UNIVERSITE DE TUNIS
INSTITUT SUPERIEUR DE L'EDUCATION ET DE LA FORMATION CONTINUE

# COURS D'ALGEBRE
# M118

## GROUPES MONOGENES, GROUPES SYMETRIQUES, OPERATION D'UN GROUPE SUR UN ENSEMBLE

KARIM BOULABIAR

# PREFACE

La notion de groupe a été introduite pour la première fois au début du dix-neuvième siècle. A cette époque, elle intervient dans les travaux d'Evariste Galois sur les équations algébriques, sous forme de groupes de permutations des racines de ces équations. Presque au même moment, les groupes commencent à jouer un rôle en géométrie, notamment, des groupes symétriques de polygone et de polyèdres réguliers. C'est à partir de cette double origine, algébrique et géométrique, qu'a été conçue, vers la fin du dix- neuvième siècle, la notion abstraite de groupe et que, petit à petit, a été construite la théorie de groupes.

Dans la théorie de groupe, une place importante a été accordée à l'étude de la structure des groupes finis, compte tenu des nombreuses interprétations concrètes qui peuvent en être données. C'est précisément dans ce carde que se place ce cours d'algèbre, dans lequel ont été traités les groupes monogènes, les groupes symétriques et la notion d'un groupe opérant sur un ensemble.

# Table des matières

# Chapitre 1

# Groupes monogènes

L'ensemble des entiers relatifs, que nous notons $\mathbb{Z}$, est un groupe pour l'addition. En outre, pour un entier non nul $n$, l'ensemble des racines $n^{éme}$ de l'unité, que nous désignons par $\mu_n$, est un groupe pour la multiplication. Ces deux groupes sont abéliens. Une autre propriété commune à ces deux groupes peut-être dégagée. Il s'agit du fait que chacun d'eux est engendré par un seul élément (1 pour $\mathbb{Z}$ et $\exp(2\pi i/n)$ pour $\mu_n$). Nous étudions dans ce chapitre les groupes possèdant cette propriété. A cet égard, nous adoptons la notation multiplicative pour énoncer et démontrer le propriétés générales des groupes. L'ensemble des entiers naturels est noté $\mathbb{N}$ et celui des entiers naturels non nuls est noté $\mathbb{N}^*$. En outre, le cardinal d'un ensemble fini $X$ est noté $\text{card}(X)$.

## 1.1 Classification des groupes monogènes

Le sous-groupe d'un groupe $G$ engendré par un élément $g$ de $G$ est noté $\langle g\rangle$. Il vient rapidement que

$$\langle g\rangle = \{g^m : m \in \mathbb{Z}\} = \left\{..., g^{-2}, g^{-1}, e, g, g^2, ...\right\},$$

où $e$ désigne l'élément neutre de $G$. Le groupe $G$ est dit **monogène** s'il existe $g$ dans $G$ tel que $G = \langle g\rangle$. S'il en est ainsi, $g$ est appelé **générateur** de $G$. Nous disons aussi que $G$ est **engendré** par $g$. Un groupe monogène fini est dit **cyclique**. Un groupe monogène est visiblement abélien. Un élément $g$ d'un groupe $G$ est dit de **torsion** s'il est d'ordre fini. L'ordre d'un élément de torsion $g$ est noté $\text{o}(g)$ et l'ordre d'un groupe fini $G$ est noté $\text{o}(G)$. Un groupe $G$ est cyclique si, et seulement si, il existe un élément de torsion $g$ tel que $G = \langle g\rangle$. Dans ce cas, nous montrons aisément que

$$G = \left\{e, g, g^2, ..., g^{\text{o}(g)-1}\right\} \quad \text{et} \quad \text{o}(G) = \text{o}(g).$$

Notons que nous pouvons remplaçer dans les deux égalités ci-dessus $g$ par n'importe quel générateur du groupe cyclique $G$ autre que $g$.

L'imge d'un groupe monogène par un morphisme de groupes est également monogène. Nous pouvons énoncer ce résultat autrement comme suit.

**Proposition 1.1.1** *Soient $G$ un groupe monogène et $H$ un groupe. S'il existe un morphisme de groupes surjectif de $G$ sur $H$ alors $H$ est monogène.*

**Démonstration.** Soient $g$ un générateur de $G$ et $\varphi$ un morphisme de groupes surjectif de $G$ sur $H$. Pour tout $h \in H$, il existe $m \in \mathbb{Z}$ tel que $h = \varphi(g^m)$. Mais comme $\varphi$ est un morphisme de groupes, nous obtenons $h = (\varphi(g))^m$. Il vient que

$$H = \{(\varphi(g))^m : m \in \mathbb{Z}\}.$$

En d'autres termes, $H$ est monogène et $\varphi(g)$ en est un générateur. ■

Rappelons que si $n \in \mathbb{N}^*$ alors l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo $n$ dans $\mathbb{Z}$ est un groupe pour l'addition définie par

$$\overline{\ell} + \overline{m} = \overline{\ell + m} \qquad \text{pour tout } (\ell, m) \in \mathbb{Z}^2,$$

où $\overline{m}$ désigne la classe de congruence de $m$ modulo $n$. En fait, $\mathbb{Z}/n\mathbb{Z}$ est le groupe quotient de $\mathbb{Z}$ par son sous-groupe $n\mathbb{Z} = \{mn : m \in \mathbb{Z}\}$. De plus, la surjection canonique $s$ définie de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ par

$$s(m) = \overline{m} \qquad \text{pour tout } m \in \mathbb{Z}$$

est un morphisme de groupes. Comme $\mathbb{Z}$ est monogène, nous pouvons appliquer 1.1.1, ce qui nous permet d'affirmer que $\mathbb{Z}/n\mathbb{Z}$ est monogène. Etant par ailleurs fini, $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Notons au passge que $\overline{1}$ est un générateur du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$. Signalons également que $\mathbb{Z}/0\mathbb{Z}$ est identifié à $\mathbb{Z}$.

Avant de poursuivre notre étude, rappelons que $H$ est un sous-groupe de $\mathbb{Z}$ si, et seulement si, il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. Nous arrivons, à présent, au résultat central de cette section.

**Théorème 1.1.2** *Un groupe $G$ est monogène si, et seulement si, il existe $n \in \mathbb{N}$ tel que $G$ soit isomorphe au groupe $\mathbb{Z}/n\mathbb{Z}$.*

**Démonstration.** La condition proposée pour que $G$ soit monogène est evidemment suffisante. Montrons qu'elle est nécéssaire. Soient $G$ un groupe monogène et $g$ un générateur de $G$. Nous avons donc

$$G = \{g^m : m \in \mathbb{Z}\}.$$

Considérons l'application $s$ définie de $\mathbb{Z}$ dans $G$ par

$$s(m) = g^m \qquad \text{pour tout } m \in \mathbb{Z}.$$

Il n'est pas ardu de voir que $\varphi$ est morphisme de groupes surjectif. Le premier théorème d'isomorphismes[1] assure le fait $G$ est isomorphe au groupe quotient $\mathbb{Z}/\ker\varphi$, où $\ker\varphi$ désigne le noyau de $\varphi$. Or, comme $\ker\varphi$ est un sous-groupe de $\mathbb{Z}$, il existe $n \in \mathbb{N}$ tel que $\ker\varphi = n\mathbb{Z}$. Par conséquent, $G$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et le problème est résolu. ■

Distinguons le cas où le groupe considéré est infini.

**Corollaire 1.1.3** *Un groupe est monogène infini si, et seulement si, il est isomorphe à $\mathbb{Z}$.*

**Démonstration.** Soit $G$ un groupe. Il est évident que si $G$ est isomorphe à $\mathbb{Z}$ alors $G$ est monogène infini. Inversement, supposons que $G$ est monongène infini. D'après 1.1.2, il existe $n \in \mathbb{N}$ tel que $G$ soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Mais comme $G$ est infini, $\mathbb{Z}/n\mathbb{Z}$ doit être infini, ce qui donne $n = 0$. Finalment, $G$ est isomorphe à $\mathbb{Z}$. ■

Traîtons le cas fini.

**Corollaire 1.1.4** *Un groupe $G$ est cyclique si, et seulement si, il existe $n \in \mathbb{N}^*$ tel que $G$ soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

**Démonstration.** Soit $G$ un groupe. Il est clair que s'il existe $n \in \mathbb{N}^*$ tel que $G$ soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$ alors $G$ est cyclique. Réciproquement, supposons que $G$ est cyclique. En vertu de 1.1.2, il existe $n \in \mathbb{N}$ tel que $G$ soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$. De plus, $G$ est fini et, par suite, $\mathbb{Z}/n\mathbb{Z}$ est fini. Il vient que $n \neq 0$. ■

A titre d'exemples, pour tout $n \in \mathbb{N}^*$, le groupe $\mu_n$ présenté dans l'introduction à ce chapitre est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Dans la suite, nous montrons que tout groupe fini d'ordre premier est cyclique.

**Proposition 1.1.5** *Tout groupe fini d'ordre un nombre premier $p$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$..*

**Démonstration.** Soit $G$ un groupe tel que $\mathrm{o}(G)$ soit un nombre premier. Comme $G$ n'est pas réduit à son élément neutre (rappelons au passage que 1 n'est pas premier), nous pouvons choisir $g \in G$ tel que $g \neq e$. D'après le théorème de Lagrange[2], $\mathrm{o}(g)$ divise $\mathrm{o}(G)$. Mais puisque $\mathrm{o}(G)$ est premier et $g \neq e$, nous obtenons $\mathrm{o}(g) = \mathrm{o}(G)$ et par suite $G = \langle g \rangle$. Autrement dit, $G$ est cyclique. Nous pouvons ainsi conclure grâce à 1.1.4. ■

Achevons cette section par un exemple d'un groupe cyclique tiré de la gémétrie plane. Supposons que $\mathbb{R}^2$ soit muni de sa struture canonique de plan affine euclidien et choisissons $n \in \mathbb{N}^*$. Considérons $\Pi_n$, un polygone régulier à $n$ cotés.

[1] Premier théorème d'isomorphismes : *Si $\phi$ est un morphisme de groupe surjectif d'un groupe $G$ sur un groupe $H$ alors $H$ est isomorphe au groupe quotient $G/\ker\phi$.*

[2] *Joseph-Louis Lagrange*, mathématicien français (1736-1813).
Théorème de Lagrange : *L'ordre d'un sous-groupe d'un groupe fini $G$ divise l'ordre de $G$.*

Muni de la composition des applications, l'ensemble $\mathcal{D}(\Pi_n)$ des déplacements de $\mathbb{R}^2$ laissant globalement invariant $\Pi_n$ est cylique d'ordre $n$ et la rotation de centre l'isobarycentre de $\Pi_n$ et d'angle $2\pi/n$ est un générateur de $\mathcal{D}(\Pi_n)$. Tenant compte de 1.1.2, nous pouvons représenter un groupe cyclique d'ordre $n$ de différentes manières : La première est algébrique avec $\mu_n$, la deuxième relève de l'arithmétique avec $\mathbb{Z}/n\mathbb{Z}$ et la troisième est de nature géométrique avec $\mathcal{D}(\Pi_n)$.

## 1.2 Générateurs d'un groupe monogène

Comme les seuls sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$, nous pouvons appliquer 1.1.3 pour voir que tout sous-groupe non réduit à l'élément neutre d'un groupe monogène infini est isomorphe à $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}^*$.

**Proposition 1.2.1** *Tout sous-groupe non réduit à l'élément neutre d'un groupe monogène infini (respectivement, d'un groupe cyclique) est monogène infini (respectivement, un groupe cyclique).*

**Démonstration.** Compte tenu de ce qui a été dit juste avant cette proposition, il nous reste à envisager le cas d'un groupe cyclique. D'après 1.1.4, il suffit de montrer que si $n \in \mathbb{N}^*$ alors tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Soit alors $H$ un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. L'image réciproque $s^{-1}(H)$ par la surjection canonique $s$ de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Il existe alors $m \in \mathbb{N}$ tel que $s^{-1}(H) = m\mathbb{Z}$. La restriction de $s$ à $m\mathbb{Z}$ induit manifestement un morphisme de groupes surjectif de $m\mathbb{Z}$ sur $H$. Le reste se déduit directement de 1.1.1. ■

Dans la suite, nous caractérisons les diviseurs de l'ordre d'un groupe cyclique en fonctions de ses sous-groupes.

**Théorème 1.2.2** *Soient $G$ un groupe cyclique et $d$ un entier naturel non nul. Alors $d$ divise $\mathrm{o}(G)$ si, et seulement si, il existe un unique sous-groupe de $G$ d'ordre $d$.*

**Démonstration.** S'il existe un unique sous-groupe de $G$ d'ordre $d$ alors le théorème de Lagrange prouve que $d$ divise $\mathrm{o}(G)$. Inversement, supposons que $d$ divise $\mathrm{o}(G)$ et posons $q = \mathrm{o}(G)/d$. Considérons un générateur $g$ de $G$ et notons $f = g^q$. Si $f^{d-1} = e$ alors $g^{\mathrm{o}(G)-q} = e$, ce qui contredit le fait que $g$ est d'ordre $\mathrm{o}(G)$. Donc $f^{d-1} \neq e$. Par ailleurs, $f^d = g^{qd} = g^{\mathrm{o}(G)} = e$. Il vient que $f$ est d'ordre $d$. Le sous-groupe $\langle f \rangle$ de $G$ est d'ordre $d$. L'existence étant établie, prouvons l'unicité. Soit $H$ un sous-groupe d'ordre $d$ de $G$. Comme $G$ est cyclique, il en est de même pour $H$ et ce d'après 1.2.1. Soit $h$ un générateur de $H$. Il existe $r \in \{1, ..., \mathrm{o}(G) - 1\}$ tel que $h = g^r$. Ainsi, $g^{rd} = h^d = e$ car $h$ est d'ordre $d$. Il vient que $\mathrm{o}(G) = qd$ divise $rd$. Donc $q$ divise $r$. Posons $\ell = r/q$ et observons que

$$h = g^r = g^{\ell q} = f^\ell \in \langle f \rangle .$$

Donc, d'une part, $\langle h\rangle$ et $\langle f\rangle$ sont deux groupes cycliques d'ordre $d$ et, d'autre part, $h \in \langle f\rangle$. Il en résulte que $H = \langle h\rangle = \langle f\rangle$ et l'unicité en découle. ■

Les groupes finis d'ordre premiers (qui sont cycliques d'après 1.1.5) peuvent-être caractérisés en fonctions de leurs sous-groupes. Mais rappelons d'abord que les **sous-groupes triviaux** du groupe $G$ sont $\{e\}$ et $G$.

**Corollaire 1.2.3** *Soit $G$ un groupe non réduit à son élément neutre. Alors $G$ est fini d'ordre premier si, et seulement, si les seul sous-groupes de $G$ sont les sous-groupes triviaux.*

**Démonstration.** Si $G$ est d'ordre premier alors, d'après le théorème de Lagrange, les sous-groupes triviaux de $G$ sont les seuls sous-groupes de $G$. Inversement, supposons que les sous-groupes triviaux de $G$ sont les seuls sous-groupes de $G$ et choisissons $g \in G$ avec $g \neq e$. Donc le sous-groupe $\langle g\rangle$ de $G$ engendré par $g$ n'est pas réduit à $\{e\}$ et donc, en vertu de la condition imposée à $G$, $\langle g\rangle = G$. Il vient que $G$ est monogène. Le reste peut être établi aisément via 1.2.2. ■

La deuxième partie de cette section est consacrée aux générateurs d'un groupe monongène.

**Théorème 1.2.4** *Tout groupe monogène infini possède exactement deux générateurs inverse l'un de l'autre.*

**Démonstration.** Soient $G$ un groupe monongène infini et $g$ un générateur de $G$. Soit $h$ un autre générateur de $G$ et $\varphi_h$ l'isomorphisme de groupes de $\mathbb{Z}$ sur $G$ défini par

$$\varphi_h(m) = h^m \qquad \text{pour tout } m \in \mathbb{Z}.$$

Comme $g$ est un générateur de $G$, $\varphi_h^{-1}(g)$ est obligatoirement un générateur de $\mathbb{Z}$. Mais les seuls générateurs de $\mathbb{Z}$ sont manifestement 1 et $-1$. Donc, $g = \varphi_h(1) = h$ ou $g = \varphi_h(-1) = h^{-1}$. Ce qu'il fallait démontrer. ■

Envisageons le cas fini. Notons $m \wedge n$ (respectivement, $m \vee n$) le plus grand diviseur commun (respectivement, le plus petit multiple commun) de deux entiers naturels non nuls $m$ et $n$. En particulier, $m$ et $n$ sont premeirs entre eux si, et seulement si, $m \wedge n = 1$.

**Théorème 1.2.5** *Soient $G$ un groupe cyclique non réduit à son élément neutre et $g$ un générateur de $G$. Alors un élément $h \in G$ engendre $G$ si, et seulement si, il existe $m \in \{1, 2, ..., \mathrm{o}(G) - 1\}$ tel que $h = g^m$ et $m \wedge \mathrm{o}(G) = 1$.*

**Démonstration.** Supposons que $h \in G$ soit un générateur de $G$. Comme $G \neq \{e\}$ et $h \in G = \left\{e, g, g^2, ..., ^{\mathrm{o}(G)-1}\right\}$, il existe $m \in \{1, ..., \mathrm{o}(G) - 1\}$ tel que $h = g^m$. Alors

$$e = g^{m \vee \mathrm{o}(G)} = h^{\mathrm{o}(G)/m \wedge \mathrm{o}(G)}.$$

Or, étant générateur de $G$, $h$ est d'ordre $\mathrm{o}(G)$. D'après le théorème de Lagrange, $\mathrm{o}(G)$ divise $\mathrm{o}(G)/m \wedge \mathrm{o}(G)$. Par suite, $m \wedge \mathrm{o}(G) = 1$. Inversement, supposons qu'il existe $m \in \{1, 2, ..., \mathrm{o}(G) - 1\}$ tel que $h = g^m$ et $m \wedge \mathrm{o}(G) = 1$. D'après l'identité de Bezout[3], il existe $u, v \in \mathbb{Z}$ tels que $um + v\mathrm{o}(G) = 1$. Donc

$$g = g^{um+v\mathrm{o}(G)} = h^u.$$

Nous déduisons aussitôt que $h$ engendre $G$. ■

Soient $n \in \mathbb{N}^*$ et $m \in \{1, 2, ..., n\}$. D'après 1.2.5, la classe de congruence de $m$ modulo $n$ engendre le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, $m$ est premier avec $n$.

## 1.3 Fonction indicatrice d'Euler

Pour tout $n \in \mathbb{N}^*$, notons $\mathcal{P}_n$ le sous-ensemble de $\{1, 2, ..., n\}$ des nombres premiers avec $n$. Le cardinal de $\mathcal{P}_n$ est noté $\varphi(n)$. En posant $\varphi(1) = 1$, nous obtenons une application $\varphi$ définie de $\mathbb{N}^*$ vers $\mathbb{N}^*$ par

$$\varphi(n) = \mathrm{card}(\mathcal{P}_n) \qquad \text{pour tout } n \in \mathbb{N}^*.$$

L'application $\varphi$ est appelée **fonction indicatrice d'Euler**[4]. Il est clair que si $p \in \mathbb{N}$ est un nombre premier alors $\varphi(p) = p - 1$.

**Proposition 1.3.1** *Un groupe cyclique d'ordre $n \in \mathbb{N}^*$ possède $\varphi(n)$ générateurs.*

**Démonstration.** Appliquer directement 1.2.5. ■

En particulier, un groupe cyclique d'ordre premier $p$ possède $p-1$ générateurs. Pour poursuivre l'étude de la fonction indictrice d'Euler, nous avons besoin de rappeler certains faits concernant le **groupe produit** de deux groupes. Soient $G$ et $H$ deux groupes dont les lois sont notées multiplicativement. Nous pouvons définir une loi de composition interne sur le produit cartésien $G \times H$ en posant

$$(g, h)(g', h') = (gg', hh') \qquad \text{pour tout } ((g, h), (g', h')) \in (G \times H)^2.$$

Nous obtenons une structure de groupe sur $G \times H$. En particulier, si $e_G$ désigne l'élément neutre de $G$ et $e_H$ désigne celui de $H$, le couple $(e_G, e_H)$ est l'élément neutre de $G \times H$.

