mathbb{Z},$$

et donc exp H divise exp G.

**Exemple 55** Si n est pair, $\exp D_n = n$. En effet, pour $k = 0, \ldots, n-1$ on a $(\rho^k)^n = (\rho^n)^k = I$ et $(\sigma\rho^k)^n = ((\sigma\rho^k)^2)^{n/2} = I$ alors que $\rho^l \neq I$ pour $1 \leqslant l < n$.

Si n est impair, $\exp D_n = 2n$. Pour $k = 0, \ldots, n-1$ on a $(\rho^k)^{2n} = (\rho^n)^{2k} = I$ et $(\sigma\rho^k)^{2n} = ((\sigma\rho^k)^2)^n = I$ alors que $\rho^l \neq I$ pour $1 \leqslant l < n$, $\sigma^n = \sigma \neq I$ et $\rho^l \neq I$ pour $n+1 \leqslant l < 2n$.

Dans les deux cas, le sous-groupe des rotations $\mathcal{R}_n = (\rho) \subset D_n$ est cyclique d'ordre n et donc $\exp \mathcal{R}_n = n$ divise $\exp D_n$. ♢

Si $\phi : G \to H$ est un morphisme, alors $a^n = e$ implique $\phi(a)^n = \phi(a^n) = \phi(e) = e$ c'est-à-dire que $L_a \subset L_{\phi(a)}$. De

$$\operatorname{Exp}(\operatorname{Im}\phi)\mathbb{Z} = \bigcap_{a\in G} L_{\phi(a)} \supset \bigcap_{a\in G} L_a = \operatorname{Exp} G\mathbb{Z},$$

nous pouvons conclure que $\operatorname{Exp}(\operatorname{Im}\phi)$ divise $\operatorname{Exp} G$. Si $\phi$ est surjectif, $\operatorname{Exp} H$ divise donc $\operatorname{Exp} G$. Si $\phi$ est injectif, $\phi(a)^n = e$ implique $\phi(a^n) = e$ et donc $a^n = e$. Dans ce cas on a $L_a = L_{\phi(a)}$ et $\operatorname{Exp}(\operatorname{Im}\phi) = \operatorname{Exp} G$. Comme $\operatorname{Im}\phi$ est un sous-groupe de $H$, $\operatorname{Exp} G$ divise donc $\operatorname{Exp} H$. En particulier, si $\phi$ est un isomorphisme, c'est-à-dire si $G \simeq H$, on a $\operatorname{Exp} G = \operatorname{Exp} H$.

Si $H \lhd G$, le résultat précédent s'applique au morphisme surjectif $\pi : G \to G/H$ et montre que $\operatorname{Exp} G/H$ divise $\operatorname{Exp} G$.

**Théorème 15** *Soit* $G$ *un groupe fini et* $\operatorname{Exp} G$ *son exposant.*

*i.* *Pour tout* $a \in G$, $a^{\operatorname{Exp} G} = e$ *et si* $a^n = e$ *pour tout* $a \in G$, $n$ *est un multiple de* $\operatorname{Exp} G$.

*ii.* $\operatorname{Exp} G = \operatorname{PPCM}\{\omega(a) \mid a \in G\}$.

*iii.* $\operatorname{Exp} G$ *divise* $|G|$.

*iv.* *Si* $H$ *est un sous-groupe de* $G$, $\operatorname{Exp} H$ *divise* $\operatorname{Exp} G$.

*v.* *Si* $H \lhd G$, $\operatorname{Exp} G/H$ *divise* $\operatorname{Exp} G$.

*vi.* *Si* $\phi \in \operatorname{Hom}(G, H)$, $\operatorname{Exp}(\operatorname{Im}\phi)$ *divise* $\operatorname{Exp} G$. *Si* $\phi$ *est surjectif,* $\operatorname{Exp} H$ *divise* $\operatorname{Exp} G$. *Si* $\phi$ *est injectif,* $\operatorname{Exp} G$ *divise* $\operatorname{Exp} H$.

*vii.* *Si* $H \simeq G$, $\operatorname{Exp} H = \operatorname{Exp} G$.

### 2.5.2 Exposant d'un groupe abélien fini

Soit $G$ un groupe abélien fini et $p$ un nombre premier tel que $p^l$ divise $\exp G$ pour un entier $l \geqslant 1$. Comme $\exp G = \operatorname{PPCM}\{\omega(a) \mid a \in G\}$, il existe un $a \in G$ tel que $p^l$ divise $\omega(a)$. Soit $k = \omega(a)/p^l$, alors $b = a^k$ est d'ordre $p^l$. En effet, on a d'une part $b^{p^l} = a^{kp^l} = a^{\omega(a)} = e$ et d'autre part, pour $j = 1, 2, \ldots, p^l - 1$, on a $b^j = a^{jk} \neq e$ puisque $jk < \omega(a)$. Soit maintenant $n$ un diviseur de $\exp G$. Alors $n = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$ où les $p_i$ sont des diviseurs premiers de $\exp G$ et $l_i \geqslant 1$. Pour chaque $i$ il existe un élément $b_i \in G$ d'ordre $p_i^{l_i}$. L'invocation répétée du lemme 2 montre que $b_1 \cdot b_2$ es d'ordre $p_1^{l_1} p_2^{l_2}$, $b_1 \cdot b_2 \cdot b_3$ d'ordre $p_1^{l_1} p_2^{l_2} p_3^{l_3}$,..., et donc $b_1 \cdot b_2 \cdots b_r$ d'ordre $n$.

**Lemme 3** *Soit* $G$ *un groupe abélien fini. Si* $n$ *divise* $\exp G$, *il existe un élément d'ordre* $n$ *dans* $G$.

En particulier, $G$ contient un élément d'ordre $\exp G$, et la relation (2.15) permet ce conclure :

**Corollaire 3** *Si* $G$ *est un groupe abélien fini, alors*

$$\exp G = \max\{\omega(a) \mid a \in G\}.$$

*En particulier,* $\operatorname{Exp} G = |G|$ *si et seulement si* $G$ *est cyclique.*

**Corollaire 4** *Si* $G$ *est un groupe abélien fini,* $|G|$ *divise une puissance de* $\operatorname{Exp} G$.

**Démonstration** Par induction sur $|G|$. Si $|G| = 1$, on a $G = \{e\}$ et par conséquent $\operatorname{Exp} G = 1$. Supposons que pour tout groupe abélien $G$ tel que $|G| < N$, $|G|$ divise une puissance de $\operatorname{Exp} G$. Soit $G$ un groupe abélien d'ordre $N$. Si $G$ est cyclique, $\operatorname{Exp} G = |G|$ et donc $|G|$ divise $\operatorname{Exp} G$. Si $G$ n'est pas cyclique, il contient un élément $a \neq e$ tel que $\omega(a) = \operatorname{Exp} G < |G|$. Le groupe $H = G/(a)$ est abélien d'ordre $|H| = [G : (a)] = |G|/|(a)| = |G|/\omega(a) = |G|/\operatorname{Exp} G < |G| = N$. L'hypothèse d'induction implique que $|H|$ divise une puissance de $\operatorname{Exp} H$. Il existe donc des entiers $l$ et $k$ tels que $(\operatorname{Exp} H)^k = l|H| = l|G|/\operatorname{Exp} G$. Comme $H$ est un quotient de $G$, $\operatorname{Exp} H$ divise $\operatorname{Exp} G$ et $\operatorname{Exp} G = m \operatorname{Exp} H$ pour un entier $m$. On a donc

$$(\operatorname{Exp} G)^k = m^k(\operatorname{Exp} H)^k = m^k l|G|/\operatorname{Exp} G,$$

d'où on peut conclure que $|G|$ divise $(\operatorname{Exp} G)^{k+1}$ terminant ainsi l'induction. □

Le lemme 3 et son corollaire 3 sont faux si on supprime l'hypothèse que $G$ est abélien. Un contre-exemple est donné par le groupe diédral $D_9$. D'après l'exemple 55, on a $\operatorname{Exp} D_9 = 18$. Les rotations de $D_9$ sont toutes d'ordre 9 sauf $I$ d'ordre 1 et $\rho_9^3$ d'angle $2\pi/3$ et $\rho_9^6$ d'angle $4\pi/3$ qui sont d'ordre 3. Les réflexions de $D_9$ sont quand-à-elles d'ordre 2. Il n'y a donc aucun élément d'ordre 6 dans $D_9$, bien que 6 soit un diviseur de 18. De manière plus générale, si $n$ est impair on a, toujours d'après l'exemple 55, $\operatorname{Exp} D_n = 2n$ alors qu'on vérifie aisément que

$$\max\{\omega(a) \mid a \in D_n\} = n,$$

pour $n \geqslant 2$.