**Théorème 1.3.2** *Soient $G$ et $H$ deux groupes cycliques d'ordres respectifs $m, n \in \mathbb{N}^*$. Le groupe $G \times H$ est cyclique si, et seulement si, $m \wedge n = 1$.*

[3] *Etienne Bezout*, mathématicien français (1730-1783).
Théorème de Bezout : *Deux entiers relatifs $a$ et $b$ sont premiers entre eux si, et seulement si, il existe deux entiers realtifs $u$ et $v$ tels que $au - bv = 1$.*

[4] *Leonhard Euler*, mathématicien suisse (1707-1783)

**Démonstration.** Comme $G$ est d'ordre $m$ et $H$ est d'ordre $n$, le produit cartésien $G \times H$ est de cardinal le produit $mn$.

Soient $g$ un générateur de $G$ et $h$ un générateur de $H$. Nous savons que $g$ est d'ordre $m$ et $h$ est d'ordre $n$. Observons que

$$(g,h)^{m\vee n} = (g^{m\vee n}, h^{m\vee n}) = (e_G, e_H)\,.$$

D'où $m \vee n$ est un multiple de l'ordre de $(g,h)$ dans $G \times H$. Inversement, si $k \in \mathbb{N}^*$ vérifie $(g,h)^k = (e_G, e_H)$ dans $G \times H$ alors $\left(g^k, h^k\right) = (e_G, e_H)$. Par suite, $g^k = e_G$ et $h^k = e_H$. Nous en déduisons que $m$ et $n$ divisent $k$. Il en résulte que $m \vee n$ est l'ordre de $(g,h)$ dans $G \times H$.

Si $m \wedge n = 1$ et donc $mn = m \vee n$ alors $(g,h)$ est un élément d'ordre $mn = \mathrm{o}\,(G \times H)$ dans $G \times H$. Par conséquent, $G \times H$ est cyclique et $(g,h)$ se présente comme un générateur de $G \times H$.

Réciproquement, si $G \times H$ est cyclique alors il existe un élément $(g,h)$ d'ordre $mn$ dans $G \times H$. Soient $g' \in G$ et $h' \in H$. Il existe $k \in \mathbb{N}$ tel que $(g',h') = (g,h)^k = \left(g^k, h^k\right)$. D'où $g' = g^k$ et $h' = h^k$. Il vient que $g$ engendre $G$ et $h$ engendre $H$. Mais d'après ce qui précède, $(g,h)$ est d'ordre $m \vee n$ dans $G \times H$. Par suite, $mn = m \vee n$ et ainsi $m \wedge n = 1$. ■

Le cas particulier où $G = \mathbb{Z}/m\mathbb{Z}$ et $H = \mathbb{Z}/n\mathbb{Z}$ s'énoncer comme suit.

**Corollaire 1.3.3** *Soient $m, n \in \mathbb{N}^*$. Alors $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/mn\mathbb{Z}$ si, et seulement si, $m \wedge n = 1$.*

**Démonstration.** C'est une conséquence directe de 1.1.4 et 1.3.2. ■

Un application $\phi$ de $\mathbb{N}^*$ vers $\mathbb{N}^*$ est dite **multiplicative** si

$$\phi\,(mn) = \phi\,(m)\,\phi\,(n) \qquad \text{pour tout } (m,n) \in (\mathbb{N}^*)^2 \text{ avec } m \wedge n = 1.$$

**Théorème 1.3.4** *La fonction indicatrice d'Euler est multiplicative.*

**Démonstration.** Soient $m, n \in \mathbb{N}\setminus\{0\}$ tels que $m \wedge n = 1$. D'après 1.3.1, $\mathbb{Z}/m\mathbb{Z}$ possède $\varphi\,(m)$ générateurs et $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi\,(n)$ générateurs. Or, $m \wedge n = 1$ et donc, d'après 1.3.3, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique. Manifestement, les générateurs de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont les couples dont les premières composantes engendrent $\mathbb{Z}/m\mathbb{Z}$ et les deuxièmes engendrent $\mathbb{Z}/n\mathbb{Z}$. Il vient que le produit $\varphi\,(m)\,\varphi\,(n)$ est le nombre de générateurs de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. En utilisant une fois de plus 1.3.1 et 1.3.3, nous constatons que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ admet le même nombre de générateurs que $\mathbb{Z}/mn\mathbb{Z}$, à savoir, $\varphi\,(mn)$. Nous en déduisons que $\varphi$ est multiplicative. ■

Nous sommes à présent en mesure de calculer $\varphi\,(n)$ pour n'importe quel $n \in \mathbb{N}^*$, à condition de pouvoir écrire la décomposition de $n$ en produits de facteurs premiers.

**Corollaire 1.3.5** *Soient $n \in \mathbb{N}^*$ et $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ la décomposition de $n$ en produit de facteurs premiers. Alors*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

**Démonstration.** Soient $p$ un nombre premier et $m \in \mathbb{N}^*$. Nous avons déjà signalé que $\varphi(p) = p - 1$. Nous nous proposons de calculer $\varphi(p^m)$. Par définition de la fonction indicatrice d'Euler, nous avons

$$\varphi(p^m) = \operatorname{card}(\mathcal{P}_{p^m}) = \operatorname{card}(\{k \in \{1, ..., p^m\} : k \wedge p^m = 1\}).$$

D'après le théorème de Gauss[5], si $k \in \{1, ..., p^m\}$ alors $k \wedge p^m = 1$ si, et seulement si, $p$ ne divise $k$. Ainsi, $k \in \{1, ..., p^m\} \setminus \mathcal{P}_{p^m}$ si, et seulement si, il existe $q \in \{1, ..., p^{m-1}\}$ tel que $k = qp$. Par suite,

$$\{1, ..., p^m\} \setminus \mathcal{P}_{p^m} = \left\{qp : q \in \left\{1, ..., p^{m-1}\right\}\right\}.$$

Il vient que

$$\varphi(p^m) = \operatorname{card}(\mathcal{P}_{p^m}) = \operatorname{card}\{1, ..., p^m\} - \operatorname{card}(\{1, ..., p^m\} \setminus \mathcal{P}_{p^m}) = p^m - p^{m-1}.$$

Appliquons ce que nous venons d'établir à $n$. Comme $\varphi$ est multiplicative (voir 1.3.4), nous pouvons écrire

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}) = \varphi(p_1^{m_1})\varphi(p_2^{m_2})\cdots\varphi(p_r^{m_r}) \\ &= \left(p_1^{m_1} - p_1^{m_1-1}\right)\left(p_2^{m_2} - p_2^{m_2-1}\right)\cdots\left(p_r^{m_r} - p_r^{m_r-1}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).\end{aligned}$$

Ce qu'il fallait démontrer. ■

Nous terminons ce chapitre avec une dernière formule faisant intervenir la fonction indicatrice d'Euler.

**Théorème 1.3.6** *Soient $n \in \mathbb{N}^*$ et $\mathcal{D}_n$ l'ensemble des diviseurs de $n$. Alors*

$$n = \sum_{d \in \mathcal{D}_n} \varphi(d).$$

**Démonstration.** Considérons $d \in \mathcal{D}(n)$. Notons $A_d$ l'ensemble des éléments d'ordre $d$ dans $\mathbb{Z}/n\mathbb{Z}$. D'après 1.2.2, il y a un seul sous-groupe $G_d$ de $\mathbb{Z}/n\mathbb{Z}$ d'ordre $d$. Nous en déduisons que $A_d \subset G_d$ et, plus précisément, $A_d$ est l'ensemble des générateurs de $G_d$ qui est cyclique d'après 1.2.1. Ainsi, $\operatorname{card}(A_d) = \varphi(d)$. Mais la famille $\{A_d : d \in \mathcal{D}_n\}$ forment visiblement une partition de $\mathbb{Z}/n\mathbb{Z}$, ce qui nous permet de conclure. ■

[5] *Carl Frédérik Gauss*, mathématicien allemand (1777-1855).

Théorème de Gauss : *Si $a, b, c$ sont trois entiers naturels tels que $a$ divise $bc$ et $a$ est premier avec $b$ alors $a$ divise $c$.*

## 1.4 Exercices

**Exercice 1.4.1** Montrer les assertions suivantes.

(**1**) Le groupe $(\mathbb{Q}, +)$ n'est pas monogène.

(**2**) Le groupe $(\mathbb{R}, +)$ n'est pas monogène.

(**3**) Si $H$ est un sous-groupes monogène non nul de $(\mathbb{Q}, +)$ alors $H$ est infini.

**Exercice 1.4.2** Est-ce qu'un groupe dont tout sous-groupe propre[6] est cyclique est lui-même cyclique ?

**Exercice 1.4.3** Soient $m \in \mathbb{N}^*$ et $G$ un groupe abélien fini. L'élément neutre de $G$ est noté $e$.

(**1**) Montrer, par récurrence sur $\mathrm{o}(G)$, que si $g^m = e$ pour tout $g \in G$ alors $\mathrm{o}(G)$ divise une puissance de $m$.

(**2**) En déduire que si $p$ est un diviseur premier $\mathrm{o}(G)$ alors $G$ contient un élément d'ordre $p$.

(**3**) En déduire que s'il existe des nombres premiers $p_1, ..., p_n$ deux à deux distincts tels que $\mathrm{o}(G) = p_1 p_2 \cdots p_n$ alors $G$ est cyclique.

**Exercice 1.4.4** Soit $G$ un groupe.

(**1**) Montrer que si le groupe quotient $G/\mathcal{Z}(G)$ est cyclique alors $G$ est abélien.

(**2**) En déduire que l'indice de $\mathcal{Z}(G)$ dans $G$ n'est pas premier.

**Exercice 1.4.5** Soit $n \in \mathbb{N}^*$. La classe de congruence modulo $n$ de $m \in \mathbb{Z}$ est notée $\overline{m}$.

(**1**) Vérifier que le groupe additif $\mathbb{Z}/n\mathbb{Z}$, muni de la multiplication $\times$ définie par

$$\overline{\ell} \times \overline{m} = \overline{\ell m} \qquad \text{pour tout } (\ell, m) \in \mathbb{Z}^2,$$

est un anneau commutatif unitaire. Le groupe des éléments inversibles[7] de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^*$.

(**2**) Montrer que si $m \in \mathbb{Z}$ alors $\overline{m}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^*$. Quel est alors l'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$?

(**3**) (Théorème d'Euler) En déduire que si $a \in \mathbb{Z}$ est premier avec $n$ alors

$$a^{\varphi(n)} \equiv 1 \,(\mathrm{mod}\, n)\,.$$

[6] Un sous-groupe $H$ d'un groupe $G$ est dit **propre** si $H \subsetneq G$.

[7] Rappelons que si $A$ est un anneau commutatif unitaire alors l'ensemble des éléments inversibles de $A$, souvent noté $A^*$, est un groupe multiplicatif.

(**4**) (Théorème de Fermat[8]) En déduire que si $a, p \in \mathbb{Z}$ avec $p$ premier alors

$$a^p \equiv a \,(\mathrm{mod}\, p)\,.$$

**Exercice 1.4.6** Soit $G$ un groupe abélien fini tel que, pour tout diviseur $d$ de $\mathrm{o}\,(G)$, l'équation $x^d = e$ $(x \in G)$ admet au plus $d$ solutions dans $G$, où $e$ désigne l'élément neutre de $G$.

(**1**) Soient $d$ un diviseur de $o(G)$ et $n_d$ le nombre d'éléments de $G$ d'ordre $d$. Montrer que $n_d \leq \varphi\,(d)$.

(**2**) En déduire que $G$ est cyclique.

**Exercice 1.4.7** Soient $n \in \mathbb{N}^*$ et $\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z})$ le groupe des automorphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$. Montrer que $\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z})$ et $(\mathbb{Z}/n\mathbb{Z})^*$, le groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, sont isomorphes et en déduire l'ordre de $\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z})$.

[8] *Pierre-Simon de Fermat*, mathématicien français (1601-1665).

# Chapitre 2

# Groupes symétriques

Tout au long de ce chapitre, $X$ désigne un ensemble non vide et $\mathrm{id}_X$ désigne l'application identitée de $X$. Sur l'ensemble des applications de $X$ vers lui-même, que nous notons $X^X$, nous introduisons une loi de composition interne, appelé **composition**, notée $\circ$ et définie par

$$(f \circ g)(x) = f(g(x)) \qquad \text{pour tout } ((f,g),x) \in \left(X^X\right)^2 \times X.$$

Cette loi est évidemment associative sur $X^X$ et admet $\mathrm{id}_X$ comme élément neutre. Cependant, muni de la composition, $X^X$ n'est pas un groupe, à moins que $X$ soit réduit à un singleton. En effet, si $X$ contient deux éléments distincts dont l'un deux est noté $x$ alors l'application $f$ définie de $X$ vers $X$ par

$$f(y) = x \qquad \text{pour tout } y \in X$$

n'admet pas d'inverse pour la composition. Pour remédier à cet inconvenient, nous considérons la restriction de la composition à $\mathfrak{S}(X)$, l'ensemble des bijections de $X$ sur lui-même. A propos, une bijection de $X$ sur $X$ est appelée **permutation** de $X$. Muni de la composition, $\mathfrak{S}(X)$ est manifestement un groupe, appelé **groupe symétrique** de $X$. L'objectif de ce chapitre est d'étudier le groupe symétrique d'un ensemble $X$.

Nous utilisons les lettres grèques pour désigner les éléments d'un groupe symétrique. Le noyau d'un morphisme de groupes $\varphi$ est noté $\ker(\varphi)$.

## 2.1 Généralités sur les groupes symétriques

Deux ensembles non vides et équipotents[1] ont, à un isomorphisme près, le même groupe symétrique.

[1] Deux ensembles non vides $X$ et $Y$ sont dit **équipotents** s'il existe une bijection de $A$ sur $B$.

**Proposition 2.1.1** *Soient $X$ et $Y$ deux ensembles non vides. Si $X$ et $Y$ sont équipotents alors $\mathfrak{S}(X)$ et $\mathfrak{S}(Y)$ sont isomorphes.*

**Démonstration.** Considérons une bijection $f$ de $X$ sur $Y$. L'application $\varphi_f$ définie de $\mathfrak{S}(X)$ vers $\mathfrak{S}(Y)$ par

$$\varphi_f(\sigma) = f \circ \sigma \circ f^{-1} \qquad \text{pour tout } g \in \mathfrak{S}(X)$$

est un isomorphisme de groupes. En effet, si $\sigma, \rho \in \mathfrak{S}(X)$ alors

$$\varphi_f(\sigma \circ \rho) = f \circ (\sigma \circ \rho) \circ f^{-1} = \left(f \circ \sigma \circ f^{-1}\right) \circ \left(f \circ \rho \circ f^{-1}\right) = \varphi_f(\sigma) \circ \varphi_f(\rho).$$

Donc $\varphi_f$ est un morphisme de groupes. De plus, si $\sigma \in \ker\left(\varphi_f\right)$ alors

$$\sigma = f^{-1} \circ f \circ \sigma \circ f^{-1} \circ f = f^{-1} \circ \varphi_f(\sigma) \circ f = f^{-1} \circ \mathrm{id}_Y \circ f = \mathrm{id}_Y.$$

Ce qui prouve que $\varphi_f$ est injectif. En outre, si $\sigma \in \mathfrak{S}(Y)$ alors

$$\sigma = f \circ f^{-1} \circ \sigma \circ f \circ f^{-1} = \varphi_f\left(f^{-1} \circ \sigma \circ f\right).$$

Ainsi $\varphi_f$ est surjectif. En résumé, $\varphi_f$ est un isomorphisme de groupes de $\mathfrak{S}(X)$ sur $\mathfrak{S}(Y)$. ■

Il est clair que si $X$ est un singleton $\{x\}$ alors $\mathfrak{S}(X) = \{\mathrm{id}_X\}$. Supposons, par ailleurs, que $X$ contient au moins deux éléments distincts $x$ et $y$. La permutation de $X$, notée $\tau_{xy}$, et définie par

$$\tau_{xy}(x) = y,\ \tau_{xy}(y) = x \quad \text{et} \quad \tau_{xy}(t) = t \qquad \text{pour tout } t \in X$$

est appelée **transposition** de $\mathfrak{S}(X)$. Parfois, une transposition $\tau_{xy}$ est notée $(x, y)$. Observons que $\tau_{xy}^2 = \mathrm{id}_X$, soit, toute transposition est égale à son propore inverse dans $\mathfrak{S}(X)$. Nous constatons aisément que si $X$ est réduit à une paire $\{x, y\}$ alors $\mathfrak{S}(X) = \{\mathrm{id}_X, \tau_{xy}\}$. Par conséquent, si $X$ est réduit à un singleton ou à une paire alors le groupe $\mathfrak{S}(X)$ est abélien. Dans la suite, nous comptons prouver la réciproque, à savoir, le groupe symétrique $\mathfrak{S}(X)$ n'est abélien que si $X$ contient un ou deux éléments. A cet effet, rappelons que le centre[2] d'un groupe $G$ est noté $\mathcal{Z}(G)$ et que $G$ est abélien si, et seulement si, $G = \mathcal{Z}(G)$.

**Théorème 2.1.2** *Soit $X$ un ensemble non vide. Le groupe symétrique $\mathfrak{S}(X)$ est abélien si, et seulement si, $X$ contient au plus deux éléments. En outre, si $X$ admet au moins trois éléments alors $\mathcal{Z}(\mathfrak{S}(X)) = \{\mathrm{id}_X\}$.*

[2]Le centre d'un groupe $G$ est donné par

$$\mathcal{Z}(G) = \{a \in G : ab = ba \quad \text{pour tout } b \in G\}.$$

**Démonstration.** Compte tenu de l'analyse faite ci-dessus, il reste à envisager le cas où $X$ contient au moins trois éléments. Soient alors $x, y, z \in X$ trois éléments distincts de $X$. Nous avons donc

$$(\tau_{xy} \circ \tau_{xz})(x) = \tau_{xy}(\tau_{xz}(x)) = \tau_{xy}(z) = z \neq y = \tau_{xz}(y) = \tau_{xz}(\tau_{xy}(x)) = (\tau_{xz} \circ \tau_{xy})(x).$$

Ceci nous permet de conclure que $\mathfrak{S}(X)$ n'est pas abélien.

Pour la deuxième partie du théorème, considérons $\sigma \in \mathfrak{S}(X) \setminus \{\mathrm{id}_X\}$ et choisissons $x \in X$ tel que $\sigma(x) \neq x$. Posons $y = \sigma(x)$. Comme $X$ contient au moins trois éléments, nous pouvons choisir un élément $z \in X$ autre que $x$ et que $y$. Observons que

$$(\sigma \circ \tau_{yz})(x) = \sigma(\tau_{yz}(x)) = \sigma(x) = y.$$

Or,

$$(\tau_{yz} \circ \sigma)(x) = \tau_{yz}(\sigma(x)) = \tau_{yz}(y) = z.$$

Il vient que $(\sigma \circ \tau_{yz}) \neq (\tau_{yz} \circ \sigma)$ et, par conséquent, $\sigma \notin \mathcal{Z}(\mathfrak{S}(X))$. Le résultat annoncé en découle. ■

Le **support** de $\sigma \in \mathfrak{S}(X)$ est l'ensemble noté $\mathrm{supp}(\sigma)$ et défini par

$$\mathrm{supp}(\sigma) = \{x \in X : \sigma(x) \neq x\}.$$

Il est clair que $\sigma = \mathrm{id}_X$ si, et seulement si, $\mathrm{supp}(\sigma) = \emptyset$ ; En outre, si $X$ contient plus de deux éléments alors $\sigma \in \mathfrak{S}(X)$ est une transposition si, et seulement si, $\mathrm{supp}(\sigma)$ est une paire.