### 2.5.3 p-groupes

Nous savons qu'un groupe d'ordre premier est cyclique. Les groupes dont l'ordre est une puissance positive d'un nombre premier ne sont pas nécessairement cycliques comme le montre le groupe d'ordre $4 = 2^2$ de l'exemple 39. Ils jouent toutefois un rôle important dans l'étude des groupes finis, et particulièrement des groupes abéliens.

Un groupe fini $G$ est un $p$-*groupe* si $|G| = p^n$ pour un nombre premier $p$ et un entier $n \geqslant 0$. Si $H$ est un sous-groupe du $p$-groupe $G$, son ordre divise $p^n$. On a donc $|H| = p^m$ pour un entier $m \leqslant n$. Un sous-groupe d'un $p$-groupe est lui-même un $p$-groupe. En particulier, le sous-groupe $(a)$ engendré par un élément quelconque

$a \in G$ est un p-groupe. L'ordre de $a$ est donc une puissance de $p$. Si $H$ est distingué dans $G$, l'ordre du groupe quotient $G/H$ est $[G : H] = |G|/|H| = p^{n-m}$. Le quotient d'un p-groupe est donc aussi un p-groupe.

Si $G$ est un p-groupe d'ordre supérieur à un, son centre est non-trivial : $Z(G) \neq \{e\}$. En effet, $p$ divise $|G|$ et tous les $[G : N_x]$, $x \in \mathcal{X} \setminus Z(G)$. L'équation des classes implique que $p$ divise aussi $|Z(G)|$ et donc que $|Z(G)| > 1$. Si $G$ n'est pas abélien, on a de plus $Z(G) \neq G$ et donc $Z(G)$ est un sous-groupe propre distingué de $G$.

**Corollaire 5** *Un p-groupe non-abélien n'est pas simple. Son centre $Z(G)$ est un sous-groupe propre distingué.*

Considérons maintenant le cas d'un p-groupe abélien $G$ d'ordre $p^n$. Si $n = 1$, $G$ n'a pas de sous-groupe propre, il est donc simple. Si $n > 1$ et $G$ est cyclique, $G = (a) = \{e, a, \ldots, a^{p^n-1}\}$ et $a^{p^n} = e$. Donc $a^{p^{n-1}}$ engendre un sous-groupe cyclique $(a^{p^{n-1}}) = \{e, a^{p^{n-1}}, \ldots, a^{(p-1)p^{n-1}}\}$ d'ordre $p$ et $G$ n'est pas simple. Si au contraire $G$ n'est pas cyclique il contient un élément $a \neq e$ tel que $(a) \neq G$. $G$ n'est donc pas simple.

**Corollaire 6** *Un p-groupe $G$ est simple si et seulement si $|G| = p$. Dans ce cas il est cyclique $G \simeq C_p$.*

Un groupe $G$ est *résoluble* s'il existe une suite décroissante de sous-groupes

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n = \{e\},$$

telle que pour tout $i = 1, \ldots, n$ le groupe quotient $F_i = G_{i-1}/G_i$, soit abélien. Les groupes résolubles jouent un rôle important notamment dans la théorie de Galois des équations algébriques.

**Théorème 16** *Un p-groupe est résoluble.*

**Démonstration** Si $|G| = 1$ cette assertion est évidente, $\{e\} = G = G_0 \rhd G_1 = \{e\}$ implique que $F_1 = \{e\}$. Supposons donc que l'assertion est vraie pour tous les p-groupes d'ordre inférieur à $p^n$ et soit $G$ un p-groupe d'ordre $p^n$. Le centre de $G$ étant non-trivial on a $|Z(G)| = p^r$ avec $r > 0$ et donc $[G : Z(G)] = p^{n-r}$. Le quotient $G/Z(G)$ est donc un p-groupe d'ordre inférieur à $p^n$ et par conséquent il est résoluble. Il existe donc une suite

$$G/Z(G) = Q_0 \rhd Q_1 \rhd \cdots \rhd Q_{n-1} \rhd Q_n = \{e \cdot Z(G)\},$$

telle que les quotients $Q_{i-1}/Q_i$ soient abéliens.

Soit $\pi : G \to G/Z(G)$ la surjection canonique. $\pi$ étant un morphisme les pré-images $G_i = \pi^{-1}(Q_i)$ sont des sous-groupes de $G$. On a $G_0 = \pi^{-1}(G/Z(G)) = G$ et $G_n = \pi^{-1}(\{e \cdot Z(G)\}) = Z(G)$.

Soit $\phi$ la restriction de $\pi$ a $G_{i-1}$. C'est donc un morphisme surjectif de $G_{i-1}$ dans $Q_{i-1}$ et $\phi^{-1}(Q_i) = \pi^{-1}(Q_i) = G_i$. Comme on a $Q_i \lhd Q_{i-1}$, il suit que $\phi^{-1}(Q_i) \lhd G_{i-1}$ (*c.f.* paragraphe 2.3.2) et donc $G_i \lhd G_{i-1}$.

Soit $\rho : Q_{i-1} \to Q_{i-1}/Q_i$ la surjection canonique, le morphisme

$$\rho \circ \phi : G_{i-1} \to Q_{i-1}/Q_i,$$

est donc lui aussi surjectif. $Q_i$ étant le noyau de $\rho$, le noyau de $\rho \circ \phi$ est $\phi^{-1}(Q_i) = G_i$. On a donc un isomorphisme $G_{i-1}/G_i \simeq Q_{i-1}/Q_i$. Le quotient $Q_{i-1}/Q_i$ étant abélien, $G_{i-1}/G_i$ l'est aussi pour $i = 1, \ldots, n$.

Finalement, le centre $Z(G)$ étant abélien, on a $G_n = Z(G) \lhd G_{n+1} = \{e\}$ avec un quotient $G_n/G_{n+1} \simeq Z(G)$ abélien. La suite

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n \rhd G_{n+1} = \{e\},$$

a donc toutes les propriétés requises, ce qui termine l'induction. □

Un sous-groupe $H$ d'un groupe $G$ est appelé $p$-*sous-groupe* si c'est un $p$-groupe et $p$-*sous-groupe de Sylow* si c'est un $p$-sous-groupe maximal, c'est-à-dire s'il contient tous les $p$-sous-groupes de $G$.

### 2.5.4 $p$-groupes abéliens

Nous avons déjà remarqué que le groupe $C_4$ était indécomposable (exemple 40). De manière plus générale, nous allons voir que les $p$-groupes cycliques sont indécomposables. Ils forment les constituants élémentaires des $p$-groupes abéliens : tout $p$-groupe abélien se décompose en un produit direct de $p$-sous-groupes cycliques.

**Théorème 17** *Un $p$-groupe cyclique est indécomposable.*

**Démonstration** Supposons au contraire que le groupe cyclique $G$, d'ordre $p^n$, se décompose en produit direct $G = G_1 \otimes G_2$ de 2 sous-groupes d'ordres respectifs $p^k$ et $p^{n-k}$ tels que $0 < k < n$. Sans restreindre la généralité, nous pouvons supposer que $k \geqslant n - k$. Soit $a \in G$ un générateur. On a $a = a_1 \cdot a_2$ avec $a_i \in G_i$ et par conséquent

$$a^{p^k} = a_1^{p^k} \cdot a_2^{p^k} = a_1^{p^k} \cdot (a_2^{p^{n-k}})^{p^{2k-n}} = e \cdot e^{p^{2k-n}} = e \cdot e = e,$$

et comme $p^k < p^n = |G|$, ceci est une contradiction. □

**Lemme 4** *Soit $G$ un $p$-groupe abélien et $a \in G$ tel que $\omega(a) = \operatorname{Exp} G$. Tout $q \in G/(a)$ possède un représentant $b \in G$ tel que $\omega(b) = \omega(q)$.*

**Démonstration** $G$ et $G/(a)$ étant des $p$-groupe on a $\omega(a) = \operatorname{Exp} G = p^N$ et $\omega(q) = p^r$ pour des entiers $N$ et $r$. On note également que

$$\omega(q) \leqslant \omega(b), \tag{2.16}$$

pour tout représentant $b$ de $q$. En effet $q^k = e_{G/(a)}$ si et seulement si $b^k \in (a)$ et donc

$$p^r\mathbb{Z} = \omega(q)\mathbb{Z} = \{k \in \mathbb{Z} \mid b^k \in (a)\} \supset \{k \in \mathbb{Z} \mid b^k = e\} = \omega(b)\mathbb{Z},$$

implique que $\omega(q)$ divise $\omega(b)$.

Soit $b_0 \in G$ un représentant de $q$ d'ordre $\omega(b_0) = p^n$. Le corollaire 3 et l'inégalité (2.16) impliquent $r \leqslant n \leqslant N$. Comme $b_0^{p^r} \in (a)$, il existe un entier $l$ tel que $b_0^{p^r} = a^l$. De plus

$$e = b_0^{p^n} = (b_0^{p^r})^{p^{n-r}} = a^{lp^{n-r}},$$

implique que $p^N$ divise $lp^{n-r}$. On peut donc écrire $l = jp^{N-n+r}$ avec un entier $j$ et obtenir ainsi $b_0^{p^r} = (a^{jp^{N-n}})^{p^r}$. En posant $b = b_0 a^{-jp^{N-n}}$ nous obtenons donc un représentant de $q$ tel que $b^{p^r} = e$ c'est-à-dire tel que $\omega(b)$ divise $p^r = \omega(q)$. L'inégalité (2.16) permet de conclure que $\omega(b) = \omega(q)$. □

**Théorème 18** *Tout $p$-groupe abélien $G$ est décomposable en produit direct de $p$-sous-groupes cycliques*

$$G = G_1 \otimes G_2 \otimes \cdots \otimes G_r.$$

**Démonstration** Par induction sur $|G|$. Si $|G| = p$, $G$ est lui-même cyclique. Supposons l'assertion vraie pour tous les $p$-groupes abéliens $G$ d'ordre $|G| < p^N$. Soit $G$ un $p$-groupe abélien d'ordre $p^N$. Si $\operatorname{Exp} G = p^N$, $G$ est cyclique d'après le corollaire 3 et il n'y a rien à démontrer. Supposons que $\operatorname{Exp} G = p^{n_1} < p^N$. D'après le lemme 3 il existe un élément $a_1 \in G$ d'ordre maximal, c'est-à-dire tel que $\omega(a_1) = \operatorname{Exp} G = p^{n_1} > 1$. Le $p$-sous-groupe cyclique $G_1 = (a_1)$ est donc un sous-groupe propre de $G$. On dénote par $\pi : G \to G/G_1$ la surjection canonique. Le quotient $Q = G/G_1$ est un $p$-groupe d'ordre strictement inférieur à $p^N$ puisque

$$|Q| = [G : G_1] = |G|/|G_1| = p^N/p^{n_1} < p^N.$$

L'hypothèse d'induction implique qu'il se décompose en produit direct de $p$-sous-groupes cycliques

$$Q = Q_2 \otimes Q_3 \otimes \cdots \otimes Q_r. \tag{2.17}$$

Pour $i = 2, \ldots, r$, soient $q_i \in Q_i$ un générateur de $Q_i$ et $a_i \in G$ un représentant de $q_i$ tel que $\omega(a_i) = \omega(q_i)$ (un tel représentant existe par le lemme 4). $G_i = (a_i)$ est un $p$-sous-groupe cyclique de $G$. Pour tout $a \in G$ on a

$$\pi(a) = q_2^{\mu_2} \cdot q_3^{\mu_3} \cdots q_r^{\mu_r} = \pi(a_2)^{\mu_2} \cdot \pi(a_3)^{\mu_3} \cdots \pi(a_r)^{\mu_r} = \pi(a_2^{\mu_2} \cdot a_3^{\mu_3} \cdots a_r^{\mu_r}),$$

c'est-à-dire $a \in (a_2^{\mu_2} \cdot a_3^{\mu_3} \cdots a_r^{\mu_r}) \cdot G_1$. Il existe donc $\mu_1$ tel que

$$a = a_1^{\mu_1} \cdot (a_2^{\mu_2} \cdot a_3^{\mu_3} \cdots a_r^{\mu_r}),$$

démontrant que $G = G_1 \cdot G_2 \cdots G_r$.

En invoquant le théorème 12 nous pouvons conclure que ce produit est direct si $a \in G_i \cap G_1 \cdots G_{i-1} \cdot G_{i+1} \cdots G_r$ implique $a = e$. On a

$$a = a_i^{\mu_i} = a_1^{\mu_1} \cdots a_{i-1}^{\mu_{i-1}} \cdot a_{i+1}^{\mu_{i+1}} \cdots a_r^{\mu_r}, \tag{2.18}$$

et donc

$$e = a_1^{\mu_1} \cdots a_{i-1}^{\mu_{i-1}} \cdot a_i^{-\mu_i} \cdot a_{i+1}^{\mu_{i+1}} \cdots a_r^{\mu_r}. \tag{2.19}$$

Il suit que

$$\pi(e) = \pi(a_1)^{\mu_1} \cdots \pi(a_{i-1})^{\mu_{i-1}} \cdot \pi(a_i)^{-\mu_i} \cdot \pi(a_{i+1})^{\mu_{i+1}} \cdots \pi(a_r)^{\mu_r},$$

ou encore

$$e_Q = q_2^{\mu_2} \cdots q_{i-1}^{\mu_{i-1}} \cdot q_i^{-\mu_i} \cdot q_{i+1}^{\mu_{i+1}} \cdots q_r^{\mu_r}.$$

Le produit (2.17) étant direct, on doit avoir $q_2^{\mu_2} = q_3^{\mu_3} = \cdots = q_r^{\mu_r} = e_Q$ c'est-à-dire que $\mu_k$ doit être un multiple de $\omega(q_k) = \omega(a_k)$ pour $k = 2, \ldots, r$. L'égalité (2.19) devient donc $e = a_1^{\mu_1}$, et (2.18) permet de conclure que $a = e$. □

Nous avons déjà remarqué, dans l'exemple 39, que la décomposition d'un groupe en produit direct de sous-groupe n'est pas unique. Supposons donc que le p-groupe abélien G du théorème précédent admette deux décompositions

$$G = G_1 \otimes \cdots \otimes G_r = H_1 \otimes \cdots \otimes H_s,$$

en produit direct de sous-groupes cycliques. Notons $p^{n_i}$ l'ordre de $G_i$ et $p^{m_i}$ celui de $H_i$. Le produit direct étant commutatif (*c.f.* remarque 3) nous pouvons supposer également, sans restreindre la généralité, que

$$n_1 \geqslant n_2 \geqslant \cdots \geqslant n_r \quad \text{et} \quad m_1 \geqslant m_2 \cdots \geqslant m_s.$$

**Lemme 5** *Dans ce cas on a* $r = s$ *et* $n_i = m_i$ *pour* $i = 1, \ldots, r$. *Le nombre* $r$ *de facteurs et la suite décroissante* $p^{n_1} \geqslant \ldots \geqslant p^{n_r}$ *de leurs ordres est donc uniquement déterminée par* G.