**Proposition 2.1.3** *Soit $X$ un ensemble non vide. Si $\sigma \in \mathfrak{S}(X) \setminus \{\mathrm{id}_X\}$ alors $\sigma(x) \in \mathrm{supp}(\sigma)$ pour tout $x \in \mathrm{supp}(\sigma)$.*

**Démonstration.** Soient $x \in \mathrm{supp}(\sigma)$ et $y = \sigma(x)$. Supposons que $y \notin \mathrm{supp}(\sigma)$. Donc $\sigma(y) = y$ et, par suite, $x = y$ car $\sigma$ est injective. Nous aboutissons à une contradiction. Ceci montre que notre supposition est fausse et par suite $y \in \mathrm{supp}(\sigma)$. D'où le résultat. ■

Bien qu'en général $\mathfrak{S}(X)$ ne soit pas abélien, nous pouvons permuter deux permutations à supports disjoints.

**Théorème 2.1.4** *Soit $X$ un ensemble contenant au moins deux éléments. Alors deux permutations de $\mathfrak{S}(X)$ à supports disjoints commutent.*

**Démonstration.** Considérons $\sigma, \rho \in \mathfrak{S}(X)$ tels que $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\rho) = \emptyset$. Si l'un des deux supports est vide alors l'une des deux parmutations est $\mathrm{id}_X$. La propriété est dans ce cas vérifiée. Supposons donc que les deux supports soient non vides. Soit $x \in \mathrm{supp}(\sigma)$. Alors $x \notin \mathrm{supp}(\rho)$ et, d'après 2.1.3, $\sigma(x) \notin \mathrm{supp}(\rho)$. Par conséquent,

$$(\sigma \circ \rho)(x) = \sigma(x) \quad \text{et} \quad (\rho \circ \sigma)(x) = \sigma(x).$$

Le cas où $x \in \text{supp}(\rho)$ se traîte par symétrie des rôles de $\sigma$ et de $\rho$. Ainsi, $\sigma\rho$ et $\rho\sigma$ coïncident sur $\text{supp}(\sigma) \cup \text{supp}(\rho)$. Il nous reste à envisager le cas échéant où $x \notin \text{supp}(\sigma) \cup \text{supp}(\rho)$. Nous avons dans ce cas

$$(\sigma \circ \rho)(x) = x = (\rho \circ \sigma)(x).$$

En résumé, $\sigma \circ \rho = \rho \circ \sigma$, ce qui achève la démonstration. ■

A tout couple $(\sigma, x) \in \mathfrak{S}(X) \times X$, nous associons une partie de $X$ définie par

$$\Omega_\sigma(x) = \{\sigma^m(x) : m \in \mathbb{Z}\}$$

et appelée **$\sigma$-orbite** de $x$.

**Théorème 2.1.5** *Soient $X$ un ensemble non vide et $\sigma \in \mathfrak{S}(X)$. Alors la relation binaire $\mathcal{R}_\sigma$ définie sur $X$ par*

$$x\mathcal{R}_\sigma y \quad \textit{si, et seulement si,} \quad y \in \Omega_\sigma(x)$$

*est une relation d'équivalence et $\Omega_\sigma(x)$ est la classe d'équivalence de $x \in X$ modulo $\mathcal{R}_\sigma$.*

**Démonstration.** Soient $x, y, z \in X$. Comme $x = \sigma^0(x) \in \Omega_\sigma(x)$, la relation $\mathcal{R}_\sigma$ est reflexive. De plus, si $x\mathcal{R}_\sigma y$ alors il existe $m \in \mathbb{Z}$ tel que $y = \sigma^m(x)$. Il vient que $x = \sigma^{-m}(y) \in \Omega_\sigma(y)$ et donc $y\mathcal{R}_\sigma x$. Autrement dit, la relation $\mathcal{R}_\sigma$ est symétrique. Enfin, si $x\mathcal{R}_\sigma y$ et $y\mathcal{R}_\sigma z$ alors $y \in \Omega_\sigma(x)$ et $z \in \Omega_\sigma(y)$. Nous déduisons qu'il existe $m, n \in \mathbb{Z}$ tels que $y = \sigma^m(x)$ et $z = \sigma^n(y)$. Nous obtenons

$$z = \sigma^n(y) = \sigma^n(\sigma^m(x)) = (\sigma^n \circ \sigma^m)(x) = \sigma^{m+n}(x) \in \mathfrak{S}(X).$$

Il s'en suit que $\mathcal{R}_\sigma$ est transitive. ■

En particulier, les $\sigma$-orbites forment une partition de $X$. En outre, $\Omega_\sigma(x)$ est réduite à un singleton (et donc à $\{x\}$) si, et seulement si, $x \notin \text{supp}(\sigma)$. D'ailleurs, une $\sigma$-orbite réduite à un singleton est dite **ponctuelle**. A ce propos, 2.1.5 entraîne que les $\sigma$-orbites non ponctuelles forment une partition de $\text{supp}(\sigma)$.

**Théorème 2.1.6** *Soient $X$ un ensemble non vide, $\sigma \in \mathfrak{S}(X)$ et $\Omega$ une $\sigma$-orbite fini de cardinal $m \in \mathbb{N}$. Alors*

$$\Omega = \left\{x, \sigma(x), ..., \sigma^{m-1}(x)\right\} \quad \textit{et} \quad \sigma^m(x) = x \qquad \textit{pour tout } x \in \Omega.$$

**Démonstration.** Soit $x \in \Omega$ et $\mathfrak{N} = \{n \in \mathbb{N} : \sigma^n(x) = x\}$. Supposons que $\mathfrak{N} = \emptyset$ et observons que, dans ce cas, l'application de $\mathbb{N}$ dans $\Omega$ qui à tout $n$ fait correspondre $\sigma^n(x)$ est injective. Ceci contredit le fait que $\Omega$ soit finie. Donc $\mathfrak{N} \neq \emptyset$. Posons alors $n_0 = \min(\mathfrak{N})$ et remarquons que $\sigma^{n_0}(x) = x$. Considérons

$n \in \mathbb{Z}$ et effectuons la division euclidienne de $n$ par $n_0$ pour trouver $q, r \in \mathbb{Z}$ tels que $n = qn_0 + r$ et $0 \leq r < n_0 - 1$. Donc,

$$\sigma^n(x) = \sigma^{qn_0+r}(x) = (\sigma^r \sigma^{qn_0})(x) = \sigma^r(x).$$

Par suite,

$$\Omega = \left\{x, \sigma(x), ..., \sigma^{n_0-1}(x)\right\}.$$

Choisissons $p, q$ dans $\{0, ..., n_0 - 1\}$ tels que $p < q$. Alors $\sigma^q(x) \neq \sigma^p(x)$ car, si non, $\sigma^{q-p}(x) = x$ et $q - p < n_0$ et donc $q - p \in \mathfrak{N}$ et $q - p < \min(\mathfrak{N})$, ce qui est une contradiction. Nous en déduisons que $m = n_0$ et donc

$$\Omega = \left\{x, \sigma(x), ..., \sigma^{m-1}(x)\right\} \quad \text{et} \quad \sigma^m(x) = x.$$

Ce qu'il fallait démontrer. ■

## 2.2 Groupes symétriques d'un ensemble fini

Supposons que $X$ soit un ensemble fini de cardinal $n \in \mathbb{N}^*$. Nous déduisons de 2.1.1 que l'étude de $\mathfrak{S}(X)$ revient à l'étude de $\mathfrak{S}(\{1, 2, ..., n\})$, le groupe symétrique de l'ensemble $\{1, 2, ..., n\}$, appelé désormais **groupe symétrique de degré** $n$ et noté $\mathfrak{S}_n$. A cet égard, l'élément neutre de $\mathfrak{S}_n$ est noté $\iota_n$. D'après 2.1.2, $\mathcal{Z}(\mathfrak{S}_n) = \{\iota_n\}$ dès que $n \geq 3$. La composé $\sigma \circ \rho$ de deux permutations $\sigma, \rho \in \mathfrak{S}_n$ est notée simplement $\sigma\rho$. Un permutation $\sigma \in \mathfrak{S}_n$ est souvent notée par

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

Le groupe $\mathfrak{S}_n$ est fini, ce qui ne semble pas très surprenant.

**Théorème 2.2.1** *Soit $n \in \mathbb{N}^*$. Le groupe symétrique $\mathfrak{S}_n$ est fini d'ordre $n!$.*

**Démonstration.** Démontrons le résultat par récurrence sur $n$. Le cas $n = 1$ étant trivial, considérons $n \geq 2$ et supposons que $\mathfrak{S}_{n-1}$ est fini d'ordre $(n-1)!$. Pour tout $x \in \{1, 2, ..., n\}$, posons

$$A_x = \{\sigma \in \mathfrak{S}_n : \sigma(n) = x\}.$$

Si $x \in \{2, ..., n-1\}$ alors l'application $\varphi_x$ définie de $A_x$ vers $A_n$ par

$$\varphi_x(\sigma) = \tau_{xn}\sigma \qquad \text{pour tout } \sigma \in A_x$$

est manifestement bijective. De plus, l'application $\varphi$ définie de $A_n$ vers $\mathfrak{S}_{n-1}$ par

$$\varphi(\sigma) = \begin{pmatrix} 1 & 2 & \cdots & n-1 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) \end{pmatrix} \qquad \text{pour tout } \sigma \in A_n$$

est également bijective. Par hypothèse de récurrence, $\mathfrak{S}_{n-1}$ est un ensemble fini de cardinal $(n-1)!$. Il vient que

$$\text{Card}\,(A_x) = (n-1)! \qquad \text{pour tout } x \in \mathbb{N}_n.$$

Or, la famille $(A_1, ..., A_n)$ forme une partition de $\mathfrak{S}_n$. Ainsi,

$$\text{Card}\,(\mathfrak{S}_n) = \sum_{x=1}^{n} \text{Card}\,(A_x) = n\,(n-1)! = n!.$$

Ce qui achève la démonstration. ■

Avant de continuer notre étude de $\mathfrak{S}_n$, remarquons que, pour tout $\sigma \in \mathfrak{S}_n$, les $\sigma$-orbites, étant des parties de $\{1, 2, ..., n\}$, sont finies. Une permutation $\sigma \in \mathfrak{S}_n$ est appelée **cycle** s'il existe une unique $\sigma$-orbite non ponctuelle. Dans ce cas, le cardinal de cette $\sigma$-orbite est appelé **longueur du cycle**. Pour tout $m \in \{1, 2, ..., n\}$, un cycle de longueur $m$ est appelé $m$**-cycle**. Une transposition $(x, y) \in \mathfrak{S}_n$ est un 2-cycle de support $\{x, y\}$.

En vertu de 2.1.6, nous pouvons affirmer que si $m \in \mathbb{N}$, $\sigma$ est un $m$-cycle de $\mathfrak{S}_n$ et $\Omega$ est l'unique $\sigma$-orbite non ponctuelle, alors

$$\Omega = \text{supp}\,(\sigma) = \left\{x, \sigma\,(x), ..., \sigma^{m-1}\,(x)\right\} \qquad \text{pour tout } x \in \Omega.$$

Un $m$-cycle $\sigma$ dont l'orbite est $\{x, \sigma\,(x), ..., \sigma^{m-1}\,(x)\}$ est noté $(x, \sigma\,(x), ..., \sigma^{m-1}\,(x))$.

Nous avons signalé auparavant qu'une transposition est égale à son propre inverse. Autrement dit, une transposition est un élément d'ordre 2 dans $\mathfrak{S}_n$. Ce résultat se généralise aux cycles de $\mathfrak{S}_n$.

**Proposition 2.2.2** *Soit $n \in \mathbb{N}^*$. Un $m$-cycle est un élément d'ordre $m$ dans $\mathfrak{S}_n$.*

**Démonstration.** Soient $m \in \mathbb{N}^*$ et $\sigma = (x, \sigma\,(x), ..., \sigma^{m-1}\,(x))$ un $m$-cycle dans $\mathfrak{S}_n$. D'après 2.1.6, $\Omega = \{x, \sigma\,(x), ..., \sigma^{m-1}\,(x)\}$ est l'unique $\sigma$-orbite non ponctuelle et est de cardinal $m$, $\sigma^{m-1}\,(x) \neq x$, ce qui prouve que $\sigma^{m-1} \neq \iota_n$. Par ailleurs, si $y \in \Omega$ alors $\sigma^m\,(y) = y$ et ce, encore, grâce à 2.1.6. En outre, pour $y \notin \Omega = \text{supp}\,(\sigma)$, $\sigma\,(y) = y$ et donc $\sigma^m\,(y) = y$. Finalement, $\sigma^m = \iota_n$ et $\sigma$ est d'ordre $m$. ■

Le lemme suivant sert à établir le résultat central de ce paragraphe.

**Lemme 2.2.3** *Soient $n \in \mathbb{N}^*$ et $\sigma_1, ..., \sigma_m$ des cycles de $\mathfrak{S}_n$ à supports deux à deux disjoints. Si $\sigma = \sigma_1 \cdots \sigma_m$ alors* $\text{supp}\,(\sigma_1), ..., \text{supp}\,(\sigma_m)$ *forment une partition de* $\text{supp}\,(\sigma)$ *et sont les $\sigma$-orbites non ponctuelles.*

**Démonstration.** Par hypothèse, $\text{supp}\,(\sigma_1), ..., \text{supp}\,(\sigma_m)$ sont deux à deux disjoints. Soient $x \in \cup_{k=1}^{m} \text{supp}\,(\sigma_k)$ et $\ell \in \{1, ..., m\}$ tel que $x \in \text{supp}\,(\sigma_\ell)$.

Donc $\sigma_\ell(x) \neq x$. En outre, $x \notin \text{supp}(\sigma_k)$ pour tout $k \in \{1,...,m\} \setminus \{\ell\}$ et par suite $\sigma_k(x) = x$ pour tout $k \in \{1,...,m\} \setminus \{\ell\}$. De plus, 2.1.4 entraîne que si $p, q \in \{1,...,m\}$ alors $\sigma_p \sigma_q = \sigma_q \sigma_p$. En résumé,

$$\sigma(x) = (\sigma_\ell \sigma_1 \cdots \sigma_{\ell-1} \sigma_{\ell+1} \cdots \sigma_m)(x) = \sigma_\ell(x) \neq x$$

et donc $x \in \text{supp}(\sigma)$. Inversement, si $x \in \text{supp}(\sigma)$ alors $\sigma(x) \neq x$ et par conséquent, il existe $\ell \in \{1,...,m\}$ tel que $\sigma_\ell(x) \neq x$, soit, $x \in \text{supp}(\sigma_\ell)$. Ainsi, $x \in \cup_{k=1}^m \text{supp}(\sigma_k)$ et donc

$$\text{supp}(\sigma) = \cup_{k=1}^m \text{supp}(\sigma_k).$$

Montrons à présent que $\text{supp}(\sigma_1), ..., \text{supp}(\sigma_m)$ sont les $\sigma$-orbites non ponctuelles de $\sigma$. Soient $x \in \text{supp}(\sigma)$ et $\ell \in \{1,...,m\}$ tel que $x \in \text{supp}(\sigma_\ell)$. Alors, tenant compte de 2.1.4, nous pouvons écrire

$$\begin{aligned}\Omega_\sigma(x) &= \{\sigma^p(x) : p \in \mathbb{Z}\} = \{(\sigma_1 \cdots \sigma_m)^p(x) : p \in \mathbb{Z}\} \\ &= \{\sigma_\ell^p(x) : p \in \mathbb{Z}\} = \Omega_{\sigma_\ell}(x) = \text{supp}(\sigma_\ell).\end{aligned}$$

Ainsi, $\text{supp}(\sigma_1), ..., \text{supp}(\sigma_m)$ sont des $\sigma$-orbites non ponctuelles. Par ailleurs, $\text{supp}(\sigma_1), ..., \text{supp}(\sigma_m)$ forment une partition de $\text{supp}(\sigma)$ et il en est de même pour les $\sigma$-orbites non ponctuelles. Il vient que $\text{supp}(\sigma_1), ..., \text{supp}(\sigma_m)$ sont précisément les $\sigma$-orbites non ponctuelles. ■

Nous sommes à présent en mesure d'établir le résultat principal de cette section, à savoir, que les cycles engendrent $\mathfrak{S}_n$.

**Théorème 2.2.4** *Soit $n \in \mathbb{N}^*$. Toute permutation dans $\mathfrak{S}_n \setminus \{\iota_n\}$ se décompose de manière unique (à l'ordre des facteurs près) en un produit de cycles à supports deux à deux disjoints.*

**Démonstration.** Soit $\sigma \in \mathfrak{S}_n \setminus \{\iota_n\}$. Il existe alors des $\sigma$-orbites non ponctuelles. Notons $\Sigma_1, ..., \Sigma_m$ toutes les $\sigma$-orbites non ponctuelles et considérons les permutation $\sigma_1, ..., \sigma_m \in \mathfrak{S}_n$ définies par, pour $\ell \in \{1,...,m\}$,

$$\sigma_\ell(x) = \sigma(x) \text{ si } x \in \Sigma_\ell \quad \text{et} \quad \sigma_\ell(x) = x \text{ sinon.}$$

Il est clair que , pour $\ell \in \{1,...,m\}$, $\Sigma_\ell$ est l'unique $\sigma_\ell$-orbite non ponctuelle. De ce fait, $\sigma_1, ..., \sigma_m$ sont des cycle à supports respectifs $\Sigma_1, ..., \Sigma_n$ qui sont deux à deux disjoints. De plus, si $x \in \text{supp}(\sigma)$ alors il existe $\ell \in \{1,...,m\}$ tel que $x \in \Sigma_\ell$. Donc $\sigma(x) = \sigma_\ell(x)$ et, en appliquant 2.1.4, nous obtenons

$$\sigma(x) = \sigma_\ell(x) = \sigma_\ell(\sigma_1 \cdots \sigma_{\ell-1} \sigma_{\ell+1} \cdots \sigma_m)(x) = (\sigma_1 \cdots \sigma_m)(x).$$

Si par ailleurs $x \notin \text{supp}(\sigma)$ alors $\sigma(x) = x = \sigma_\ell(x)$ pour tout $\ell \in \{1,...,m\}$ car

$$\text{supp}(\sigma) = \cup_{k=1}^m \Sigma_k = \cup_{k=1}^m \text{supp}(\sigma_k).$$

Finalement,

$$\sigma = \sigma_1 \cdots \sigma_m.$$

D'où l'existence de la décomposition de $\sigma$ en un produit de cycles à supports deux à deux disjoints.

Pour établir l'unicité, supposons que $\sigma = \gamma_1 \cdots \gamma_\ell$ soit une autre décomposition de $\sigma$ en produit de cycles à support deux à deux disjoints. D'après 2.2.3, les $\sigma$-orbites sont exactement $\text{supp}(\gamma_1), ..., \text{supp}(\gamma_\ell)$. Ceci prouve que $m = \ell$ et que, pour tout $i \in \{1, ..., m\}$, il existe $j \in \{1, ..., m\}$ tel que $\text{supp}(\gamma_i) = \text{supp}(\sigma_j)$. Nous en déduisons, via la disjonction des supports, que si $x \in \{1, ..., n\}$ alors

$$\gamma_i(x) = \sigma_j(x) = x \text{ si } x \in \text{supp}(\gamma_i) \quad \text{et} \quad \gamma_i(x) = \sigma_j(x) = \sigma(x) \text{ sinon.}$$

Il vient que $\gamma_i = \sigma_j$. D'où l'unicité. ■

La décomposition ci-dessus peut-être utilisée pour trouver l'ordre d'une permutation puisque dans un groupe fini $G$, l'ordre d'un produit de deux éléments d'ordres respectifs $\ell$ et $m$ qui commutent est égal à $\ell \vee m$.