**Démonstration** Par induction sur $|G|$. On note que tout $a \in G$ s'écrivant de manière unique

$$a = a_1 \cdots a_r,$$

avec $a_i \in G_i$ on a $a^k = a_1^k \cdots a_r^k = e$ si et seulement si $a_i^k = e$ pour tous les $i$. On peut donc conclure que

$$\omega(a)\mathbb{Z} = \{k \in \mathbb{Z} \mid a^k = e\} = \bigcap_{i=1}^{r} \{k \in \mathbb{Z} \mid a_i^k = e\} = \bigcap_{i=1}^{r} \omega(a_i)\mathbb{Z},$$

c'est-à-dire que $\omega(a) = \text{PPCM}\{\omega(a_i) \mid i = 1, \ldots, r\}$. Il suit immédiatement du corollaire 3 que $\text{Exp}\, G = p^{n_1}$. Le même raisonnement appliqué à la décomposition

$$a = b_1 \cdots b_s,$$

avec $b_i \in H_i$ montre que $\text{Exp}\, G = p^{m_1}$. On peut donc conclure que $m_1 = n_1$. En particulier, si $|G| = p$, G est cyclique d'ordre p et on a $r = s = 1$ et $m_1 = n_1 = 1$.

Supposons l'assertion vraie pour tous les p-groupes G d'ordre $|G| < p^N$. Soit G un p-groupe d'ordre $p^N$. On a donc $N = n_1 + \cdots + n_r = m_1 + \cdots + m_s$ et on remarque que $G^p = \{a^p \mid a \in G\}$ est un groupe. De plus, tout élément de $G^p$ s'écrit de manière unique comme $a_1^p \cdots a_r^p = b_1^p \cdots b_s^p$. On a donc deux décompositions

$$G^p = G_1^p \otimes \cdots \otimes G_r^p = H_1^p \otimes \cdots \otimes H_s^p. \tag{2.20}$$

On vérifie aisément que $G_i^p$ est cyclique d'ordre $p^{n_i - 1}$. En effet, si a est un générateur de $G_i$, $a^p$ est un générateur de $G_i^p$. Comme $(a^p)^k = e$ si et seulement si pkest un multiple de $p^{n_i}$ on a bien $\omega(a^p) = p^{n_i - 1}$. De même, $H_i^p$ est cyclique d'ordre $p^{m_i - 1}$. Soient $r'$ et $s'$ les entiers déterminés par les conditions

$$n_1 \geqslant \ldots \geqslant n_{r'} > 1 = n_{r'+1} = \cdots = n_r,$$

et

$$m_1 \geqslant \ldots \geqslant m_{s'} > 1 = m_{s'+1} = \cdots = m_s.$$

On peut alors récrire la décomposition (2.20) en omettant les facteurs triviaux

$$G^p = G_1^p \otimes \cdots \otimes G_{r'}^p = H_1^p \otimes \cdots \otimes H_{s'}^p.$$

$G^p$ est donc un p-groupe d'ordre $p^M$ avec

$$M = \sum_{i=1}^{r'} (n_i - 1) = \sum_{i=1}^{s'} (m_i - 1) < N.$$

L'hypothèse d'induction implique que $r' = s'$ et $n_i - 1 = m_i - 1$ pour $i = 1, \ldots, r'$. Comme $|G| = p^N = p^{M+r} = p^{M+s}$, on en déduit immédiatement que $r = s$ et que $m_i = n_i$ pour $i = 1, \ldots, r$, achevant ainsi l'induction. □

On dit qu'un p-groupe abélien G est de *type* $(p^{n_1}, p^{n_2}, \ldots, p^{n_r})$ si c'est le produit direct de sous-groupes cycliques d'ordre $p^{n_1}, p^{n_2}, \ldots, p^{n_r}$ avec $n_1 \geqslant \cdots \geqslant n_r$.

### 2.5.5 Structure des groupes abéliens finis

Soit G un groupe abélien fini et $|G| = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$ la factorisation en facteurs premiers de l'ordre de G. Posons $\mathcal{P} = \{p_1, p_2, \ldots, p_l\}$ et pour $p \in \mathcal{P}$

$$G(p) = \{a \in G \mid \omega(a) = p^n \text{ pour un entier } n \geqslant 0\}. \tag{2.21}$$

$G(p)$ est un sous-groupe :

i. Soient $a, b \in G(p)$. Comme $\omega(a \cdot b)$ divise $\omega(a)\omega(b)$ (*c.f.* lemme 2), on a bien $a \cdot b \in G(p)$.

ii. $\omega(e) = 1 = p^0$.

iii. $(a^{-1}) = (a)$ implique $\omega(a^{-1}) = \omega(a)$.

$G(p)$ est un p-sous-groupe de Sylow de $G$ :

i. $\operatorname{Exp} G(p) = \operatorname{PPCM}\{\omega(a) \mid a \in G(p)\}$ est une puissance de $p$.

ii. $|G(p)|$ divise une puissance de $\operatorname{Exp} G(p)$ par le corollaire 4. $|G(p)|$ est donc une puissance de $p$ et par conséquent $G(p)$ est un p-sous-groupe.

iii. Soit $H$ est un p-sous-groupe de $G$ d'ordre $p^N$. Pour tout $a \in H$, $\omega(a)$ divise $|H|$ et donc $\omega(a) = p^n$ pour un entier $n$. On en conclut que $a \in G(p)$ et donc que $H \subset G(p)$.

En utilisant encore le lemme 2, on arrive aisément à la conclusion que si $a_i \in G(p_i)$, l'ordre du produit $a_1 \cdots a_{k-1} \cdot a_k \cdots a_l$ est un entier de la forme $p_1^{\nu_1} \cdots p_{k-1}^{\nu_{k-1}} \cdot p_{k+1}^{\nu_{k+1}} \cdots p_l^{\nu_l}$. Il suit que

$$G(p_k) \cap G(p_1) \cdots G(p_{k-1}) \cdot G(p_{k+1}) \cdots G(p_l) = \{e\}.$$

Soit $a \in G$, alors $\omega(a)$ divise $|G|$ et donc $\omega(a) = p_1^{m_1} \cdots p_l^{m_l}$. Pour $i = 1, \ldots l$, posons

$$k_i = \frac{\omega(a)}{p_i^{m_i}} = p_1^{m_1} \cdots p_{i-1}^{m_{i-1}} p_{i+1}^{m_{i+1}} \cdots p_l^{m_l},$$

et $a_i = a^{k_i}$. Alors

$$a_i^{p_i^{m_i}} = (a^{k_i})^{p_i^{m_i}} = a^{\omega(a)} = e,$$

implique que $\omega(a_i)$ divise $p_i^{m_i}$. On a donc $a_i \in G(p_i)$.

Les entiers $k_1, \ldots, k_l$ étant premiers entre eux, il existe des entiers $r_1, \ldots, r_l$ tels que $\sum_i r_i k_i = 1$ (Bezout). On a donc

$$a = a^{\sum_i r_i k_i} = \prod_i (a^{k_i})^{r_i} = \prod_i a_i^{r_i} \in G(p_1) \cdots G(p_l),$$

et nous pouvons conclure par le résultat suivant.

**Théorème 19** *Soient $G$ un groupe abélien fini, $\mathcal{P}$ l'ensemble des diviseurs premiers de $|G|$ et, pour $p \in \mathcal{P}$, $G(p)$ le sous-groupe défini par (2.21). Alors $G$ se décompose canoniquement selon*

$$G = \bigotimes_{p \in \mathcal{P}} G(p). \tag{2.22}$$

En appliquant le théorème 18 à chaque facteur $G(p)$ de cette décomposition, nous obtenons le théorème suivant qui détermine la structure de tout groupe abélien fini.

**Théorème 20** *Tout groupe abélien fini* $G$ *est un produit direct de sous-groupes cycliques dont les ordres sont des puissances des diviseurs premiers de* $|G|$.

On remarquera que si la décomposition en produit direct de sous-groupes de Sylow (2.22) est unique, la décomposition de chaque facteur $G(p)$ en produit de sous-groupes cyclique ne l'est pas. Le lemme 5 assure cependant l'unicité des ordres des facteurs de cette décomposition. Deux groupes abéliens finis sont donc isomorphes si et seulement si les même ordres apparaissent dans cette décomposition.

**Exemple 56** Déterminons, à l'isomorphisme près, tous les groupes abéliens d'ordre 140400. La décomposition en facteurs premiers de ce nombre est

$$140400 = 2^4 3^3 5^2 13^1.$$

Les puissances apparaissant dans cette décomposition peuvent être partitionnées de la manière suivante

$$\begin{aligned}
4 &= 1+1+1+1,\\
&= 1+1+2,\\
&= 2+2,\\
&= 1+3,\\
&= 4.\\
3 &= 1+1+1,\\
&= 2+1,\\
&= 3.\\
2 &= 1+1,\\
&= 2.\\
1 &= 1.
\end{aligned}$$

Il y a donc, à l'isomorphisme près, $5 \times 3 \times 2 \times 1 = 30$ groupes abéliens d'ordre 140400. Ils sont de la forme $G(2) \times G(3) \times G(5) \times G(13)$.

$G(2)$ peut prendre 5 formes différentes

$$\begin{aligned}
&C_2 \times C_2 \times C_2 \times C_2,\\
&C_2 \times C_2 \times C_4,\\
&C_4 \times C_4,\\
&C_2 \times C_8,\\
&C_{16}.
\end{aligned}$$

$G(3)$ peut prendre 3 formes distinctes

$$\begin{aligned}
&C_3 \times C_3 \times C_3,\\
&C_3 \times C_9,\\
&C_{27}.
\end{aligned}$$

$G(5)$ peut prendre les 2 formes

$$C_5 \times C_5,$$
$$C_{25}.$$

Finalement $G(13)$ est donné par

$$C_{13}.$$

**Exemple 57** Soit $G$ un groupe cyclique d'ordre $m = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$ et

$$G = G(p_1) \otimes \cdots \otimes G(p_l),$$

sa décomposition canonique. $G(p_i)$ est un $p_i$-sous-groupe de $G$, c'est donc un groupe cyclique d'ordre $p_i^{k_i}$. On obtient

$$|G| = m = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l} = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l},$$

et l'unicité de la décomposition en facteurs premiers permet de conclure $k_i = n_i$. On a donc

$$G \simeq C_{p_1^{n_1}} \times \cdots \times C_{p_l^{n_l}},$$

où, d'après le théorème 17, chaque facteur est indécomposable.

## 2.6 Groupes symétriques

Si $X$ est un ensemble fini et $N = |X|$, le groupe de permutation $\mathfrak{S}_X$ est isomorphe au groupe $S_N$ des permutations de l'ensemble $\{1, 2, \ldots, N\}$. On appelle $S_N$ *groupe symétrique de degré* $N$. $S_N$ est d'ordre $N!$.

Une permutation $\sigma \in S_N$ telle que $\sigma : i \mapsto \sigma(i)$ est notée

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

L'ordre des colonnes n'est pas important. On peut écrire la même permutation sous la forme

$$\sigma = \begin{pmatrix} 4 & N & \cdots & 2 \\ \sigma(4) & \sigma(N) & \cdots & \sigma(2) \end{pmatrix}.$$

Ainsi, l'inverse de $\sigma$ peut s'écrire

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(N) \\ 1 & 2 & \cdots & N \end{pmatrix}.$$

**Exemple 58** La permutation

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

s'écrit également

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

Son inverse est

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

### 2.6.1 Cycles

La permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} \in S_5,$$

représentée graphiquement sur la figure 2.4 est un exemple de *cycle*. On peut la décrire de manière plus concise par la notation

$$\sigma = (13254) = (32541) = (25413) = (54132) = (41325).$$

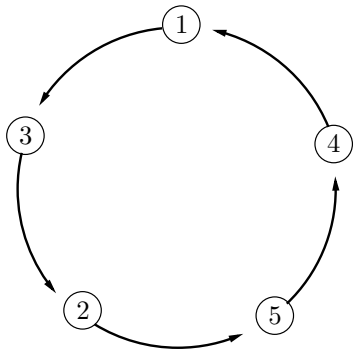


Fig. 2.4 – Le cycle $(13254)$.

De même la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \in S_5,$$

qui laisse les éléments 2 et 4 invariant peut s'écrire plus simplement

$$\sigma = (135) = (351) = (513).$$

On dit que c'est un *cycle de longueur* 3 ou un 3-*cycle*. Un $l$-*cycle* de $S_N$ s'écrit $\sigma = (i_1 i_2 \cdots i_l)$ où $i_1, i_2, \ldots i_l$ sont $l$ éléments distincts de $\{1, 2, \ldots, N\}$. Il représente la permutation

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_l & i_{l+1} & \cdots & i_N \\ i_2 & i_3 & \cdots & i_1 & i_{l+1} & \cdots & i_N \end{pmatrix} \in S_N.$$

qui laisse fixés les éléments de $\{i_{l+1}, \ldots, i_N\} = \{1, 2, \ldots, N\} \setminus \{i_1, i_2, \ldots, i_l\}$. On a alors

$$\begin{aligned}
\sigma^2 &= \begin{pmatrix} i_1 & i_2 & \cdots & i_l & i_{l+1} & \cdots & i_N \\ i_3 & i_4 & \cdots & i_2 & i_{l+1} & \cdots & i_N \end{pmatrix}, \\
\sigma^3 &= \begin{pmatrix} i_1 & i_2 & \cdots & i_l & i_{l+1} & \cdots & i_N \\ i_4 & i_5 & \cdots & i_3 & i_{l+1} & \cdots & i_N \end{pmatrix}, \\
&\vdots \\
\sigma^k &= \begin{pmatrix} i_1 & i_2 & \cdots & i_l & i_{l+1} & \cdots & i_N \\ i_{k+1} & i_{k+2} & \cdots & i_k & i_{l+1} & \cdots & i_N \end{pmatrix}, \\
&\vdots \\
\sigma^l &= \begin{pmatrix} i_1 & i_2 & \cdots & i_l & i_{l+1} & \cdots & i_N \\ i_1 & i_2 & \cdots & i_l & i_{l+1} & \cdots & i_N \end{pmatrix} = \mathrm{Id}.
\end{aligned}$$

Un $l$-cycle est un élément d'ordre $l$ de $S_N$. En effet, on a $\sigma^k(i_1) = i_{k+1} \neq i_1$ et donc $\sigma^k \neq \mathrm{Id}$ pour $k = 1, \ldots, l-1$ alors que $\sigma^l = \mathrm{Id}$. L'inverse de $\sigma$ est

$$\sigma^{-1} = \begin{pmatrix} i_2 & i_3 & \cdots & i_1 & i_{l+1} & \cdots & i_N \\ i_1 & i_2 & \cdots & i_l & i_{l+1} & \cdots & i_N \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \cdots & i_l & i_{l+1} & \cdots & i_N \\ i_l & i_1 & \cdots & i_{l-1} & i_{l+1} & \cdots & i_N \end{pmatrix},$$

c'est-à-dire $\sigma^{-1} = (i_1 i_l i_{l-1} \cdots i_2) = (i_l i_{l-1} \cdots l_2 l_1)$. L'inverse d'un $l$-cycle est donc le $l$-cycle obtenu en inversant l'ordre des éléments $i_k$ le constituant.