A l'image des cycles, les transpositions engendrent le groupe $\mathfrak{S}_n$ pour $n \geq 2$. Ceci provient de la simple constatation que si $\sigma = (x_1, ..., x_m)$ est un $m$-cycle de $\mathfrak{S}_n$ alors $\sigma = (x_1, x_2) \cdots (x_{m-1}, x_m)$ est une décomposition de $\sigma$ en produits de transpositions. Cependant, ce résultat peut-être obtenu directement et avec un peu plus de précisions.

**Théorème 2.2.5** *Soit $n \in \mathbb{N}$ tel que $n \geq 2$. Toute permutation de $\mathfrak{S}_n$ est produit d'au plus $n-1$ transpositions.*

**Démonstration.** Comme $\mathfrak{S}_2 = \{e, (1,2)\}$, le résultat est vrai pour $n = 2$. Considérons $n \geq 3$ et supposons que toute permutation de $\mathfrak{S}_{n-1}$ se décompose en produit d'au plus $n-2$ transpositions. Soit $\sigma \in \mathfrak{S}_n$.

Supposons d'abord que $\sigma(n) = n$ et notons $\widetilde{\sigma}$ la permutation de $\mathfrak{S}_{n-1}$ définie par

$$\widetilde{\sigma}(x) = \sigma(x) \qquad \text{pour tout } x \in \{1, ..., n-1\}.$$

L'hypothèse de récurrence assure l'existence de $p$ ($p \leq n-2$) transpositions de $\mathfrak{S}_{n-1}$, notées $\widetilde{\tau}_1, ..., \widetilde{\tau}_p$, telles que

$$\widetilde{\sigma} = \widetilde{\tau}_1 \cdots \widetilde{\tau}_p.$$

Pour tout $i \in \{1, ..., p\}$, nous considèrons la transposition $\tau_i$ de $\mathfrak{S}_n$ définie par

$$\tau_i(n) = n \quad \text{et} \quad \tau_i(x) = \widetilde{\tau}_i(x) \qquad \text{pour tout } x \in \{1, ..., n-1\}.$$

Il est simple de constater que

$$\sigma = \tau_1 \cdots \tau_p$$

est produit d'au plus $n-2$ transpositions.

Supposons à présent que $\sigma(n) = x < n$. Posons $\gamma = \tau_{xn}\sigma$. Ainsi, $\gamma$ est une permutation de $\mathfrak{S}_n$ telle que $\gamma(n) = n$. D'après le cas précédent, il existe $p$ $(p \leq n-2)$ transpositions de $\mathfrak{S}_n$ telles que

$$\gamma = \tau_1 \cdots \tau_p.$$

Par suite,

$$\sigma = \tau_{xn}\tau_1 \cdots \tau_p.$$

Finalement, $\sigma$ est le produit d'au plus $n-1$ transpositions. ■

## 2.3 L'application signature

Dans cette section, nous considérons $n \in \mathbb{N}$ avec $n \geq 2$. Pour tout $\sigma \in \mathfrak{S}_n$, notons $\mu(\sigma)$ le nombre des $\sigma$-orbites. A titre d'exemples, $\mu(\iota_n) = n$ et $\mu(\tau) = n-1$ pour toute transposition de $\mathfrak{S}_n$. La **signature** de $\sigma$ est l'élément $\varepsilon(\sigma) \in \{-1, 1\}$ défini par

$$\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}.$$

Nous avons ainsi $\varepsilon(\iota_n) = 1$. De plus,

$$\varepsilon(\tau) = -1 \qquad \text{pour toute transposition } \tau \text{ de } \mathfrak{S}_n.$$

L'application de $\mathfrak{S}_n$ vers l'ensemble $\mathbb{C}^*$ des nombres complexes non nuls qui à toute permutation de $\mathfrak{S}_n$ fait correspondre sa signature est appelé **signature** sur $\mathfrak{S}_n$ et est notée $\varepsilon$. Pour continuer notre étude, rappelons que $\mathbb{C}^*$ est un groupe pour la multiplication.

**Théorème 2.3.1** *Soit $n \in \mathbb{N}^*$. L'application $\varepsilon$ est un morphisme de groupes de $\mathfrak{S}_n$ vers $\mathbb{C}^*$.*

**Démonstration.** Commençons par établir que si $\tau = (x, y)$ est une transposition de $\mathfrak{S}_n$ alors

$$\varepsilon(\sigma\tau) = -\varepsilon(\sigma) \qquad \text{pour tout } \sigma \in \mathfrak{S}_n.$$

Soient $\sigma \in \mathfrak{S}_n$ et $\rho = \sigma\tau$. Soit $\Omega$ une $\sigma$-orbite telle que $x, y \notin \Omega$. Considérons $z \in \Omega$. Nous avons donc $\Omega = \Omega_\sigma(z)$. Si $m \in \mathbb{N}^*$ alors

$$\begin{aligned}\rho^m(z) = (\sigma\tau)^m(z) &= (\sigma\tau)^{m-1}\sigma(\tau(z)) = (\sigma\tau)^{m-1}\sigma(z)\\ &= (\sigma\tau)^{m-2}\sigma(\tau(\sigma(z))) = (\sigma\tau)^{m-2}\sigma^2(z)\\ &= \cdots = (\sigma\tau)\sigma^{m-1}(z) = \sigma^m(z).\end{aligned}$$

Par suite, $\Omega = \Omega_\rho(z)$, qui est donc une $\rho$-orbite. En d'autres termes, les $\sigma$-orbites qui ne rencontrent pas $x$ et $y$ sont des $\rho$-orbites. Examinons alors $\Omega_\sigma(x)$ et $\Omega_\sigma(y)$. Posons $\text{card}(\Omega_\sigma(x)) = \ell$ et $\text{card}(\Omega_\sigma(y)) = m$. Nous pouvons écrire

$$\Omega_\sigma(x) = \left\{x, \sigma(x), ..., \sigma^{\ell-1}(x)\right\} \quad \text{et} \quad \Omega_\sigma(y) = \left\{y, \sigma(y), ..., \sigma^{m-1}(y)\right\}.$$

Si $\Omega_\sigma(x) = \Omega_\sigma(y)$ alors il existe un unique $r \in \{1, ..., \ell-1\}$ tel que $y = \sigma^r(x)$. Comme $\sigma^\ell(x) = x$ (voir 2.1.6), nous déduisons que

$$\Omega_\rho(x) = \left\{x, \sigma^{r+1}(x), ..., \sigma^{\ell-1}(x)\right\} \quad \text{et} \quad \Omega_\rho(y) = \left\{y, \sigma(x), ..., \sigma^{r-1}(x)\right\}.$$

Ainsi,

$$\Omega_\rho(x) \cup \Omega_\rho(y) = \Omega_\sigma(x) \quad \text{et} \quad \Omega_\rho(x) \cap \Omega_\rho(y) = \emptyset.$$

Il vient que $\mu(\sigma) = \mu(\rho) - 1$. Supposons enfin que $\Omega_\sigma(x) \neq \Omega_\sigma(y)$, soit, $\Omega_\sigma(x) \cap \Omega_\sigma(y) = \emptyset$. Nous obtenons,

$$\Omega_\rho(x) = \left\{x, \sigma(y), ..., \sigma^{m-1}(y), y, \sigma(x), ..., \sigma^{\ell-1}(x)\right\} = \Omega_\sigma(y).$$

Donc $\mu(\sigma) = \mu(\rho) + 1$. Finalement,

$$\varepsilon(\sigma\tau) = \varepsilon(\rho) = (-1)^{n-\mu(\rho)} = (-1)^{n-\mu(\sigma)\pm 1} = -(-1)^{n-\mu(\sigma)} = -\varepsilon(\sigma).$$

C'est ce que nous voulons obtenir dans cette première étape.

Soient alors $\sigma, \rho$ deux permutations de $\mathfrak{S}_n$. D'après 2.2.5, il existe des transpositions $\tau_1, ..., \tau_\ell, \tau_{\ell+1}, ..., \tau_m$ telles que

$$\sigma = \tau_1 \cdots \tau_\ell \quad \text{et} \quad \rho = \tau_{\ell+1} \cdots \tau_{\ell+m}.$$

En appliquant le résultat obtenu ci-dessus, nous observons que

$$\begin{aligned}\varepsilon(\sigma\rho) &= \varepsilon(\tau_1 \cdots \tau_{\ell+m}) = -\varepsilon(\tau_1 \cdots \tau_{\ell+m-1}) \\ &= \cdots = (-1)^{\ell+m} = (-1)^\ell (-1)^m = \varepsilon(\sigma)\sigma(\rho).\end{aligned}$$

En d'autres termes, $\varepsilon$ est morphisme de groupes de $\mathfrak{S}_n$ vers $\mathbb{C}^*$. ■

Nous pouvons donc calculer la signature d'un cycle de $\mathfrak{S}_n$.

**Corollaire 2.3.2** *Soient $n \in \mathbb{N}^*$ et $r \in \{2, ...n\}$. Alors $\varepsilon(\sigma) = (-1)^{r-1}$ pour tout $r$-cycle $\sigma$ de $\mathfrak{S}_n$.*

**Démonstration.** Posons

$$\sigma = (x_1, x_2, ..., x_r)$$

et observons que

$$\sigma = (x_1, x_2)(x_2, x_3) \cdots (x_{r-1}, x_r).$$

Donc

$$\varepsilon(\sigma) = \varepsilon((x_1, x_2)(x_2, x_3)\cdots(x_{r-1}, x_r)) = \prod_{k=1}^{r-1} \varepsilon((x_k, x_{x+1})) = \prod_{k=1}^{r-1} (-1) = (-1)^{r-1}.$$

Ce qu'il fallait démontrer. ■

La suite de notre étude est basée sur le fait que deux cycles de $\mathfrak{S}_n$ de même longueur sont conjugués.

**Proposition 2.3.3** *Soient $n \in \mathbb{N}^*$, $m \in \{1, ..., n\}$ et $\sigma, \rho$ deux $m$-cycles de $\mathfrak{S}_n$. Il existe une permutation $\delta \in \mathfrak{S}_n$ telle que $\rho = \delta\sigma\delta^{-1}$.*

**Démonstration.** Posons

$$\sigma = \left(x, \sigma(x), ..., \sigma^{m-1}(x)\right) \quad \text{et} \quad \rho = \left(y, \rho(y), .., \rho^{m-1}(y)\right).$$

Ecrivons

$$\{1, ..., n\} = \{x_1, ..., x_n\} = \{y_1, ..., y_n\},$$

où

$$x_\ell = \sigma^{\ell-1}(x) \quad \text{et} \quad y_\ell = \rho^{\ell-1}(y) \qquad \text{pour tout } \ell \in \{1, ..., m\}.$$

Définissons $\delta \in \mathfrak{S}_n$ en posant

$$\delta(x_\ell) = y_\ell \qquad \text{pour tout } \ell \in \{1, ..., n\}.$$

Pour tout $\ell \in \{1, ..., m\}$, nous avons

$$(\rho\delta)(x_\ell) = \rho(y_\ell) = \rho^\ell(y) = \delta\left(\sigma^\ell(x)\right) = \delta\left(\sigma\left(\sigma^{\ell-1}(x)\right)\right) = (\delta\sigma)(x_\ell).$$

Soit alors $\ell \in \{m+1, ..., n\}$. Nous écrivons

$$(\rho\delta)(x_\ell) = \rho(y_\ell) = y_\ell = \delta(x_\ell) = \delta(\sigma(x_\ell)) = (\delta\sigma)(x_\ell).$$

Ce qui montre que $\rho\delta = \delta\sigma$ et par conséquent $\rho = \delta\sigma\delta^{-1}$. ■

En particulier, deux transpositions de $\mathfrak{S}_n$ sont conjuguées.

Dans la suite, nous fournissons un moyen de calculer la signature d'une permutation.

**Théorème 2.3.4** *Soit $n \in \mathbb{N}^*$. Alors*

$$\varepsilon(\sigma) = \prod_{1 \le x < y \le n} \frac{\sigma(y) - \sigma(x)}{y - x} \qquad \textit{pour tout } \sigma \in \mathfrak{S}_n.$$

**Démonstration.** Posons

$$\mathcal{D} = \left\{(x,y) \in \{1,...,n\}^2 : x < y\right\}$$

et notons

$$\pi(\sigma) = \prod_{1 \leq x < y \leq n} \frac{\sigma(y) - \sigma(x)}{y - x} \qquad \text{pour tout } \sigma \in \mathfrak{S}_n.$$

Considérons $\sigma, \rho \in \mathfrak{S}_n$. Si $\delta = \rho\sigma$ alors

$$\begin{aligned}
\pi(\rho\sigma) = \pi(\delta) &= \prod_{(x,y)\in\mathcal{D}} \frac{\delta(y) - \delta(x)}{y - x} = \prod_{(x,y)\in\mathcal{D}} \frac{\delta(y) - \delta(x)}{\sigma(y) - \sigma(x)} \frac{\sigma(y) - \sigma(x)}{y - x} \\
&= \prod_{(x,y)\in\mathcal{D}} \frac{\rho(\sigma(y)) - \rho(\sigma(x))}{\sigma(y) - \sigma(x)} \prod_{(x,y)\in\mathcal{D}} \frac{\sigma(y) - \sigma(x)}{y - x} \\
&= \prod_{(x,y)\in\mathcal{D}} \frac{\rho(y) - \rho(x)}{y - x} \prod_{(x,y)\in D} \frac{\sigma(y) - \sigma(x)}{y - x} = \pi(\rho)\pi(\sigma).
\end{aligned}$$

Autrement dit, l'application $\pi$ ainsi définie de $\mathfrak{S}_n$ vers $\mathbb{C}^*$ est un morphisme de groupes. Pour établir que $\varepsilon$ et $\pi$ coïncident, il suffit, d'après 2.2.5, de montrer que $\varepsilon(\tau) = \pi(\tau)$ pour toute transposition $\tau$ de $\mathfrak{S}_n$. Commençons par la transposition $\tau_{12}$. Il est clair que si $y \in \{3,..,n\}$ alors

$$\frac{\tau_{12}(y) - \tau_{12}(x)}{y - x} = 1 \qquad \text{pour tout } x \in \{1,...,n\}.$$

Pour $x = 1$ et $y = 2$, nous avons

$$\frac{\tau_{12}(y) - \tau_{12}(x)}{y - x} = -1.$$

Ainsi, $\pi(\tau_{12}) \leq 0$. Or, nous voyons que $|\pi(\sigma)| = 1$ pour tout $\sigma \in \mathfrak{S}_n$. Il vient que $\pi(\tau_{12}) = -1$. Soit $\tau$ une transposition de $\mathfrak{S}_n$. D'après 2.3.3, il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que $\tau = \sigma\tau_{12}\sigma^{-1}$. D'où

$$\pi(\tau) = \pi\left(\sigma\tau_{12}\sigma^{-1}\right) = \pi(\sigma)\pi(\tau_{12})\pi(\sigma)^{-1} = \pi(\tau_{12}) = -1 = \varepsilon(\tau).$$

Ce qui donne le résultat demandé. ■

Le noyau du morphisme de groupes $\varepsilon$ est un sous-groupe de $\mathfrak{S}_n$ appelé **groupe alterné de degré** $n$ et est noté $\mathfrak{A}_n$. En d'autres termes,

$$\mathfrak{A}_n = \ker(\varepsilon) = \{\sigma \in \mathfrak{S}_n : \varepsilon(\sigma) = 1\}.$$

En tant que noyau d'un morphisme de groupes, $\mathfrak{A}_n$ est distingué[3] dans $\mathfrak{S}_n$.

[3] Un sous-groupe $H$ d'un groupe $G$ est dit **distingué** si $ghg^{-1} \in H$ pour tout $(g,h) \in G \times H$.

**Proposition 2.3.5** *Soit $n \in \mathbb{N}^*$. L'indice*[4] *de $\mathfrak{A}_n$ dans $\mathfrak{S}_n$ est égal à 2. Donc $\mathfrak{A}_n$ est d'ordre $n!/2$.*

**Démonstration.** Le premier théorème d'isomorphisme pour les groupes montre que le groupe quotient $\mathfrak{S}_n/\ker(\varepsilon)$ est isomorphe au sous-groupe $\mathrm{Im}(\varepsilon)$ de $\mathbb{C}^*$, où $\mathrm{Im}(\varepsilon)$ désigne l'image de $\varepsilon$. Or, il est clair que $\mathrm{Im}(\varepsilon) = \{-1, 1\}$. Il vient que $\mathfrak{S}_n/\mathfrak{A}_n$ est isomrophe à $\{-1, 1\}$ et par suite

$$2 = \mathrm{o}(\mathfrak{S}_n)/\mathrm{o}(\mathfrak{A}_n) = [\mathfrak{S}_n : \mathfrak{A}_n].$$

D'où le résultat. ■

Une permutation de $\mathfrak{A}_n$ est dite **paire**. Ainsi, une permutation **impaire** est un élément de $\mathfrak{S}_n \backslash \mathfrak{A}_n$. L'usage de cette terminologie est justifié par la proposition suivante.

**Proposition 2.3.6** *Soit $n \in \mathbb{N}^*$. Si $\sigma \in \mathfrak{S}_n$ alors $\sigma \in \mathfrak{A}_n$ si, et seulement si, $\sigma$ est produit d'un nombre pair de transpositions.*

**Démonstration.** Soit $\sigma \in \mathfrak{S}_n$. S'il existe $\tau_1, ..., \tau_{2m}$ des transpositions de $\mathfrak{S}_n$ telles que $\sigma = \tau_1 \cdots \tau_{2m}$ alors

$$\varepsilon(\sigma) = \varepsilon(\tau_1 \cdots \tau_{2m}) = \varepsilon(\tau_1) \cdots \varepsilon(\tau_{2m})$$

et ce d'après 2.3.1. Donc

$$\varepsilon(\sigma) = (-1)^{2m} = 1$$

et ainsi $\sigma \in \ker(\varepsilon) = \mathfrak{A}_n$.

Inversement, supposons que $\sigma \in \mathfrak{A}_n = \ker(\varepsilon)$. D'après 2.2.5, il existe $\tau_1, ..., \tau_m$ des transpositions de $\mathfrak{S}_n$ telles que $\sigma = \tau_1 \cdots \tau_m$. En utilisant une fois de plus 2.3.1, nous obtenons

$$1 = \varepsilon(\sigma) = \varepsilon(\tau_1 \cdots \tau_m) = \varepsilon(\tau_1) \cdots \varepsilon(\tau_m) = (-1)^m.$$

L'entier $m$ doit donc être pair, ce qui prouve le résultat demandé. ■

D'après 2.3.6, $\mathfrak{A}_n$ est engendré par les permutations produits de deux transpositions. Cette remarque est utile pour prouver que les 3-cycles engendrent $\mathfrak{A}_n$ dès que $n \geq 3$. C'est le dernier résultat de ce chapitre.

**Théorème 2.3.7** *Soit $n \in \mathbb{N}^*$ tel que $n \geq 3$. Alors les 3-cycles de $\mathfrak{S}_n$ engendrent $\mathfrak{A}_n$.*

[4] Si l'ensemble des classes à gauche modulo un sous-groupe $H$ de $G$ est fini alors son cardinal est appelé **indice** de $H$ dans $G$ et est noté $[G : H]$. Dans ce cas, $H$ est dit d'**indice fini** dans $G$.

**Démonstration.** Soit $(x, y, z)$ un 3-cycle de $\mathfrak{S}_n$. Comme

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

il vient que $\mathfrak{A}_n$ contient les 3-cycles de $\mathfrak{S}_n$.