Deux cycles

$$\sigma = (i_1 i_2 \cdots i_l) = \begin{pmatrix} i_1 & i_2 & \cdots & i_l & i_{l+1} & i_{l+2} & \cdots & i_{l+r} & i_{l+r+1} & \cdots & i_N \\ i_2 & i_3 & \cdots & i_1 & i_{l+1} & i_{l+2} & \cdots & i_{l+r} & i_{l+r+1} & \cdots & i_N \end{pmatrix},$$

et

$$\tau = (i_{l+1} i_{l+2} \cdots i_{l+r}) = \begin{pmatrix} i_1 & i_2 & \cdots & i_l & i_{l+1} & i_{l+2} & \cdots & i_{l+r} & i_{l+r+1} & \cdots & i_N \\ i_1 & i_2 & \cdots & i_l & i_{l+2} & i_{l+3} & \cdots & i_{l+1} & i_{l+r+1} & \cdots & i_N \end{pmatrix},$$

sont disjoints si $\{i_1, \ldots, i_l\} \cap \{i_{l+1}, \ldots, i_{l+r}\} = \varnothing$. Dans ce cas ils commutent

$$\begin{aligned}
\sigma\tau &= (i_1 i_2 \cdots i_l)(i_{l+1} i_{l+2} \cdots i_{l+r}) \\
&= \begin{pmatrix} i_1 & i_2 & \cdots & i_l & i_{l+1} & i_{l+2} & \cdots & i_{l+r} & i_{l+r+1} & \cdots & i_N \\ i_2 & i_3 & \cdots & i_1 & i_{l+2} & i_{l+3} & \cdots & i_{l+1} & i_{l+r+1} & \cdots & i_N \end{pmatrix} \\
&= (i_{l+1} i_{l+2} \cdots i_{l+r})(i_1 i_2 \cdots i_l) \\
&= \tau\sigma.
\end{aligned}$$

Toute permutation $\sigma$ se décompose en un produit de cycles disjoints. Cette décomposition est unique à l'ordre des facteurs près.

**Exemple 59** Pour obtenir la décomposition de la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 1 & 3 & 2 & 8 & 7 & 6 \end{pmatrix}, \tag{2.23}$$

en produit de cycles disjoint on commence par suivre l'image de 1 par application répétée de $\sigma$

$$1 \to 4 \to 3 \to 1,$$

nous identifions ainsi le cycle $(143)$. Le premier élément de la première ligne de (2.23) qui n'apparaît pas dans ce cycle est 2. En suivant son image on obtient

$$2 \to 5 \to 2,$$

et donc le cycle $(25)$. Le premier élément de la première ligne de (2.23) qui n'apparaît pas dans un des deux cycles déjà identifiés est 6. On obtient cette fois

$$6 \to 8 \to 6,$$

et donc le cycle $(68)$. Finalement il ne reste sur la première ligne de (2.23) que l'élément 7 qui est fixé par $\sigma$ et qui donne le cycle $(7)$. Nous avons obtenu la décomposition

$$\sigma = (143)(25)(68)(7). \tag{2.24}$$

On remarque que les cycles de longueur 1 n'apportent aucune information dans la décomposition d'une permutation. On peut donc les omettre et écrire plus simplement

$$\sigma = (143)(25)(68).$$

Comme ces cycles sont disjoints par construction, ils commutent et l'ordre des facteurs dans (2.24) est arbitraire. Par contre les facteurs apparaissant dans cette décomposition sont clairement déterminés de manière unique par $\sigma$.

**Définition 11** *Une permutation $\sigma \in S_N$ dont la décomposition en cycles disjoints comporte $n_1$ 1-cycles, $n_2$ 2-cycles, $\ldots$, $n_N$ N-cycles est dite de type*

$$(n_1, n_2, \ldots, n_N).$$

*On a donc toujours $\sum_{l=1}^{N} l n_l = N$.*

**Exemple 60** Déterminons la représentation en produit de cycles disjoints de tous les éléments du groupe $S_3$. On a

$$S_3 = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\},$$

et donc

$$S_3 = \{(1)(2)(3), (1)(23), (12)(3), (13)(2), (123), (132)\}.$$

$S_3$ contient donc une permutation de type $(3,0,0)$, trois de type $(1,1,0)$ et deux de type $(0,0,1)$.

Après élimination des 1-cycles on obtient

$$S_3 = \{\mathrm{Id}, (23), (12), (123), (132), (13)\}. \tag{2.25}$$

### 2.6.2 Transpositions, signature

Un 2-cycle $(ij)$ est appelé transposition. Une transposition $(ij)$ est un élément d'ordre 2 dont l'action se réduit à l'échange de $i$ et $j$, laissant tous les autres éléments fixés

$$(14) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}.$$

Un calcul simple montre que

$$(i_1 i_2 \cdots i_l)(i_l i_{l+1}) = (i_1 i_2 \cdots i_l i_{l+1}),$$

d'où on déduit

$$(i_1 i_2 \cdots i_l) = (i_1 i_2)(i_2 i_3) \cdots (i_{l-1} i_l). \tag{2.26}$$

Un cycle peut donc se décomposer en produit de transpositions. Comme nous avons montré qu'une permutation quelconque se décompose en produit de cycles, en en conclut qu'elle se décompose également en produit de transpositions. On remarquera cependant que les transpositions apparaissant dans la formule (2.26) ne sont pas disjointes. Elles ne commutent donc pas en général, par exemple

$$(123) = (12)(23) \neq (23)(12) = (132),$$

ce qui implique que $S_N$ n'est pas abélien pour $N \geqslant 3$. De plus, contrairement à la décomposition en cycles disjoints, la décompositions en transpositions n'est pas unique. On vérifie par exemple

$$(123) = (12)(23) = (23)(12)(32)(21).$$

Soit $P = \{\{i,j\} \,|\, i,j \in \{1,\ldots,N\}, i \neq j\}$ l'ensemble des sous-ensembles à deux éléments de $\{1,\ldots,N\}$. Pour $\sigma \in S_N$ et $p = \{i,j\} \in P$ on pose

$$\varepsilon_p(\sigma) = \frac{\sigma(i) - \sigma(j)}{i - j}.$$

La signature de $\sigma \in S_N$ est définie par

$$\varepsilon(\sigma) = \prod_{p \in P} \varepsilon_p(\sigma).$$

$S_N$ opère sur $P$ par l'action

$$\begin{array}{rcl} S_N \times P & \to & P \\ (\sigma, \{i,j\}) & \mapsto & \{\sigma(i), \sigma(j)\}, \end{array}$$

et en particulier $\tau P = \{\tau p \mid p \in P\} = P$. Si $\sigma, \tau \in S_N$ et $p = \{i,j\} \in P$ on a

$$\varepsilon_p(\sigma\tau) = \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau(j)}{i - j} = \varepsilon_{\tau p}(\sigma) \cdot \varepsilon_p(\tau),$$

et donc

$$\begin{aligned} \varepsilon(\sigma\tau) &= \prod_{p \in P} \varepsilon_p(\sigma\tau) = \prod_{p \in P} (\varepsilon_{\tau p}(\sigma) \cdot \varepsilon_p(\tau)) = \prod_{p \in P} \varepsilon_{\tau p}(\sigma) \cdot \prod_{p \in P} \varepsilon_p(\tau) \\ &= \prod_{q \in \tau P} \varepsilon_q(\sigma) \cdot \prod_{p \in P} \varepsilon_p(\tau) = \prod_{q \in P} \varepsilon_q(\sigma) \cdot \prod_{p \in P} \varepsilon_p(\tau) \\ &= \varepsilon(\sigma)\varepsilon(\tau). \end{aligned} \tag{2.27}$$

Il est aisé de calculer la signature d'une transposition $\sigma = (kl)$. On considère la partition de $P$ en trois sous-ensembles $P_r = \{p \in P \mid |p \cap \{k,l\}| = r\}$, $r = 0, 1, 2$.