Soient $x, y, z \in \{1, ..., n\}$ deux à deux distincts. Alors

$$(x, y)(x, y) = \iota_n = (x, y, z)^3 \text{ et } (x, y)(x, z) = (x, z, y).$$

En outre, si $n \geq 4$ et $u \in \{1, ..., n\} \setminus \{x, y, z\}$ alors

$$(x, y)(z, u) = (x, z, y)(x, z, u).$$

Nous venons d'envisager tous les cas possible ce qui nous permet d'affirmer que $\mathfrak{A}_n$ est bien engendré par les 3-cycles de $\mathfrak{S}_n$. ■

## 2.4 Exercices

**Exercice 2.4.1** Pour chacune des permutations suivantes, déterminer sa décomposition en produits de cycles à supports deux à deux disjoints, son ordre, sa signature et une décomposition en produits de transpositions.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_6$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix} \in \mathfrak{S}_9$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 2 & 1 & 8 & 7 & 9 & 11 & 12 & 10 & 5 & 6 \end{pmatrix} \in \mathfrak{S}_{12}$$

Calculer $\sigma^{50}, \rho^{100}$ et $\tau^{10}$.

**Exercice 2.4.2** Soit $n \in \mathbb{N}$ tel que $n \geq 2$. On pose

$$A = \{(1, x) : 2 \leq x \leq n\}$$
$$B = \{(x, x + 1) : 1 \leq x \leq n - 1\}$$
$$C = \{(1, 2), (1, 2, ..., n)\}$$

Montrer que $\mathfrak{S}_n$ est engendré par l'un quelconque des ensembles $A, B$ et $C$.

**Exercice 2.4.3** Soit $n \in \mathbb{N}$ tel que $n \geq 2$.

(**1**) Montrer que si $r \in \{2, 3, ..., n\}$ alors le nombre des $r$-cycles est égal à $(r - 1)!\complement_n^p$.

(**2**) En déduire que si $n$ est un nombre premier alors $\mathfrak{S}_n$ contient exactement $(n - 1)!$ éléments d'ordre $n$.

**Exercice 2.4.4** Soit $n \in \mathbb{N}$ tel que $n \geq 2$ et soit $\theta$ l'application définie de $\mathfrak{S}_n$ vers $\mathbb{C}^*$ par

$$\theta(\sigma) = 1 \quad \text{pour tout } \sigma \in \mathfrak{S}_n.$$

Montrer que $\theta$ et $\varepsilon$ sont les morphismes de groupes de $\mathfrak{S}_n$ dans le groupe multiplicatif $\mathbb{C}^*$.

**Exercice 2.4.5** Soit $(n, r) \in \mathbb{N}^2$ tel que $n \geq 2$ et $2 \leq r \leq n$. Montrer que si $\rho \in \mathfrak{S}_n$ et $\sigma = (x_1, ..., x_r)$ est un $r$-cycle de $\mathfrak{S}_n$ alors $\rho\sigma\rho^{-1}$ est le $r$-cycle $(\rho(x_1), ..., \rho(x_r))$.

**Exercice 2.4.6** Soit $n \in \mathbb{N}$ tel que $n \geq 3$. On pose

$$\begin{aligned} A &= \{(1, x)(1, y) : 2 \leq x, y \leq n\} \\ B &= \{(1, 2, x) : 3 \leq x \leq n\} \\ C &= \left\{\sigma^2 : \sigma \in \mathfrak{S}_n\right\} \end{aligned}$$

Montrer que $\mathfrak{A}_n$ est engendré par l'un quelconque des ensembles $A, B$ et $C$.

**Exercice 2.4.7** Déterminer le centre de $\mathfrak{A}_n$ pour $n \in \mathbb{N}^*$.

**Exercice 2.4.8** Montrer que si $n \in \mathbb{N}$ tel que $n \geq 3$ alors $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 dans $\mathfrak{S}_n$.

**Exercice 2.4.9** Dans $\mathfrak{S}_4$, on pose

$$H = \{\iota_4, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

(**1**) Vérifier que $H$ est un sous-groupe de $\mathfrak{S}_4$.

Dans la suite, on suppose que $\mathfrak{A}_4$ contient un sous-groupe $K$ d'ordre 6.

(**2**) Prouver que $K$ est distingué dans $\mathfrak{A}_4$.

(**3**) Montrer que $K$ contient un nombre pair de 3-cycles.

(**4**) Soient $x, y, z, t$ quatre éléments distincts de $\{1, 2, 3, 4\}$. Montrer que si $\sigma = (x, y, z)$ alors

$$\sigma(x, y)(z, t)\sigma^{-1} = (y, z)(x, t).$$

(**5**) En déduire que $H$ est contenu dans $K$.

(**6**) Conclure que $\mathfrak{A}_4$ ne contient pas de sous-groupes d'ordre 6.

# Chapitre 3

# Opération d'un groupe sur un ensemble

Soient $G$ un groupe et $X$ un ensemble non vide. Une **opération** de $G$ sur $X$ est une application $\omega$ de $G \times X$ vers $X$ vérifiant

$$(\mathbf{i})\ \omega(e,x) = x \quad \text{et} \quad (\mathbf{ii})\ \omega(g,\omega(h,x)) = \omega(gh,x) \quad \text{pour tout } ((g,h),x) \in G^2 \times X,$$

où $e$ désigne l'élément neutre de $G$. Il est commode de noter $\omega(g,x)$ par $g \cdot x$ pour tout $(g,x) \in G \times X$. Dans ce cas, les conditions (**i**) et (**ii**) ci-dessus s'écrivent

$$(\mathbf{i})\ e \cdot x = x \quad \text{et} \quad (\mathbf{ii})\ g \cdot (h \cdot x) = (gh) \cdot x \quad \text{pour tout } ((g,h),x) \in G^2 \times X.$$

Lorsqu'il existe une opération de $G$ sur $X$, nous disons que $G$ **opère** sur $X$ et que $X$ est un $G$-**ensemble**.

La notion de groupe opérant sur un ensemble est essentielle. En effet, c'est une notion qui permet d'obtenir des renseignements sur le groupe considéré comme nous le verrons avec les théorèmes de Sylow. Mais au delà de cet aspect, nous rencontrons souvent la notion de groupe opérant sur un ensemble en géométrie euclidienne et notemment pour la représentation de certains groupes géométriques. A cet égard, nous étudions dans ce chapitre le groupe du symplexe régulier.

Tout au long de ce chapitre, $G$ désigne un groupe dont l'élément neutre est noté $e$ et $X$ désigne un ensemble non vide.

## 3.1 Groupe opérant sur un ensemble

La notion de groupe opérant sur un ensemble est en lien trés étroit avec la notion de groupes symétriques. Rappelons que le groupe symétrique de $X$ est noté $\mathfrak{S}(X)$ et que l'application identitée de $X$ est notée $\mathrm{id}_X$.

**Théorème 3.1.1** *Soit $G$ un groupe. Un ensemble $X$ est un $G$-ensemble si, et seulement si, il existe un morphisme de groupes de $G$ vers $\mathfrak{S}(X)$.*

**Démonstration.** Supposons que $X$ est un $G$-ensemble. Pour tout $g \in G$, considérons $\gamma_g$ l'application de $X$ vers lui-même définie par

$$\gamma_g(x) = g \cdot x \quad \text{pour tout } x \in X.$$

Si $y \in X$ alors

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

Ainsi $\gamma_g$ est surjective. En outre, si $x, y \in X$ tels que $\gamma_g(x) = \gamma_g(y)$ alors

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

Ce qui montre que $\gamma_g$ est injective. D'où $\gamma_g$ est une permutation de $X$. Nous pouvons donc considérer l'application $\gamma$ définie de $G$ vers $\mathfrak{S}(X)$ par

$$\gamma(g) = \gamma_g \quad \text{pour tout } g \in G.$$

Si $g, h \in G$ et $x \in X$ alors

$$\gamma(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \gamma_g(\gamma_h(x)) = \left(\gamma_g \circ \gamma_h\right)(x) = (\gamma(g) \circ \gamma(h))(x)$$

et donc $\gamma(gh) = \gamma(g) \circ \gamma(h)$. Nous déduisons que $\gamma$ un morphisme de groupes.

Inversement, soit $\gamma$ un morphisme de groupes de $G$ sur $\mathfrak{S}(X)$. Considérons l'application de $G \times X$ vers $X$ qui à tout couple $(g, x) \in G \times X$ fait correspondre un élément $g \cdot x \in X$ défini par

$$g \cdot x = \gamma(g)(x).$$

Observons que, si $g, h \in G$ et $x \in X$ alors

$$g \cdot (h \cdot x) = \gamma(g)(\gamma(h)(x)) = (\gamma(g) \circ \gamma(h))(x) = \gamma(gh)(x) = (gh) \cdot x$$

et

$$e \cdot x = \gamma(e)(x) = \mathrm{id}_X(x) = x.$$

Il vient que $X$ est $G$-ensemble. ■

Le morphisme $\gamma$ défini dans la preuve de 3.1.1 est appelé **morphisme de groupes canoniquement associé** au $G$-ensemble $X$ ou à l'opération de $G$ sur $X$. Si ce morphisme est injectif, nous disons que l'opération de $G$ sur $X$ est **fidèle**. Nous disons aussi que $G$ opère **fidèlement** sur $X$. S'il en est ainsi, $G$ est isomorphe à un sous-groupe de $\mathfrak{S}(X)$.

Le groupe $G$ peut opérer sur lui-même de différentes manières. A titre d'exemple posons

$$g \cdot x = gx \quad \text{pour tout } (g, x) \in G^2.$$

Nous vérifions assez facilement que nous venons de définir une opération fidèle de $G$ sur lui-même, dite **opération par translation à gauche**. C'est une opération fondamentale. Le théorème de Cayley[1] est une première application de cette opération.

[1] *Arthur Cayley*, mathématicien anglais (1821-1895)

**Corollaire 3.1.2** (Théorème de Cayley) *Tout groupe $G$ est isomorphe à un sous-groupe de $\mathfrak{S}(G)$.*

**Démonstration.** Il suffit de considérer le morphisme de groupes canoniquement associé à l'opération fidèle de $G$ sur lui-même par translation à gauche. ■

Une autre opération de $G$ sur lui-même mérite d'être considérée. En effet, il est clair qu'en posant

$$g \cdot x = gxg^{-1} \quad \text{pour tout } (g,x) \in G^2,$$

nous obtenons une opération de $G$ sur lui-même, dite **opération par conjugaison** (ou par **automorphismes intérieurs**). Nous montrons aisément que l'action de $G$ sur lui-même par conjugaison est fidèle si, et seulement si, $\mathcal{Z}(G) = \{e\}$, où, rappelons le, $\mathcal{Z}(G)$ désigne le centre de $G$. Compte tenu de 2.1.2, si $n \in \mathbb{N}$ avec $n \geq 3$ alors l'opération de $\mathfrak{S}_n$ sur lui-même par conjugaison est fidèle.

Nous terminons ce paragraphe par une application géométrique. Il s'agit, pour commencer, de l'étude de l'ensemble des isométries du plan affine euclidien qui conservent un triangle équilatéral. A cet égard, supposons que $\mathbb{R}^2$ est muni de sa structure canonique de plan affine euclidien et considérons un triangle équilatéral $\Delta$ de $\mathbb{R}^2$ de sommets $A_1, A_2, A_3$. Notons $\mathcal{G}$ l'ensemble des isométries de $\mathbb{R}^2$ qui laissent globalement invariant $\Delta$. Nous observons aisément que $\mathcal{G}$ est un sous-groupe de $\mathfrak{S}(\mathbb{R}^2)$, appelé **groupe du triangle équilatéral**.

**Théorème 3.1.3** *Le groupe du triangle equilatéral est isomorphe à $\mathfrak{S}_3$.*

**Démonstration.** Puisque les isométries de $\mathbb{R}^2$ conservent les distances, une isométrie $f$ de $\mathbb{R}^2$ est dans $\mathcal{G}$ si, et seulement si, $f$ laisse globalement invariant le triplet $\{A_1, A_2, A_3\}$. De ce fait, nous pouvons faire opérer $\mathcal{G}$ sur $\{A_1, A_2, A_3\}$ en posant

$$f \cdot A_i = f(A_i) \qquad \text{pour tout } (f,i) \in \mathcal{G} \times \{1,2,3\}.$$

Cette opération est fidèle car $\mathrm{id}_{\mathbb{R}^2}$ est l'unique application affine de $\mathbb{R}^2$ qui conserve trois points non alignés de $\mathbb{R}^2$. Ainsi, $\mathcal{G}$ est isomorphe à un sous-groupe de $\mathfrak{S}(\{A_1, A_2, A_3\})$ et donc, d'après 2.1.1, à un sous-groupe de $\mathfrak{S}_3$. Le théorème de Lagrange assure que $\mathrm{o}(\mathcal{G})$ divise $\mathrm{o}(\mathfrak{S}_3) = 6$. Par conséquent, $\mathrm{o}(\mathcal{G}) \in \{1,2,3,6\}$. En outre, les rotations de centre $O$, l'isobarycentre de $\Delta$, et d'angles respectifs $2\pi/3$ et $4\pi/3$ sont manifestment des éléments de $\mathcal{G}$. De même, la réflexion d'axe la droite $OA_1$ est dans $\mathcal{G}$. Tenant compte de $\mathrm{id}_{\mathbb{R}^2}$, nous constatons que $\mathcal{G}$ contient au moins 4 éléments. Il vient que l'ordre de $\mathcal{G}$ est 6 et donc $\mathcal{G}$ est isomorphe à $\mathfrak{S}_3$. ■

Notons que le sous-groupe du groupe du triangle equilatéral formé par les rotations est ismorphe à $\mathfrak{A}_3$. Signalons enfin que 3.1.3 admet une version en

dimension $n \in \mathbb{N}$ avec $n \geq 3$. En effet, munissons $\mathbb{R}^n$ de sa structure affine euclidienne canonique et considérons $n+1$ points $A_1, ..., A_{n+1} \in \mathbb{R}^n$ tels que $A_iA_j = A_kA_\ell$ dès que $i, j, k, \ell \in \mathbb{N}_{n+1}$ et $i \neq j, k \neq \ell$. L'enveloppe convexe[2] $\Sigma$ des points $A_1, ..., A_{n+1}$ est appelé **symplexe régulier de degré** $n$ et les points $A_1, ..., A_n$ sont appelés **sommets** de $\Sigma$. Pour fixer les idées, le symplexe régulier de degré 3 est le tétraèdre régulier. Le **groupe du symplexe régulier de degré** $n$ est, par définition, le groupe des isométries de $\mathbb{R}^n$ qui laissent globalement invariant $\Sigma$. Une méthode analogue à celle employée pour établir 3.1.3 permet de prouver que le groupe du symplexe régulier de degré $n$ est isomorphe à $\mathfrak{S}_n$.

## 3.2 Equation aux classes

Soient $\langle\sigma\rangle$ le sous-groupe de $\mathfrak{S}(X)$ engendré par une permutation $\sigma$ de l'ensemble $X$. L'application définie de $\langle\sigma\rangle \times X$ vers $X$ par

$$\rho \cdot x = \rho(x) \quad \text{pour tout } (\rho, x) \in \langle\sigma\rangle \times X$$

est manifestement une opération de $\langle\sigma\rangle$ sur $X$. Observons que si $x \in X$ alors la partie de $X$ donnée par

$$\{\rho \cdot x : \rho \in \langle\sigma\rangle\}$$

est la $\sigma$-orbite de $x$. Dans cette section, nous nous proposons de généraliser la notion de $\sigma$-orbite à toute opération d'un groupe sur un ensemble.

Dans la suite, $X$ désigne un $G$-ensemble. Si $x \in X$ alors la partie

$$\Omega(x) = \{g \cdot x : g \in G\}$$

est appelée **orbite** de $x \in X$ **sous l'action** de $G$ sur $X$. Comme exemple, considérons $n \in \mathbb{N}^*$ et notons $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices carrées d'ordre $n$ et à coefficients dans un corps commutatif $\mathbb{K}$. En outre, désignons le groupe des matrices inversibles dans $\mathcal{M}_n(\mathbb{K})$ par $\mathcal{GL}_n(\mathbb{K})$. Grâce à l'application définie de $\mathcal{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K})$ vers $\mathcal{M}_n(\mathbb{K})$ par

$$P \cdot M = PMP^{-1} \quad \text{pour tout } (P, M) \in \mathcal{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}),$$

$\mathcal{M}_n(\mathbb{K})$ est un $\mathcal{GL}_n(\mathbb{K})$-ensemble. Il s'avère que l'orbite $\Omega(M)$ d'une matrice $M \in \mathcal{M}_n(\mathbb{K})$ sous cette action est l'ensemble des matrices de $\mathcal{M}_n(\mathbb{K})$ semblables à $M$. A propos, $\Omega(M)$ est dite **classe de semblabilité** de $M$.

Nous nous plaçons à nouveau dans le cadre général de notre étude.

[2] Une partie non vide $\mathcal{C}$ de $\mathbb{R}^n$ est **convexe** si, pour tout $(M, N) \in \mathcal{C}^2$ et pour tout $\mu \in [0, 1]$, le barycentre des points pondérés $(M, \mu)$ et $(N, 1-\mu)$ reste dans $\mathcal{C}$. L'**enveloppe convexe** de $A_1, ..., A_{n+1}$ est le plus petit (pour l'inclusion) convexe de $\mathbb{R}^n$ contenant $A_1, ..., A_{n+1}$.

**Théorème 3.2.1** *Soient $G$ un groupe et $X$ un $G$-ensemble. La relation binaire définie sur $X$ par*

$$x\mathcal{R}y \quad \textit{si, et seulement si,} \quad y \in \Omega(x)$$

*est une relation d'équivalence sur $X$. De plus, $\Omega(x)$ est la classe d'équivalence de $x \in X$ modulo $\mathcal{R}$.*

**Démonstration.** Soient $x, y, z \in X$. Comme $x = e \cdot x \in \Omega(x)$, la relation $\mathcal{R}$ est reflexive. De plus, si $y\mathcal{R}x$ alors $y \in \Omega(x)$. Il existe donc $g \in G$ tel que $y = g \cdot x$ et par suite $x = g^{-1} \cdot y \in \Omega(y)$. D'où $y\mathcal{R}x$ et $\mathcal{R}$ est ainsi symétrique. Enfin, si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors il existe $g, h \in G$ tels que $y = g \cdot x$ et $z = h \cdot y$. Par conséquent,

$$z = h \cdot g \cdot x = (hg) \cdot x \in \Omega(x).$$

Donc $x\mathcal{R}z$ et $\mathcal{R}$ est, par suite, transitive. Finalement, $\mathcal{R}$ est une relation d'équivalence. Le fait que $\Omega(x)$ est la classe d'équivalence de $x \in X$ modulo $\mathcal{R}$ est simple à établir. ■

Il s'en suit, en particulier, que les orbites sous l'action de $G$ sur $X$ forment une partition de $X$.

Pour tout $x \in X$, la partie

$$G(x) = \{g \in G : g \cdot x = x\}$$

de $G$ est appelée **stabilisateur** de $x$ **sous l'action** de $G$ sur $X$.

**Proposition 3.2.2** *Soient $G$ un groupe et $X$ un $G$-ensemble. Pour tout $x \in X$, $G(x)$ est un sous-groupe de $G$.*

**Démonstration.** Comme $e \cdot x = x$, $e \in G(x)$ et $G(x) \neq \emptyset$. Soient alors $g, h \in G(x)$. Alors

$$\begin{aligned}\left(gh^{-1}\right) \cdot x &= g \cdot \left(h^{-1} \cdot x\right) = g \cdot \left(h^{-1} \cdot (h \cdot x)\right) \\ &= g \cdot \left(\left(h^{-1}h\right) \cdot x\right) = g \cdot (e \cdot x) = g \cdot x = x.\end{aligned}$$

Ainsi $gh^{-1} \in G(x)$ et par suite $G(x)$ est un sous-groupe de $G$. ■

C'est pour cette rasion, que le stabilisateur d'un élément $x \in E$ est souvent appelé **sous-groupe d'isotropie** de $x$ **sous l'action** de $G$ sur $X$. Les stabilisateurs de deux éléments d'une même orbites sont conjugués[3].

**Proposition 3.2.3** *Soient $G$ un groupe, $X$ un $G$-ensemble et $x, y \in X$ tels que $\Omega(x) = \Omega(y)$. Alors $G(x)$ et $G(y)$ sont conjugués.*

[3]Deux sous-groupe $H$ et $K$ de $G$ sont dits **conjugués** s'il existe $g \in G$ tel que $H = gKg^{-1}$.

**Démonstration.** Puisque $y \in \Omega(y) = \Omega(x)$, il existe $g \in G$ tel que $y = g \cdot x$. Pour tout $h \in G(x)$, on a

$$\left(ghg^{-1}\right) \cdot y = (gh) \cdot \left(g^{-1} \cdot y\right) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = y.$$

Par conséquent, $gG(x)\, g^{-1} \subset G(y)$. Inversement, si $h \in G(y)$ alors

$$\left(g^{-1}hg\right) \cdot x = \left(g^{-1}h\right) \cdot (g \cdot x) = \left(g^{-1}h\right) \cdot y = g^{-1} \cdot (h \cdot y) = g^{-1} \cdot y = x.$$

Par suite, $g^{-1}hg \in G(x)$. Mais alors

$$y = g\left(g^{-1}hg\right) g^{-1} \in gG_x g^{-1},$$

soit,

$$G(y) = gG(x)\, g^{-1}$$

et $G(x)$ et $G(y)$ sont ainsi conjugués. ■

Rappelons que si $G$ est d'ordre fini alors $H$ est d'indice fini et $[G : H] = \mathrm{o}(G)/\mathrm{o}(H)$. Rappelons également que l'ensemble des classes à gauche modulo $H$ est noté $(G/H)_g$. Le théorème suivant est fondamental.

**Théorème 3.2.4** *Soient $G$ un groupe, $X$ un $G$-ensemble et $x \in X$. Alors $\Omega(x)$ et $(G/G(x))_g$ sont équipotents. En particulier, $\Omega(x)$ est fini si, et seulement si, $G(x)$ est d'indice fini dans $G$. Dans ce cas,*

$$\mathrm{card}\,(\Omega(x)) = [G : G(x)].$$

**Démonstration.** Considérons l'application $\varphi$ définie de $\Omega(x)$ vers $(G/G(x))_g$ par

$$\varphi(g \cdot x) = gG(x) \quad \text{pour tout } g \in G.$$

Soient $g, h \in G$ tels que $g \cdot x = h \cdot x$. Alors $(h^{-1}g) \cdot x = x$ et donc $h^{-1}g \in G(x)$. Il vient que $gG(x) = hG(x)$. Ceci montre que $\varphi$ est bien-définie. De plus, $\varphi$ est évidemment surjective. Finalement, soient $g, h \in G$ tels que $\varphi(g \cdot x) = \varphi(h \cdot x)$. Alors $gG(x) = hG(x)$ et donc $h^{-1}g \in G(x)$. Nous obtenons $(h^{-1}g) \cdot x = x$ et par suite $g \cdot x = h \cdot x$. Autrement dit, $\varphi$ est injective. En résumé, $\varphi$ est bijective et le théorème se trouve ainsi démontré. ■

Nous arrivons au résultat autour du quel s'articule cette section.

**Théorème 3.2.5** (Equations aux Classes) *Soient $G$ un groupe et $X$ un $G$-ensemble fini. Si $A$ est une partie de $X$ qui rencontre chaque orbite en un seul élément alors*

$$\mathrm{card}\,(X) = \sum_{x \in A} \mathrm{card}\,(\Omega(x)) = \sum_{x \in A} [G : G(x)].$$

**Démonstration.** Conséquence immédiate de 3.2.1 et 3.2.4. ■

Nous allons appliquer 3.2.5 à l'opération de $G$ sur lui-même par conjugaison.

**Corollaire 3.2.6** *Soit $G$ un groupe fini. Si $\mathcal{B}$ est une partie de $G\backslash\mathcal{Z}(G)$ contenant un et un seul élément de chaque orbite sous l'action de $G$ sur lui-même par conjugaison alors*

$$\mathrm{o}(G) = \mathrm{o}(\mathcal{Z}(G)) + \sum_{x\in B} \mathrm{card}(\Omega(x)),$$

*où $\Omega(x)$ désigne l'orbite de $x \in G$ sous l'action de $G$ sur lui-même par conjugaison.*

**Démonstration.** Nous faisons opérer $G$ sur lui-même par conjugaison et nous appliquons 3.2.5 pour avoir

$$\begin{aligned}\mathrm{o}(G) &= \mathrm{card}(G) = \sum_{x\in A} \mathrm{card}(\Omega(x)) \\ &= \sum_{x\in A\cap\mathcal{Z}(G)} \mathrm{card}(\Omega(x)) + \sum_{x\in A\cap(G\backslash\mathcal{Z}(G))} \mathrm{card}(\Omega(x)),\end{aligned}$$

où $A$ est une partie de $G$ qui ne contient qu'un élément et un seul de chaque orbite. Observons que si $x \in G$ alors $x \in \mathcal{Z}(G)$ si, et seulement si, $\Omega(x) = \{x\}$. Ainsi, $A \cap \mathcal{Z}(G) = \mathcal{Z}(G)$ . En posant $B = A \cap (G\backslash\mathcal{Z}(G))$, nous obtenons

$$\begin{aligned}\mathrm{o}(G) &= \sum_{x\in A\cap\mathcal{Z}(G)} \mathrm{card}(\Omega(x)) + \sum_{x\in A\cap(G\backslash\mathcal{Z}(G))} \mathrm{card}(\Omega(x)) \\ &= \sum_{x\in\mathcal{Z}(G)} \mathrm{card}(\{x\}) + \sum_{x\in B} \mathrm{card}(\Omega(x)) = \mathrm{o}(\mathcal{Z}(G)) + \sum_{x\in B} \mathrm{card}(\Omega(x)).\end{aligned}$$

Ce qu'il fallait démontrer. ■

La formule obtenue dans 3.2.6 admet plusieurs applications, à l'image du théorème de Burnside[4] sur les $p$-groupe. A ce propos, un $p$-**groupe** est un groupe fini dont l'ordre est une puissance non nulle de $p$. A titre d'exemples, $\mathbb{Z}/5\mathbb{Z}$ est un 5-groupe, $\mathbb{Z}/9\mathbb{Z}$ est un 3-groupe, $\mu_8$ est un 2-groupe mais $\mu_6$ n'est pas un $p$-groupe.

**Théorème 3.2.7** (Théorème de Burnside) *Le centre d'un $p$-groupe n'est jamais réduit à l'élément neutre.*

**Démonstration.** Soient $m \in \mathbb{N}^*$ et $G$ un groupe d'ordre $p^m$. Si $G$ opère sur lui-même par conjugaison alors, d'après 3.2.6,

$$p^m = \mathrm{o}(G) = \mathrm{o}(\mathcal{Z}(G)) + \sum_{x\in B} \mathrm{card}(\Omega(x)).$$

[4] *William Snow Burnside*, mathématicien irlandais (1852-1921)

Si $x \notin \mathcal{Z}(G)$ alors $\mathrm{card}(\Omega(x)) \geq 2$. De plus, 3.2.4 montre que, pour $x \in G$, $\mathrm{card}(\Omega(x))$ divise l'ordre de $G$ et donc $p$ divise $\mathrm{card}(\Omega(x))$. Par suite, il existe $\ell \in \mathbb{N}$ tel que

$$p^m = \mathrm{o}(\mathcal{Z}(G)) + p\ell.$$

Par conséquent, $p$ divise $\mathrm{o}(\mathcal{Z}(G))$ et $\mathcal{Z}(G)$ ne peut donc pas être réduit à l'élément neutre. ■

## 3.3 Théorèmes de Sylow

Dans cette section, le groupe $G$ est supposé fini. D'après le théorème de Lagrange, l'ordre d'un sous groupe de $G$ divise $\mathrm{o}(G)$. Que peut-on dire de la réciproque ? Autrement dit, existe-t-il, pour tout diviseur $d$ de $\mathrm{o}(G)$, un sous-groupe de $G$ d'ordre $d$? En général, la réponse à cette question est négative. En effet, le groupe alterné $\mathfrak{A}_4$ est d'ordre 12 mais ne contient aucun sous-groupe d'ordre 6 (voir 2.4.9). Cependant, la situation est toute autre si le diviseur en question est une puissance d'un nombre premier $p$. C'est ce que nous allons voir dans la suite de cette section.

Dans tout ce qui suit, $p$ désigne un nombre premier qui dévise $\mathrm{o}(G)$.

**Lemme 3.3.1** *Soient $G$ un groupe abélien fini et $p$ un nombre premier diviseur de $\mathrm{o}(G)$. Alors il existe $g \in G$ d'ordre $p$.*

**Démonstration.** Nous procédons par récurrence sur $\mathrm{o}(G)$. Le résultat étant évident si $\mathrm{o}(G) = 2$, nous supposons que $\mathrm{o}(G) > 2$ et que le résultat est vrai pour n'importe quel groupe d'ordre strictement inférieur à celui de $G$.

Commeçons par le cas où les seuls sous-groupes de $G$ sont les sous-groupes triviaux. Soit $g \in G$ tel que $g \neq e$. Alors le sous-groupe $\langle g \rangle$ de $G$ engendré par $g$ est égal à $G$ tout entier. Autrement dit, $g$ est d'ordre $\mathrm{o}(G)$ et par suite $g^{\mathrm{o}(G)/p}$ est d'ordre $p$.

A présent, nous traîtons le cas où $G$ admet un sous-groupe non trivial $H$ dont l'ordre est un multiple de $p$. Dans ce cas, $\mathrm{o}(H) < \mathrm{o}(G)$. Donc, l'hypothèse de récurrence assure que $H$ admet un élément d'ordre $p$ qui est également d'ordre $p$ dans $G$.

Il nous reste à envisager le cas où $G$ possède des sous-groupes non triviaux et $p$ ne divise aucun des ordres de ces sous-groupes. Soit $H$ un sous-groupe non trivial de $G$. Comme $G$ est abélien, $H$ est distingué dans $G$. Nous pouvons alors considérer le groupe quotient $G/H$. Puisque $H \neq \{e\}$, $\mathrm{o}(G/H) < \mathrm{o}(G)$. De plus, $\mathrm{o}(G) = \mathrm{o}(H)\,\mathrm{o}(G/H)$ et $p$ est premier avec $\mathrm{o}(H)$. Le théorème de Gauss prouve alors que $p$ divise $\mathrm{o}(G/H)$. Nous pouvons donc appliquer l'hypothèse de récurrence à $G/H$. Il existe alors $g \in G$ tel que $\mathrm{o}(gH) = p$ dans $G/H$. Par suite, $gH \neq H$ et $g^p H = H$. Il vient que $g \notin H$ et $g^p \in H$. En posant $f = g^{\mathrm{o}(H)}$, nous obtenons

$$f^p = g^{p\mathrm{o}(H)} = (g^p)^{\mathrm{o}(H)} = e.$$

Si $f = e$ alors $(gH)^{o(H)} = H$ dans $G/H$. Or, $(gH)^p = H$ dans $G/H$ et par conséquent $gH = H$. Contradiction. Ainsi, $f \neq e$ et l'élément $f$ répond à la question. ■

Le lemme précédent sert surtout à établir le théorème fondamental suivant.

**Théorème 3.3.2** *Soient $G$ un groupe fini, $p$ un nombre premier diviseur et $m \in \mathbb{N}^*$ tels que $p^m$ divise $o(G)$. Alors, $G$ admet un sous-groupe d'ordre $p^m$.*

**Démonstration.** Nous raisonnons par récurrence sur $o(G)$. Pour le cas où $o(G) = 2$, il n'y a rien à démontrer. Supposons alors que $o(G) > 2$ et que le résultat est vrai pour tous les groupes d'ordres strictement inférieurs à $o(G)$. Faisons opérer $G$ sur lui-même par conjugaison.

Commençons par le cas où il existe $x \in G \backslash \mathcal{Z}(G)$ tel que $p$ ne divise pas $\text{card}(\Omega(x))$. D'après 3.2.4, $G(x)$ est un sous-groupe non trivial de $G$. De plus, $p^m$ divise $o(G(x))$. Ainsi, l'hypothèse de récurrence permet de conclure.

Considérons alors le cas où $p$ divise $\text{card}(\Omega(x))$ pour tout $x \in G \backslash \mathcal{Z}(G)$. En utilisant 3.2.7, nous pouvons voir que $p$ divise $o(\mathcal{Z}(G))$. Comme $\mathcal{Z}(G)$ est abélien, 3.3.1 entraîne l'existence de $x \in \mathcal{Z}(G)$ d'ordre $p$. Le sous-groupe $H = \langle x \rangle$ est distingué dans $G$ car contenu dans $\mathcal{Z}(G)$. Comme $o(H) = p$ et $p^m$ divise $o(G)$, $p^{m-1}$ divise $G/H$. L'hypothèse de récurrence appliquée à $G/H$ et à $p^{m-1}$ assure l'existence d'un sous-groupe $\widetilde{K}$ de $G/H$ d'ordre $p^{m-1}$. Notons $\varphi$ la surjection canonique de $G$ sur $G/H$ et $K = \varphi^{-1}\left(\widetilde{K}\right)$, qui est un sous-groupe de $G$. Il est clair que $H$ est contenu dans $K$. La restriction de $\varphi$ à $K$ est un morphisme de groupes surjectif de $K$ sur $\widetilde{K}$ dont le noyau est $H$. Par suite, $K/H$ est isomorphe à $\widetilde{K}$. Finalement, $K$ est un sous-groupe de $G$ d'ordre $p^m$. Ceci achève la démonstration du théorème. ■

Rappelons qu'un $p$-groupe est un groupe dont l'ordre est une puissance de $p$. Si un sous-groupe $H$ de $G$ est un $p$-groupe alors $H$ est dit $p$-**sous-groupe** de $G$.

Le corollaire suivante se déduit directement de 3.3.2.

**Corollaire 3.3.3** *Soit $p$ un nombre premier. Si $m \in \mathbb{N}^*$ et $G$ est un $p$-groupe d'ordre $p^m$ alors, $G$ admet un sous-groupe d'ordre $p^\ell$ pour tout $\ell \in \{1, ..., m\}$.*

Un $p$-sous-groupe $H$ de $G$ est appelé $p$-**sous-groupe de Sylow**[5] (ou, simplement, un $p$-**Sylow**) si $p \wedge [G : H] = 1$. En d'autre termes, si $o(G)$ est de la forme $\ell p^m$ avec $\ell \wedge p = 1$ alors $H$ est un $p$-Sylow de $G$ si, et seulement si, $o(H) = p^m$. L'ordre d'un $p$-Sylow de $G$ est donc la plus grande puissance de $p$ divisant $o(G)$. L'ensemble des $p$-Sylow de $G$ est noté $\mathcal{S}(p)$.

Le résultat suivant découle également de 3.3.2.

**Théorème 3.3.4** (Premier Théorème de Sylow) *Soient $G$ un groupe fini et $p$ un nombre premier diviseur de $o(G)$. Alors $\mathcal{S}(p)$ n'est pas vide.*

[5] *Peter Ludwig Mejdell Sylow*, mathématicien norvégien (1832-1918).

Si $G$ est un $p$-groupe alors $\mathcal{S}(p) = \{G\}$. Dans $\mu_6$, le sous-groupe cyclique engendré par $\exp(2\pi i/3)$ est un 3-Sylow. Le sous-groupe cyclique de $\mathbb{Z}/10\mathbb{Z}$, engendré par la classe de 5, est un 2-Sylow.

Une partie $\mathcal{R}(p)$ de $\mathcal{S}(p)$ est dite **stable par conjugaison** si $gRg^{-1} \in \mathcal{R}(p)$ pour tout $R \in \mathcal{R}(p)$.

**Proposition 3.3.5** *Soient $G$ un groupe fini et $p$ un nombre premier diviseur de $\mathrm{o}(G)$.*

(**i**) *$\mathcal{S}(p)$ est stable par conjugaison.*

(**ii**) *Si $H$ est un sous-groupe de $G$ et $\mathcal{R}(p)$ est une partie non vide de $\mathcal{S}(p)$ stable par conjugaison alors $H$ opère sur $\mathcal{R}(p)$ par*

$$h \cdot S = hSh^{-1} \quad \textit{pour tout } (h, S) \in H \times \mathcal{R}(p).$$

**Démonstration.** (**i**) Soient $S \in \mathcal{S}(p)$ et $g \in G$. L'application $\gamma_g$ définie de $S$ vers $gSg^{-1}$ par

$$\gamma_g(x) = gxg^{-1} \quad \text{pour tout } x \in H$$

est manifestment un isomorphisme de groupes. Il vient que $gSg^{-1} \in \mathcal{S}(p)$ et le problème est résolu.

(**ii**) L'application est bien définie car $\mathcal{R}(p)$ est stable par conjugaison. De plus, si $h, k \in H$ et $S \in \mathcal{R}(p)$ alors

$$e \cdot S = eSe^{-1} = S \text{ et } h \cdot (k \cdot S) = h\left(kSk^{-1}\right)h^{-1} = (hk)S(hk)^{-1} = (hk) \cdot S.$$

D'où le résultat. ■

L'opération de $H$ sur $\mathcal{R}(p)$ définie dans 3.3.5 est dite **opération par conjugaison** de $H$ sur $\mathcal{R}(p)$

Dans tout ce qui suit, nous faisons opérer $G$ sur $\mathcal{S}(p)$ par conjugaison. A cet effet, l'orbite de $S \in \mathcal{S}$ sous cette opération est notée $\mathcal{O}(S)$ et son stablisateur est noté $\mathcal{G}(S)$. Donc

$$\mathcal{O}(S) = \left\{gSg^{-1} : g \in G\right\} \quad \text{et} \quad \mathcal{G}(S) = \left\{g \in G : gSg^{-1} = S\right\}.$$

Nous gardons cette notation jusqu'à la fin du chapitre.

**Lemme 3.3.6** *Soient $G$ un groupe fini, $p$ un nombre premier diviseur de $\mathrm{o}(G)$, $H$ un $p$-sous-groupe de $G$ et $S \in \mathcal{S}(p)$. Alors $H \subset S$ si, et seulement si, $H \subset \mathcal{G}(S)$.*

**Démonstration.** Le fait que si $H \subset S$ alors $H \subset \mathcal{G}(S)$ ne pose aucun problème car $S \subset \mathcal{G}(S)$. Inversement, supposons que $H \subset \mathcal{G}(S)$. Comme $S$ est distingué dans $\mathcal{G}(S)$, le produit

$$HS = \{hg : h \in H, g \in S\}$$

est un sous-groupe de $\mathcal{G}(S)$. Le troisième théorème d'isomorphismes[6] entraîne que le groupe quotient $H/H \cap S$ est isomorphe au groupe quotient $HS/S$. En particulier, $\mathrm{o}(H/H \cap S) = \mathrm{o}(HS/S)$. Mais $\mathrm{o}(H/H \cap S)$ divise $\mathrm{o}(H)$ et est ainsi une puissance de $p$. Donc il en est de même pour $\mathrm{o}(HS/S)$ et à fortiori de $\mathrm{o}(HS)$. Par conséquent, $HS$ est $p$-sous-groupe de $G$ contenant $S$ qui est un $p$-Sylow. Ainsi $HS = S$ et $H$ est contenu dans $S$. Ce qu'il fallait démontrer. ■

Nous sommes maintenant en mesure d'établir le deuxième théorème de Sylow.