i. Pour $p = \{i,j\} \in P_0$ on a $\sigma(i) = i$ et $\sigma(j) = j$. On en conclut $\varepsilon_p(\sigma) = 1$ et donc

$$\prod_{p \in P_0} \varepsilon_p(\sigma) = 1.$$

ii. On remarque que

$$P_1 = \bigcup_{i \in \{1,2,\ldots,N\} \setminus \{k,l\}} \{\{i,k\}, \{i,l\}\}.$$

Si $p = \{i,k\}$ et $p' = \{i,l\}$ on a $\varepsilon_p(\sigma)\varepsilon_{p'}(\sigma) = \frac{i-l}{i-k}\frac{i-k}{i-l} = 1$ et donc

$$\prod_{p \in P_1} \varepsilon_p(\sigma) = 1.$$

iii. On a $\sigma(k) = l$ et $\sigma(l) = k$ et donc $\varepsilon_p(\sigma) = -1$ pour $p \in P_2 = \{\{k,l\}\}$, c'est-à-dire

$$\prod_{p \in P_2} \varepsilon_p(\sigma) = -1.$$

On peut donc conclure que $\varepsilon(\sigma) = -1$ pour toute transposition $\sigma$. Si $\sigma \in S_N$ est le produit de $t$ transpositions on a par conséquent $\varepsilon(\sigma) = (-1)^t$. On en déduit d'une part que $\varepsilon(\sigma) \in \{-1, +1\}$ pour toute permutation $\sigma \in S_N$ et d'autre part que la parité du nombre de facteurs présents dans toutes les représentations de $\sigma$ comme produit de transpositions est la même.

La formule (2.26) montre que la signature d'un $l$-cycle est $(-1)^{l-1}$. Si $\sigma \in S_N$ est de type $(n_1, \ldots, n_N)$ on a donc

$$\varepsilon(\sigma) = (-1)^{\sum_{l=1}^{N}(l-1)n_l} = (-1)^{N + \sum_{l=1}^{N} n_l}.$$

### 2.6.3 Conjugaison dans les groupes symétriques

Considérons la conjugaison par $\sigma \in S_N$ d'une permutation $\tau \in S_N$. On a

$$\sigma(i) \overset{\sigma^{-1}}{\mapsto} i \overset{\tau}{\mapsto} \tau(i) \overset{\sigma}{\mapsto} \sigma(\tau(i)),$$

pour $i = 1, 2, \ldots, N$ et donc

$$j_\sigma(\tau) = \sigma\tau\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(N) \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(N)) \end{pmatrix}.$$

En particulier, si $\tau$ est un $l$-cycle $(i_1 i_2 \cdots i_l)$,

$$j_\sigma(\tau) = \begin{pmatrix} \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_l) & \sigma(i_{l+1}) & \cdots & \sigma(i_N) \\ \sigma(i_2) & \sigma(i_3) & \cdots & \sigma(i_1) & \sigma(i_{l+1}) & \cdots & \sigma(i_N) \end{pmatrix},$$

et donc

$$j_\sigma((i_1 i_2 \cdots i_l)) = (\sigma(i_1)\sigma(i_2)\cdots\sigma(i_l)),$$

est toujours un $l$-cycle. Plus généralement, il est clair que le conjugué d'un produit de cycle disjoints de type $(n_1, \ldots, n_N)$ est un produit de cycles du même type. Montrons la réciproque : si $\tau$ et $\tau'$ sont des éléments de même type de $S_N$, ils sont conjugués. Soient

$$\tau = (i_1 \cdots i_{l_1})(j_1 \cdots j_{l_2}) \cdots (k_1 \cdots k_{l_r}), \quad \tau' = (i'_1 \cdots i'_{l_1})(j'_1 \cdots j'_{l_2}) \cdots (k'_1 \cdots k'_{l_r}),$$

deux éléments de même type et

$$\sigma = \begin{pmatrix} i_1 & \cdots & i_{l_1} & j_1 & \cdots & j_{l_2} & \cdots & k_1 & \cdots & k_{l_r} \\ i'_1 & \cdots & i'_{l_1} & j'_1 & \cdots & j'_{l_2} & \cdots & k'_1 & \cdots & k'_{l_r} \end{pmatrix}.$$

On a alors

$$\begin{aligned} j_\sigma(\tau) &= j_\sigma((i_1 \cdots i_{l_1})(j_1 \cdots j_{l_2}) \cdots (k_1 \cdots k_{l_r})) \\ &= j_\sigma((i_1 \cdots i_{l_1}))j_\sigma((j_1 \cdots j_{l_2})) \cdots j_\sigma((k_1 \cdots k_{l_r})) \\ &= (\sigma(i_1) \cdots \sigma(i_{l_1}))(\sigma(j_1) \cdots \sigma(j_{l_2})) \cdots (\sigma(k_1) \cdots \sigma(k_{l_r})) \\ &= (i'_1 \cdots i'_{l_1})(j'_1 \cdots j'_{l_2}) \cdots (k'_1 \cdots k'_{l_r}) \\ &= \tau'. \end{aligned}$$

**Théorème 21** *Deux permutations sont conjuguées si et seulement si elles sont de même type. En particulier, le nombre de classes de conjugaison de* $S_N$ *est égal au nombre de types d'éléments de* $S_N$.

On parlera donc naturellement de la classe $(n_1, \ldots, n_N)$ pour désigner la classe de conjugaison formée de tous les éléments de type $(n_1, \ldots, n_N)$.

**Exemple 61** Il y a trois type de permutations dans $S_3$ (exemple 60) et donc trois classes de conjugaison. Plus précisément, il y a une permutation de type (3,0,0), trois de type $(1,1,0)$ et deux de type $(0,0,1)$. Il n'existe qu'une seule classe ne comportant qu'un seul élément, il s'agit bien entendu de la classe de Id. On peut en conclure que $Z(S_3) = \{e\}$. L'équation des classes de $S_3$ est donc

$$6 = 1 + 3 + 2.$$

**Exemple 62** Il y a cinq type de permutations dans $S_4$ (exemple 65) et donc cinq classes de conjugaison. Le nombre d'élément de chaque classe est donné par le tableau suivant.

| $n_1$ | $n_2$ | $n_3$ | $n_4$ | |
|---|---|---|---|---|
| 4 | 0 | 0 | 0 | 1 |
| 2 | 1 | 0 | 0 | 6 |
| 1 | 0 | 1 | 0 | 8 |
| 0 | 2 | 0 | 0 | 3 |
| 0 | 0 | 0 | 1 | 6 |

Dans ce cas encore, la seule classe ne contenant qu'une permutation est celle de Id, on a donc $Z(S_4) = \{e\}$ et l'équation des classes

$$24 = 1 + 6 + 8 + 3 + 6.$$

**Théorème 22** *Pour tout* $N > 2$ *on a* $Z(S_N) = \{\mathrm{Id}\}$.

**Démonstration** Nous savons que $\sigma \in Z(S_N)$ si et seulement si sa classe de conjugaison se réduit à $\{\sigma\}$ et que la classe de Id est $(N, 0, \ldots, 0)$. Il suffit donc de montrer que toute classe $(n_1, \ldots, n_N)$ distincte de la classe $(N, 0, \ldots, 0)$ contient plus d'un élément. Les conclusions des deux exemples précédents nous permettent en outre de nous restreindre à $N \geqslant 5$. Nous considérons trois cas :

i. La classe $(N-2, 1, 0, \ldots, 0)$ contient $(12)$ et $(13)$.

ii. La classe $(N-2s, s, 0, \ldots, 0)$ avec $s > 1$ contient $(12)(34)\cdots$ et $(13)(24)\cdots$.

iii. La classe $(r, s, \ldots, t, \ldots)$ avec $t > 0$ contient $\cdots(123\cdots)\cdots$ et $\cdots(132\cdots)\cdots$.

□

### 2.6.4 Groupes alternés

La relation (2.27) montre que $\varepsilon : S_N \to \{-1, +1\}$ est un morphisme.