**Théorème 3.3.7** (Deuxième théorème de Sylow) *Soient $G$ un groupe fini et $p$ un nombre premier diviseur de $\mathrm{o}(G)$. Si $H$ un $p$-sous-groupe de $G$ et $S \in \mathcal{S}(p)$ alors, il existe $R \in \mathcal{O}(S)$ tel que $H \subset R$. En particulier, tout $p$-sous-groupe de $G$ est contenu dans un $p$-Sylow.*

**Démonstration.** Comme $S \subset \mathcal{G}(S)$, le théorème de Lagrange assure que $\mathrm{o}(S)$ divise $\mathrm{o}(\mathcal{G}(S))$. Autrement dit, $[G : \mathcal{G}(S)]$ divise $[G : S]$. Puisque $[G : S] \wedge p = 1$, il vient

$$\mathrm{card}(\mathcal{O}(S)) \wedge p = [G : \mathcal{G}(S)] \wedge p = 1.$$

D'après 3.3.5, nous pouvons faire agir $H$ sur $\mathcal{O}(S)$ par conjugaison. Les orbites sous cette action sont toutes de cardinaux divisant $\mathrm{o}(H)$, donc des puissances de $p$. Mais comme $\mathrm{card}(\mathcal{O}(S))$ n'est pas divisible par $p$ et que les l'orbite sous l'action de $H$ sur $\mathcal{O}(S)$ forment une partition de $\mathcal{O}(S)$, il existe au moins une orbite de $\mathcal{O}(S)$ dont le cardinal est premier avec $p$. Une telle orbite est manifestement réduite à un singleton. Il s'en suit qu'il existe $g \in G$ tel que

$$hgS(hg)^{-1} = gSg^{-1} \quad \text{pour tout } h \in H.$$

Ceci montre que $H \subset \mathcal{G}(gSg^{-1})$ et donc, compte tenu de 3.3.5, 3.3.6 et du fait que $gSg^{-1} \in \mathcal{S}(p)$, $H \subset gSg^{-1}$. Ceci achève la démonstration du théorème. ■

Nous avons vu dans 3.3.5 qu'un conjugué d'un $p$-sous-groupe de Sylow est à son tour un $p$-sous-groupe de Sylow. La réciproque de ce résultat est également vraie comme le montre le corollaire suivant.

**Corollaire 3.3.8** *Soient $G$ un groupe fini, $p$ un nombre premier diviseur de $\mathrm{o}(G)$ et $S \in \mathcal{S}(p)$.*

- **(i)** *Si $H$ est un sous-groupe de $G$ alors $H \in \mathcal{S}(p)$ si, et seulement si, $H$ et $S$ sont conjugués.*
- **(ii)** *Deux $p$-Sylows de $G$ sont conjugués.*
- **(iii)** *$S$ est l'unique $p$-Sylow de $G$ si, et seulement si, $S$ est distingué dans $G$.*

[6] Troisième théorème d'isomorphismes : *Si $H$ et $K$ sont deux sous-groupes d'un groupe $G$ avec $H$ distingué dans $G$ alors les deux groupes quotients $K/H \cap K$ et $HK/H$ existent et sont isomorphes.*

**Démonstration.** (**i**) Si $H$ et $S$ sont conjugués alors $H \in \mathcal{S}(p)$ et ce grâce à 3.3.5. Inversement, si $H \in \mathcal{S}(p)$ alors $H$ est un $p$-sous-groupe de $G$ et donc il existe, d'après 3.3.7, $g \in G$ tel que $H \subset gSg^{-1}$. Comme $H$ et $gSg^{-1}$ ont même ordre (ce sont deux $p$-Sylows de $G$), nous obtenons $H = gSg^{-1}$ et $H$ et $S$ sont donc conjugués.

(**ii**) Si $H$ et $K$ sont deux $p$-Sylows de $G$ alors ils sont conjugués à $S$ et donc conjugués entre eux.

(**iii**) Si $\mathcal{S}(p) = \{S\}$ alors, d'après 3.3.5,

$$gSg^{-1} \in \mathcal{S}(p) = \{S\} \quad \text{pour tout } g \in G.$$

Il vient que

$$gSg^{-1} = S \quad \text{pour tout } g \in G$$

et donc $S$ est distingué dans $G$. Inversement, si $S$ est distingué dans $G$ et si $H \in \mathcal{S}(p)$, d'après (**ii**), $H$ et $S$ sont conjugués. Il existe alors $g \in G$ tel que

$$H = gSg^{-1} = S.$$

D'où $S(p) = \{S\}$. Ce qu'il fallait démontrer. ■

Le troisième théorème de Sylow présente des informations sur le nombre des $p$-Sylows de $G$.

**Théorème 3.3.9** (troisième théorème de Sylow) $\operatorname{card}(\mathcal{S}(p)) \equiv 1 \pmod{p}$ *et* $\operatorname{card}(\mathcal{S}(p))$ *divise* $[G : S]$ *pour tout* $S \in \mathcal{S}$.

**Démonstration.** Montrons la première égalité. Soient $S \in \mathcal{S}(p)$ et $\Omega(S)$ l'orbite de $S$ sous l'action de $S$ sur $\mathcal{S}$ par conjugaison. Il est clair que $\Omega(S) = \{S\}$. Si $R \in \mathcal{S} - \{S\}$ alors l'orbite de $R$ n'est pas réduite à un singleton. En effet, sinon, nous aurons

$$gRg^{-1} = R \quad \text{pour tout } g \in S.$$

Par suite, $S \subset \mathcal{G}(R)$ et donc, d'après 3.3.6, $S \subset R$. Par conséquent, $S = R$. L'orbite de $R \in \mathcal{S}(p) \setminus \{S\}$ est donc de cardinal divisible par $p$ puisque c'est un diviseur non trivial de $\mathrm{o}(S)$. L'équation aux classes établie dans 3.2.5 permet de conclure que $p$ divise $\operatorname{card}(\mathcal{S}(p)) - 1$. En outre, 3.3.8 montre que $\mathcal{S}$ est l'unique orbite de l'action de $S$ sur $\mathcal{S}$ par conjugaison. Ce qui prouve que $\operatorname{card}(\mathcal{S}(p))$ divise $[G : S]$ (et donc $\mathrm{o}(G)$). ■

A titre d'exemples, un groupe d'ordre 15 admet un seul 3-Sylow et un seul 5-Sylow qui est donc disitngué.

## 3.4 Exercices

**Exercice 3.4.1** Soient $G$ et $H$ deux groupes et $\varphi$ un morphisme de groupes de $G$ vers $H$. En faisant opérer $G$ sur $\operatorname{Im}(\varphi)$ retrouver la formule

$$\mathrm{o}(G) = \mathrm{o}(\ker(\varphi)) \times \mathrm{o}(\operatorname{Im}(\varphi)),$$

déjà obtenue comme corollaire du théorème d'isomorphisme.

**Exercice 3.4.2** Soient $\mathcal{C}$ un cube dans l'espace affine euclidien $\mathbb{R}^3$ et $G$ l'ensemble des déplacements de $\mathbb{R}^3$ qui laissent globalement invariant $\mathcal{C}$.

(**1**) Montrer que $\mathcal{C}$ est un groupe pour la composition des applications.

(**2**) Vérifier que si $\Delta$ est une diagonale de $\mathcal{C}$ et $g \in G$ alors $g(\Delta) = \{g(M) : M \in \Delta\}$ est une diagonale de $\mathcal{C}$.

(**3**) En déduire que l'on peut faire opérer $G$ sur $X$, l'ensemble des diagonales de $\mathcal{C}$, en posant

$$g \cdot \Delta = g(\Delta) \quad \text{pour tout } (g, \Delta) \in G \times X.$$

(**4**) Montrer que $G$ est isomorphe à $\mathfrak{S}_4$.

**Exercice 3.4.3** Montrer que si $p$ est un nombre premier qui divise l'ordre d'un groupe $G$ alors $G$ contient un élément d'ordre $p$.

**Exercice 3.4.4** Soit $p$ un nombre premier et $G$ un groupe d'ordre $p^2$.

(**1**) Montrer que $G$ est abélien.

(**2**) En déduire que $G$ est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou au groupe produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

**Exercice 3.4.5** Dans cette exercice, $G$ désigne un groupe fini non abélien et $p$ désigne un nombre premier.

(**1**) Montrer que si $\mathrm{o}(G)$ est une puissance de $p$ alors $G$ n'est pas simple[7].

(**2**) En déduire que si $G$ est simple et si $p$ divise $\mathrm{o}(G)$ alors $G$ admet au moins deux $p$-Sylows.

**Exercice 3.4.6** Soient $p$ et $q$ deux nombres premiers distincts et $G$ un groupe fini d'ordre $pq$.

(**1**) Montrer que si $p$ ne divise pas $q-1$ alors $G$ admet un unique $p$-sous-groupe de Sylow.

(**2**) En déduire que $G$ n'est pas simple.

(**3**) Prouver que si $p$ ne divise pas $q-1$ et si $q$ ne divise pas $p-1$ alors $G$ est cyclique.

(**4**) Que peut-on dire d'un groupe d'ordre 35 ?

[7] Un groupe $G$ est dit **simple** si les seuls sous-groupes distingués de $G$ sont $G$ et $\{e\}$, où $e$ désigne l'élément neutre de $G$.

**Exercice 3.4.7** Soit $G$ un groupe fini non réduit à son élément neutre tel qu'il existe $m_1, m_2, ..., m_n, p_1, p_2, ..., p_n \in N^*$ vérifiant $p_1, p_2, ..., p_2$ sont premiers deux à deux distincts et $\mathrm{o}(G) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$.

(**1**) Montrer que si, pour tout $k \in \{1, 2, ..., n\}$, $G$ admet un unique $p_k$-Sylow $S_k$ alors $G$ est isomorphe au groupe produit $S_1 \times S_2 \times \cdots \times S_n$.

(**2**) En déduire que si $G$ est abélien alors $G$ est isomorphe au groupe produit de tous ses sous-groupes de Sylow.

**Exercice 3.4.8** Soient $G$ un groupe d'ordre 48 et $\mathcal{S}(2)$ l'ensemble des 2-Sylows de $G$.

(**1**) Montrer que $\mathcal{S}(2)$ n'est pas vide et que $\mathrm{card}(\mathcal{S}(2)) \in \{1, 3\}$.

(**2**) Vérifier que $G$ n'est pas simple dans le cas où $\mathrm{card}(\mathcal{S}(2)) = 1$.

Dans la suite, on suppose que $\mathrm{card}(\mathcal{S}(2)) = 3$ et on pose $\mathcal{S}(2) = \{S_1, S_2, S_3\}$.

(**3**) Montrer que $G$ opère fidèlement sur $\mathcal{S}(2)$ en posant

$$g \cdot S_k = g S_k g^{-1} \quad \text{pour tout } (g, k) \in G \times \{1, 2, 3\}.$$

(**4**) En déduire que $G$ n'est pas simple.

**Exercice 3.4.9** Soient $G$ un groupe et $p$ est un nombre premier. Montrer que $G$ est un $p$-groupe si, et seulement si, l'ordre de tout élément de $G$ est une puissance de $p$.

# Chapitre 4

# Solutions des exercices

## 4.1 Groupes monogènes

**Solution 4.1.1** (Exercice 1.4.1)

(**1**) *Supposons que* $(\mathbb{Q},+)$ *est monogène. Choisissons dans ce cas un générateur* $m/n$ *de* $(\mathbb{Q},+)$*. Il est clair que nous pouvons supposer que* $m,n\in\mathbb{N}^*$*. Ainsi, il existe* $\ell\in\mathbb{Z}$ *tel que*

$$\frac{m}{2n}=\ell\frac{m}{n}$$

*et donc* $1/2=\ell\in\mathbb{Z}$*. Absurde.*

(**2**) *Comme* $(\mathbb{Q},+)$ *est un sous-groupe de* $(\mathbb{R},+)$ *et* $(\mathbb{Q},+)$ *n'est pas monogène,* $(\mathbb{R},+)$ *ne peut pas être monogène* (*voir* 1.2.1).

(**3**) *Soit* $H$ *un sous-groupe monogène de* $(\mathbb{Q},+)$*. Supposons que* $H$ *est cyclique d'ordre* $\ell>0$*. Quitte à considérer l'opposé, nous pouvons affirmer qu'il existe* $m,n\in\mathbb{N}^*$ *tel que*

$$H=\left\{0,\frac{m}{n},2\frac{m}{n},...,(\ell-1)\frac{m}{n}\right\}.$$

*Or,* $\ell m/n\in H$*. Contradiction. Ainsi* $H$ *est infini.*

*Il est à signaler que les résultats de cet exercice découlent directement d'un résultat classique, à savoir, les sous-groupes non nuls de* $(\mathbb{R},+)$ *sont ou bien isomorphes à* $\mathbb{Z}$ *ou denses dans* $\mathbb{R}$ *pour la topologie usuelle.*

**Solution 4.1.2** (Exercice 1.4.2) *Le groupe* $G=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ *n'est pas cyclique. En effet, il est d'ordre* 4 *et tous ses éléments autres que l'élément neutre sont d'ordre* 2*. Cependant, si* $H$ *est un sous-groupe propre de* $G$ *alors, d'après le théorème de Lagrange,* $\mathrm{o}(H)\in\{1,2\}$ *et dont* $H$ *est obligatoirement cyclique* (*voir par exemple* 1.1.5)*. Ainsi,* $G$ *est un exemple d'un groupe non cyclique dont tous les sous-groupes propres sont cycliques.*

**Solution 4.1.3** (Exercice 1.4.3) *L'objectif de cet exercice est de fournir une autre démonstartion de* 3.3.1.

(**1**) *Le résultat étant trivial pour* $\mathrm{o}(G) = 1$, *supposons que* $\mathrm{o}(G) \geq 2$ *et que le résultat est vrai dans n'importe quel groupe d'ordre inférieur ou égal à* $\mathrm{o}(G)$. *Commençons par un premier cas, à savoir,* $G = \langle g \rangle$ *pour tout* $g \in G \backslash \{e\}$. *Dans ce cas,* $G$ *est cyclique et* $\mathrm{o}(G)$ *est premier* (*voir* 1.1.5). *Considérons* $g \in G \backslash \{e\}$. *Alors* $\mathrm{o}(g)$ *divise* $m$ *car* $g^m = e$. *Mais* $o(g) = \mathrm{o}(G)$ *et le problème est donc résolu. Passons au deuxième cas en supposant l'existence d'un élément* $h \in G \backslash \{e\}$ *tel que* $1 < \mathrm{o}(h) < \mathrm{o}(G)$. *Posons* $H = \langle h \rangle$ *et observons que, comme* $G$ *est abélien,* $H$ *est distingué dans* $G$. *Nous pouvons affirmer que* $\mathrm{o}(G/H) < \mathrm{o}(G)$. *Par ailleurs, puisque* $g^n = e$ *pour tout* $g \in G$, *l'égalité* $(gH)^n = H$ *est vérifiée dans* $G/H$ *pour tout* $g \in G$. *Nous pouvons ainsi appliquer l'hypothèse de récurrence à* $G/H$. *Nous en déduisons que* $\mathrm{o}(G/H)$ *est une puissance de* $m$. *Or,* $\mathrm{o}(H) = \mathrm{o}(h)$ *et donc, comme* $h^m = e$, $\mathrm{o}(H)$ *divise* $m$. *Il en résulte que* $\mathrm{o}(G)$ *divise une puissance de* $m$.

(**2**) *Posons*

$$G = \left\{g_1, ..., g_{\mathrm{o}(G)}\right\} \quad et \quad m = \mathrm{o}(g_1)\,\mathrm{o}(g_2) \cdots \mathrm{o}\left(g_{\mathrm{o}(G)}\right).$$

*Il est clair que* $g^m = e$ *pour tout* $g \in G$. *D'après* (**1**), *il existe* $\ell \in \mathbb{N}^*$ *tel que* $o(G)$ *divise* $m^\ell$ *et donc* $p$ *divise* $m^\ell$. *Le théorème de Gauss prouve qu'il existe* $i \in \{1, 2, ..., \mathrm{o}(G)\}$ *tel que* $p$ *divise* $\mathrm{o}(g_i)$. *Notons* $h = g_i^{\mathrm{o}(g_i)/p}$ *et observons que* $\mathrm{o}(h) = p$.

(**3**) *D'après* (**2**), *pour tout* $i \in \{1, 2, ..., n\}$, *il existe* $g_i \in G$ *tel que* $\mathrm{o}(g_i) = p_i$. *Posons* $g = g_1 g_2 \cdots g_n$ *et observons que*

$$\mathrm{o}(g) = \mathrm{ppcm}\left(\mathrm{o}(g_1), \mathrm{o}(g_2), ..., \mathrm{o}(g_n)\right) = p_1 p_2 \cdots p_n = \mathrm{o}(G).$$

*Ceci montre que* $G$ *est cyclique.*

**Solution 4.1.4** (Exercice 1.4.4) *Rappelons d'abord que* $\mathcal{Z}(G)$ *est distingué dans* $G$.

(**1**) *Soit* $f, g, h \in G$ *et supposons que* $f\mathcal{Z}(G)$ *engendre* $G/\mathcal{Z}(G)$. *Ainsi, il existe* $m, n \in \mathbb{N}$ *tels que*

$$g\mathcal{Z}(G) = f^m\mathcal{Z}(G) \quad et \quad h\mathcal{Z}(G) = f^n\mathcal{Z}(G).$$

*Il existe alors* $u, v \in \mathcal{Z}(G)$ *tels que* $g = f^m u$ *et* $h = f^m v$. *Ainsi*

$$gh = f^m u f^n v = f^m f^n uv = f^{m+n} vu = f^n f^m vu = f^n v f^m u = hg.$$

*Il vient que* $G$ *est abélien.*

(**2**) *Supposons que* $[G : \mathcal{Z}(G)]$ *est premier. En particulier,* $[G : \mathcal{Z}(G)] \neq 1$. *Par ailleurs, comme* $\mathrm{o}(G/\mathcal{Z}(G)) = [G : \mathcal{Z}(G)]$, *le groupe* $G/\mathcal{Z}(G)$ *est cyclique* (*voir* 1.1.5). *D'après* (**1**), $G$ *est abélien et donc* $G = \mathcal{Z}(G)$, *soit,* $[G : \mathcal{Z}(G)] = 1$. *Contradicition.*

**Solution 4.1.5** (Exercice 1.4.5) *Pour* $n \in \mathbb{N}^*$, $\varphi(n)$ *indique la valeur de la fonction indicatrice d'Euler en* $n$.

(**1**) *C'est une question simple, bien qu'il ne faut pas oublier de vérifier que la* $\times$ *est bien-définie sur* $\mathbb{Z}/n\mathbb{Z}$, *c'est-dire-dire, le produit* $\overline{\ell} \times \overline{m}$ *ne dépend que de* $\overline{\ell}$ *et* $\overline{m}$ *et non de leurs représentants respectifs* $\ell$ *et* $m$.

(**2**) *Supposons que* $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^*$. *Il existe alors* $\ell \in \mathbb{Z}$ *tel que*

$$\overline{\ell} \times \overline{m} = \overline{\ell m} = \overline{1} \quad \textit{dans } \mathbb{Z}/n\mathbb{Z}.$$

*Ainsi,* $n$ *divise* $1 - \ell m$ *et donc il existe* $u \in \mathbb{Z}$ *tel que* $1 = \ell m + un$. *Le théorème de Bezout permet de dire que* $m$ *et* $n$ *sont premiers entre eux. Réciproquement, si* $m$ *et* $n$ *sont premiers entre eux alors il existe* (*encore d'après le théorème de Bezout*) $u, v \in \mathbb{Z}$ *tels que* $um + vn = 1$. *Par suite,*

$$\overline{um} = \overline{u} \times \overline{m} = \overline{1} \quad \textit{dans } \mathbb{Z}/n\mathbb{Z}$$

*et donc* $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^*$. *Compte tenu de* 1.3.1, *il vient en particulier que* $\mathrm{o}\left((\mathbb{Z}/n\mathbb{Z})^*\right) = \varphi(n)$

(**3**) *Le théorème de Lagrange assure donc que si* $m$ *et* $n$ *sont premiers entre eux alors* $\overline{m}^{\varphi(n)} = \overline{1}$ *dans* $\mathbb{Z}/n\mathbb{Z}$.