**Définition 12** *Une permutation* $\sigma \in S_N$ *est dite paire si* $\varepsilon(\sigma) = 1$ *et impaire si* $\varepsilon(\sigma) = -1$. *L'ensemble* $A_N \subset S_N$ *des permutations paires est le noyau du morphisme* $\varepsilon : S_N \to \{-1, +1\}$. $A_N$ *est donc un sous-groupe distingué de* $S_N$, *on l'appelle groupe alterné de degré* N.

Le théorème d'isomorphisme montre que $S_N/A_N \simeq \{-1,+1\} \simeq C_2$. On a donc

$$[S_N : A_N] = 2,$$

et par conséquent

$$|A_N| = \frac{N!}{2}.$$

**Exemple 63** $A_2 = \{\mathrm{Id}\}$.

**Exemple 64** De (2.25) on obtient immédiatement

$$A_3 = \{\mathrm{Id}, (12), (23), (13)\}.$$

Les seuls groupes d'ordre 4 sont le groupe cyclique $C_4$ et le groupe des 4 de Klein $C_2 \times C_2$. Comme les transpositions sont d'ordre 2, on conclut que $A_3 \simeq C_2 \times C_2$. En particulier, $A_3$ n'est pas simple. Il est abélien et admet trois sous-groupes cycliques d'ordre 2 $\{\mathrm{Id}, (12)\}, \{\mathrm{Id}, (13)\}$ et $\{\mathrm{Id}, (23)\}$. $S_3$ admet donc une suite décroissante

$$S_3 \rhd A_3 \rhd \{\mathrm{Id}, (12)\} \rhd \{e\},$$

dont les facteurs

$$S_3/A_3 \simeq C_2, \quad A_3/\{\mathrm{Id}, (13)\} \simeq C_2, \quad \{\mathrm{Id}, (13)\}/\{e\} \simeq C_2,$$

sont abéliens. $S_3$ et $A_3$ sont donc résolubles.

**Exemple 65** Il y a 5 types d'éléments de $S_4$

$$(4,0,0,0), \quad (2,1,0,0), \quad (1,0,1,0), \quad (0,2,0,0), \quad (0,0,0,1).$$

Les éléments de $A_4$ sont de type $(4,0,0,0)$, $(1,0,1,0)$ et $(0,2,0,0)$. On obtient facilement la liste de ces éléments

$$\mathrm{Id}, (123), (124), (132), (134), (142), (143), (234), (243), (12)(34), (13)(24), (14)(23).$$

Les éléments de type $(0,2,0,0)$ forment un sous-groupe distingué abélien (vérifiez le !)

$$H = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2.$$

Comme $[A_4 : H] = |A_4|/|H| = 12/4 = 3$, le quotient $A_4/H$ est cyclique. $S_4$ et $A_4$ sont résolubles, les facteur de la suite

$$S_4 \rhd A_4 \rhd H \rhd \{\mathrm{Id}, (12)(34)\} \rhd \{e\},$$

étant tous abéliens

$$S_4/A_4 \simeq C_2, \quad A_4/H \simeq C_3, \quad H/\{\mathrm{Id}, (12)(34)\} \simeq C_2, \quad \{\mathrm{Id}, (12)(34)\}/\{e\} \simeq C_2.$$

**Lemme 6** *Pour* $N \geqslant 3$, *le groupe alterné* $A_N$ *est engendré par les* 3*-cycles de* $S_N$.

**Démonstration** Un trois cycle est pair, en effet $(123) = (12)(23)$. Nous devons montrer que toute permutation paire $\sigma$ est un produit de 3-cycle. $\sigma$ étant un produit d'un nombre pair de transpositions, il suffit de montrer que tout produit de 2 transpositions distinctes est un produit de 3-cycles. Deux cas se présentent :

i. Les deux transpositions sont disjointes. Dans ce cas

$$(12)(34) = (123)(234).$$

ii. Les deux transpositions ont un élément commun. Alors

$$(12)(23) = (123).$$

□

Le théorème suivant est d'une importance fondamentale pour la théorie des équations algébriques. Il implique, que $S_N$ n'est pas résoluble pour $N \geqslant 5$ et la théorie de Galois permet d'en conclure qu'il n'existe pas de formule générale permettant d'exprimer les zéros d'un polynôme de degré supérieur ou égal à 5 par des radicaux.

**Théorème 23** *Le groupe alterné* $A_N$ *est simple pour tout* $N \geqslant 5$.

**Démonstration** Soit $H \lhd A_N$. Nous montrons tout d'abord que $H$ contient un 3-cycle. A cet effet, soit $\sigma \in H \setminus \{\mathrm{Id}\}$ et $\sigma = \alpha\beta\gamma\cdots$ sa décomposition en cycles disjoints qu'on suppose rangés en ordre de longueur décroissante. Si $\sigma$ n'est pas un 3-cycle, plusieurs cas sont possible :

1. $\alpha = (i_1 i_2 \cdots i_l)$ avec $l \geqslant 4$. Posons alors $\tau = (i_1 i_2 i_3)$. Ce 3-cycle étant disjoint de $\beta, \gamma, \ldots$ il commute avec eux et on a $j_\tau(\sigma) = j_\tau(\alpha)\beta\gamma\cdots$ et donc aussi

$$\begin{aligned}\sigma j_\tau(\sigma)^{-1} = \alpha j_\tau(\alpha)^{-1} &= (i_1 i_2 \cdots i_l)(i_l \cdots \tau(i_3)\tau(i_2)\tau(i_1)) \\ &= (i_1 i_2 \cdots i_l)(i_l \cdots i_1 i_3 i_2) \\ &= (i_1 i_4 i_2) \in H.\end{aligned}$$

2. $\alpha = (i_1 i_2 i_3)$. Dans ce cas on peut également supposer que $\beta, \gamma, \ldots$ sont des 3-cycles (en passant éventuellement de $\sigma$ à $\sigma^2$ pour éliminer les 2-cycles). Soit donc $\beta = (i_4 i_5 i_6)$ et $\tau = (i_1 i_4 i_5)$. Comme $\tau$ est disjoint de $\gamma, \ldots$ il commute avec eux et $\sigma j_\tau(\sigma)^{-1} = \alpha\beta j_\sigma(\alpha\beta)^{-1} = (i_1 i_5 i_2 i_4 i_3) \in H$ ce qui nous ramène au cas précédent.
3. $\sigma = (i_1 i_2)(i_3 i_4)$. Comme $N \geqslant 5$, il existe $i_5 \in \{1, \ldots, N\} \setminus \{i_1, i_2, i_3, i_4\}$. Soit $\tau = (i_5 i_4 i_3)$, alors $\tau = \sigma j_\tau(\sigma)^{-1} \in H$.
4. $\sigma = (i_1 i_2)(i_3 i_4)\gamma\cdots$. Posons dans ce cas $\tau = (i_3 i_2 i_1)$, alors

$$\sigma j_\tau(\sigma)^{-1} = (i_1 i_4)(i_2 i_3) \in H,$$

nous ramène au cas précédent.

Sans restreindre la généralité, nous pouvons donc supposer que $(123) \in H$. Montrons que $H$ contient tous les 3-cycles. Soit en effet $\sigma = (i_1 i_2 i_3)$ un 3-cycle quelconque. Comme $N \geqslant 5$ il est possible de trouver une permutation

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots \\ i_1 & i_2 & i_3 & \cdots \end{pmatrix} \in A_N,$$

et on en conclut que $\sigma = j_\tau((123)) \in H$.

Finalement, $H$ contenant tous les 3-cycles, il contient aussi $A_N$ par le lemme 6, et on conclut que $H = A_N$. □

Nous ne démontrerons pas le théorème suivant qui est une conséquence du théorème 23.

**Théorème 24** *$S_N$ et $A_N$ ne sont pas résolubles si $N \geqslant 5$.*