(**4**) *Il suffit d'appliquer* (**3**) *avec* $n = p$ *et ensuite de se rappeler que* $\varphi(p) = p - 1$.

**Solution 4.1.6** (Exercice 1.4.6) *Cet exercice est une application de la fonction indicatrice d'Euler.*

(**1**) *Si* $n_d = 0$ *alors le problème est résolu. Suppoons que* $n_d > 1$. *Soit* $g \in G$ *tel que* $\mathrm{o}(g) = d$. *Alors,* $o(\langle g \rangle) = d$ *et donc* $h^d = e$ *pour tout* $h \in \langle g \rangle$. *L'hypothèse montre alors que tous les éléments d'ordre* $d$ *appartiennent à* $\langle g \rangle$. *Or, d'après* 1.3.1, $\langle g \rangle$ *contient* $\varphi(d)$ *éléments d'ordre* $d$. *Il vient que* $n_d \leq \varphi(d)$ *pour tout diviseur* $d$ *de* $\mathrm{o}(G)$.

(**2**) *Notons* $\mathcal{D}$ *l'ensemble des diviseurs de* $\mathrm{o}(G)$ *et, pour un diviseur* $d$ *de* $\mathrm{o}(G)$, *notons* $\mathcal{O}(d)$ *l'ensemble des éléments de* $G$ *d'ordre* $d$. *Il est clair que* $\mathrm{card}\left(\mathcal{O}(d)\right) = n_d$ *et que la famille* $(\mathcal{O}(d) : d \in \mathcal{D})$ *forme une partition de* $G$. *En utilisant* 1.3.6, *nous pouvons écrire*

$$\mathrm{o}(G) = \sum_{d \in \mathcal{D}} \varphi(d) = \sum_{d \in \mathcal{D}} n_d.$$

*Compte tenu de* (**1**), $n_d = \varphi(d)$ *pour tout* $d \in \mathcal{D}$. *En particulier,* $n_{\mathrm{o}(G)} = \varphi(\mathrm{o}(G)) \neq 0$. *Il existe alors un élément d'ordre* $\mathrm{o}(G)$ *dans* $G$ *et* $G$ *est donc cyclique.*

**Solution 4.1.7** (Exercice 1.4.7) *La classe de $m \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est notée $\overline{m}$. Soit $f \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$. Alors $f\left(\overline{1}\right)$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$. Par conséquent, $f\left(\overline{1}\right) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ et ce grâce au résultat établi dans* 1.4.5. *Nous pouvons ainsi définir une application $T$ de $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ vers $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ en posant*

$$T\left(f\right) = f\left(\overline{1}\right) \quad \textit{pour tout } f \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right).$$

*Considérons $f, g \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ et $m \in \{0, 1, ..., n-1\}$ tel que $\overline{m} = g\left(\overline{1}\right)$. Alors*

$$\begin{aligned} T\left(f \circ g\right) &= \left(f \circ g\right)\left(\overline{1}\right) = f\left(g\left(\overline{1}\right)\right) = f\left(\overline{m}\right) = f\left(m\overline{1}\right) \\ &= mf\left(\overline{1}\right) = \overline{m}f\left(\overline{1}\right) = f\left(\overline{1}\right)g\left(\overline{1}\right) = T\left(f\right)T\left(g\right). \end{aligned}$$

*Par suite, $T$ est un morphisme de groupes.*

*Par ailleurs, pour tout $m \in \mathbb{Z}$ tel que $\overline{m} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$, notons $S_{\overline{m}}$ l'application définie de $\mathbb{Z}/n\mathbb{Z}$ vers lui-même par*

$$S_{\overline{m}}\left(\overline{\ell}\right) = \overline{\ell m} \quad \textit{pour tout } \ell \in \mathbb{Z}.$$

*Nous vérifions aisément que $S_{\overline{m}} \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$. Une application $S$ vient ainsi d'être définie de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ vers $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ par*

$$S\left(\overline{m}\right) = S_{\overline{m}} \quad \textit{pour tout } m \in \mathbb{Z} \textit{ tel que } \overline{m} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*.$$

*Soient $k, \ell, m \in \mathbb{Z}$ tels que $\overline{\ell}, \overline{m} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$. Alors*

$$\begin{aligned} S\left(\overline{\ell} \times \overline{m}\right)\left(\overline{k}\right) &= S\left(\overline{\ell m}\right)\left(\overline{k}\right) = S_{\overline{\ell m}}\left(\overline{k}\right) = \overline{k\ell m} = S_{\overline{m}}\left(\overline{k\ell}\right) \\ &= S_{\overline{m}}\left(S_{\overline{\ell}}\left(\overline{k}\right)\right) = \left(S_{\overline{m}} \circ S_{\overline{\ell}}\right)\left(\overline{k}\right) = \left(S\left(\overline{m}\right) \circ S\left(\overline{\ell}\right)\right)\left(\overline{k}\right). \end{aligned}$$

*Ainsi,*

$$S\left(\overline{\ell} \times \overline{m}\right) = S\left(\overline{m}\right) \circ S\left(\overline{\ell}\right)$$

*et $S$ est donc un morphisme de groupes de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ vers $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$.*

*Soit $m \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{m} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$. Alors*

$$\left(T \circ S\right)\left(\overline{m}\right) = T\left(S\left(\overline{m}\right)\right) = T\left(S_{\overline{m}}\right) = S_{\overline{m}}\left(\overline{1}\right) = \overline{m}.$$

*Donc $T \circ S = \mathrm{id}_{\left(\mathbb{Z}/n\mathbb{Z}\right)^*}$. De même, soient $f \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ et $m \in \mathbb{Z}$ tel que $f\left(\overline{1}\right) = \overline{m}$. Alors, pour tout $\ell \in \mathbb{Z}$,*

$$\begin{aligned} \left(\left(S \circ T\right)\left(f\right)\right)\left(\overline{\ell}\right) &= \left(S\left(T\left(f\right)\right)\right)\left(\overline{\ell}\right) = S\left(f\left(\overline{1}\right)\right)\left(\overline{\ell}\right) = \left(S\left(\overline{m}\right)\right)\left(\overline{\ell}\right) \\ &= S_{\overline{m}}\left(\overline{\ell}\right) = \overline{\ell m} = \ell\overline{m} = \ell f\left(\overline{1}\right) = f\left(\ell\overline{1}\right) = f\left(\overline{\ell}\right). \end{aligned}$$

*Il vient que $S \circ T = \mathrm{id}_{\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)}$. En résumé, $T$ et $S$ sont inverses l'une de l'autre.*

*De tout ce que nous venons de dire, nous déduisons que $T$ est un isomorphisme de groupes de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ sur $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$. En particulier,*

$$\mathrm{o}\left(\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)\right) = \mathrm{o}\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right) = \varphi\left(n\right)$$

*et ce d'après le résultat établi dans* 1.4.5.

## 4.2 Groupes symétriques

**Solution 4.2.1** (Exercice 2.4.1) *Il est simple de constater que*

$$\sigma = (1,3,4,6)(2,5).$$

*Or, l'ordre de* $(1,2,3,4)$ *est égal à* $4$ *et l'ordre de* $(2,5)$ *est égal à* $2$*. De plus,* $(1,2,3,4)$ *et* $(2,5)$ *commutent car leurs supports sont disjoints. Ainsi, l'ordre de* $\sigma$ *est* $4 \vee 2 = 4$*. En outre, comme* $\sigma$ *est un morphisme de groupes, nous obtenons*

$$\varepsilon(\sigma) = \varepsilon((1,3,4,6))\,\varepsilon((2,5)) = (-1)^3(-1) = 1.$$

*Par ailleurs, il est clair que*

$$\sigma = (1,3)(3,4)(4,6)(2,5).$$

*Enfin, puisque l'ordre de* $\sigma$ *est égal à* $4$*, nous écrivons, en effectuant la division euclidienne de* $50$ *par* $4$*,*

$$\sigma^{50} = \sigma^{4\times 12+2} = \left(\sigma^4\right)^{12}\sigma^2 = \sigma^2 = (1,4)(3,6).$$

*Les autres exemples se traitent de la même manière.*

**Solution 4.2.2** (Exercice 2.4.2) *Rappelons que les transpositions engendrent* $\mathfrak{S}_n$*. En outre, observons que si* $(x,y)$ *est une transposition de* $\mathfrak{S}_n$ *alors*

$$(x,y) = (1,x)(1,y)(1,x).$$

*Il vient que* $A$ *engendre* $\mathfrak{S}_n$*.*

*Soit* $(x,y)$ *une transposition de* $\mathfrak{S}_n$ *avec* $x < y$*. Si* $y = x+1$ *alors* $(x,y) \in B$*. Sinon, nous avons* $y > x+1$ *et nous écrivons*

$$(x,y) = (y-1,y)(x,y-1)(y-1,y).$$

*Une récurrence simple (sur* $y$*) montre que, dans tous les cas,* $(x,y)$ *est un produit d'éléments de* $B$*. Comme les transpositions engendrent* $\mathfrak{S}_n$*, il en est de même pour* $B$*.*

*Considérons* $x < n$ *et observons que*

$$(x,x+1) = (1,2,...,n)^{x-1}(1,2)(1,2,...,n)^{1-x}.$$

*Autrement dit, tous les éléments de* $B$ *sont produits d'éléments de* $C$*. Or,* $B$ *engendre* $\mathfrak{S}_n$*. Par suite,* $C$ *engendre* $\mathfrak{S}_n$*.*

**Solution 4.2.3** (Exercice 2.4.3)

(**1**) *Soit* $S = \{x_1, x_2, ..., x_r\}$ *une partie à* $r$ *éléments de* $\{1, 2, ..., n\}$. *Dans* $\mathfrak{S}_n$, *il y a exactement* $(r-1)!$ $r$*-cycles de support* $S$. *En effet, pour construire un tel cycle, nous commençons par* $x_1$ *puis nous choisissons une manière parmi* $(r-1)!$ *de placer les* $x_2, ..., x_r$. *En outre, il y a* $\complement_n^r$ *façons de choisir une partie telle que* $S$. *Ceci nous permet de trouver le nombre énoncé.*

(**2**) *Soit* $\sigma \in \mathfrak{S}_n$ *d'ordre* $n$. *Nous écrivons la décomposition de* $\sigma$ *en produits de cycles à supports deux à deux disjoints, soit,* $\sigma = \sigma_1\sigma_2 \cdots \sigma_m$. *Or,* $n$, *l'ordre* $\sigma$, *est le plus petit multiple commun des ordres respectifs de* $\sigma_1, \sigma_2, ...$ *et* $\sigma_m$. *Comme* $n$ *est premier,* $\sigma_1, \sigma_2, ...$ *et* $\sigma_m$ *sont d'ordre* $n$. *Ce sont donc des* $n$*-cycles. Ainsi* $m = 1$ *et le nombre que nous cherchons est en fait le nombre des* $n$*-cycles de* $\mathfrak{S}_n$. *En appliquant* (**1**), *nous obtenons* $(n-1)!\complement_n^n = 1$.

**Solution 4.2.4** (Exercice 2.4.4) *Fixons une transposition* $\tau$ *de* $\mathfrak{S}_n$ *et considérons un morphisme de groupes* $\varphi$ *de* $\mathfrak{S}_n$ *vers* $\mathbb{C}^*$. *Observons d'abord que si* $\pi$ *est une autre transposition de* $\mathfrak{S}_n$ *alors il existe* $\rho \in \mathfrak{S}_n$ *tel que* $\pi = \rho\tau\rho^{-1}$ (*voir* 2.3.3) *et donc*

$$\varphi(\pi) = \varphi\left(\rho\tau\rho^{-1}\right) = \varphi(\rho)\,\varphi(\pi)\,\varphi(\rho)^{-1} = \varphi(\pi).$$

*En outre,*

$$1 = \varphi(\iota_n) = \varphi\left(\tau^2\right) = \varphi(\tau)^2.$$

*Par suite,* $\varphi(\tau) = 1$ *ou* $\varphi(\tau) = -1$. *Supposons que* $\varphi(\tau) = 1$. *Ainsi*

$$\varphi(\pi) = 1 \quad \textit{pour toute transposition } \pi \in \mathfrak{S}_n.$$

*En appliquant* 2.2.5, *nous déduisons que* $\varphi = \theta$. *Supposons, à présent, que* $\varphi(\tau) = -1$. *Donc*

$$\varphi(\pi) = -1 \quad \textit{pour toute transposition } \pi \in \mathfrak{S}_n.$$

*Par conséquent,* $\varphi$ *et* $\varepsilon$ *coïncident sur l'ensemble des transpositions qui engendre* $\mathfrak{S}_n$. *Il vient que* $\varphi = \varepsilon$. *Comme* $\theta$ *et* $\varepsilon$ *sont des déjà des morphismes de groupes de* $\mathfrak{S}_n$ *vers* $\mathbb{C}^*$, *ce sont les seuls.*

**Solution 4.2.5** (Exercice 2.4.5) *Si* $k \in \{1, 2, ..., r-1\}$ *alors*

$$\left(\rho\sigma\rho^{-1}\right)(\rho(x_k)) = \rho\sigma(x_k) = \rho(x_{k+1}).$$

*De plus,*

$$\left(\rho\sigma\rho^{-1}\right)(\rho(x_r)) = \rho\sigma(x_r) = \rho(x_1).$$

*Il vient que* $\rho\sigma\rho^{-1}$ *est le* $r$*-cycle* $(\rho(x_1), ..., \rho(x_r))$.

**Solution 4.2.6** (Exercice 2.4.6) *Le fait que $A$ engendre $\mathfrak{A}_n$ découle directement de 4.2.2 et du fait que les permutations de $\mathfrak{A}_n$ sont produits pairs de transpositions.*

*Pour $B$, il suffit d'utiliser le fait que $A$ engendre $\mathfrak{A}_n$ tout en observant que*

$$(1,x)(1,y) = (1,y,x) = (1,2,x)(1,2,y)^2 \quad \text{pour tout } (x,y) \in \{3,...,n\}^2 \text{ avec } x \neq y.$$

*Finissons avec $C$. Nous vérifions aisément que*

$$(1,2,x) = (1,x,2)^2 \quad \text{pour tout } x \in \{3,...,n\}.$$

*Le reste découle du fait que $B$ engendre $\mathfrak{A}_n$.*

**Solution 4.2.7** (Exercice 2.4.7) *Si $n \in \{1,2\}$ alors $\mathfrak{A}_n = \{\iota_n\}$ et donc $\mathcal{Z}(\mathfrak{A}_n) = \mathfrak{A}_n$. Si $n = 3$ alors $\mathfrak{A}_3$ est d'ordre 3 et est donc abélien. Il s'en suit que*

$$\mathcal{Z}(\mathfrak{A}_3) = \mathfrak{A}_3 = \{\iota_3, (1,2,3), (1,3,2)\}.$$

*Envisageons le cas $n \geq 4$. Si $\sigma \in \mathcal{Z}(\mathfrak{A}_n)$ et si $x, y, z$ sont distincts dans $\{1,2,...,n\}$ alors (voir 4.2.5)*

$$(x,y,z) = (x,y,z)\sigma\sigma^{-1} = \sigma(x,y,z)\sigma^{-1} = (\sigma(x), \sigma(y), \sigma(y)).$$

*Par suite, $\{x,y,z\} = \{\sigma(x), \sigma(y), \sigma(z)\}$. Fixons $x, y \in \{1,2,...,n\}$ tels que $x \neq y$ et choisissons $z, u$ dans $\{1,2,...,n\}$ tels que $z \neq u$ et $z, u \notin \{x,y\}$. Ainsi*

$$\{x,y\} = \{x,y,z\} \cap \{x,y,u\} = \{\sigma(x), \sigma(y), \sigma(z)\} \cap \{\sigma(x), \sigma(y), \sigma(u)\} = \{\sigma(x), \sigma(y)\}.$$

*Fixons enfin $x \in \{1,2,...,n\}$ et choisissons $y, z \in \{1,2,...,n\}$ tels que $y \neq z$ et $x, y \notin \{x\}$. Alors*

$$\{x\} = \{x,y\} \cap \{x,z\} = \{\sigma(x), \sigma(y)\} \cap \{\sigma(x), \sigma(z)\} = \{\sigma(x)\}.$$

*Il vient que*

$$\sigma(x) = x \quad \text{pour tout } x \in \{1,2,...,n\}$$

*et donc $\mathcal{Z}(\mathfrak{A}_n) = \{\iota_n\}$.*

**Solution 4.2.8** (Exercice 2.4.8) *Nous savons que $\mathfrak{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$. Supposons que $H$ est un sous-groupe de $\mathfrak{S}_n$ d'indice 2. Alors $H$ est distingué dans $\mathfrak{S}_n$ et le groupe quotient $\mathfrak{S}_n/H$, étant d'ordre 2, est abélien. D'où*

$$\sigma\rho\sigma^{-1}\rho^{-1} \in H \quad \text{pour tout } (\sigma,\rho) \in (\mathfrak{S}_n)^2.$$

*En particulier, si $x, y, z \in \{1,2,...,n\}$ distincts alors*

$$(x,y)(x,z)(x,y)^{-1}(x,z)^{-1} = (x,y)(x,z)(x,y)(x,z) = (x,y,z).$$

*Ainsi, $H$ contient un 3-cycle de $\mathfrak{S}_n$. Comme les 3-cyles sont conjugués (voir 2.3.3) et $H$ est distingué dans $\mathfrak{S}_n$, $H$ contient tous les 3-cyles. En utilisant 4.2.6, nous déduisons que $H$ contient $\mathfrak{A}_n$. Ayant le même indice, $H = \mathfrak{A}_n$.*

**Solution 4.2.9** (Exercice 2.4.9)

(**1**) *Posons*

$$\sigma = (1,2)(3,4), \rho = (1,3)(2,4), \tau = (1,4)(2,3).$$

*Un calcul simple donne*

| $\circlearrowleft$ | $\iota_4$ | $\sigma$ | $\rho$ | $\tau$ |
|---|---|---|---|---|
| $\iota_4$ | $\iota_4$ | $\sigma$ | $\rho$ | $\tau$ |
| $\sigma$ | $\sigma$ | $\iota_4$ | $\tau$ | $\rho$ |
| $\rho$ | $\rho$ | $\tau$ | $\iota_4$ | $\sigma$ |
| $\tau$ | $\tau$ | $\rho$ | $\sigma$ | $\iota_4$ |

*Ceci montre que $H$ est un sous-groupe de $\mathfrak{A}_4$. Notons au passage que $H$ est abélien.*

(**2**) *Ceci découle du fait que $K$ est d'indice 2.*

(**3**) *Il suffit de se rappeler qu'un 3-cycle est différent de son inverse.*

(**4**) *En utilisant 2.3.3, nous écrivons*

$$\sigma(x,y)(z,t)\sigma^{-1} = \sigma(x,y)\sigma^{-1}\sigma(z,t)\sigma^{-1} = (\sigma(x),\sigma(y))(\sigma(z),\sigma(t)) = (y,z)(x,t).$$

(**5**) *Comme $H$ contient 5 éléments autres aue $\iota_4$, dont un nombre pair de 3-cycles, $K$ contient au moins un élément de $H$. En outre, (**4**) montre que les éléments de $H$ sont conjugués. Puisque $K$ est disitngué dans $\mathfrak{A}_4$, $K$ contient $H$.*

(**6**) *Nous avons obtenu dans (**5**) le fait que $K$ est un sous-groupe de $H$. Mais ceci contredit le théorème de Lagrange car $H$ est d'ordre 6 et $K$ est d'ordre 4. Notre supposition est donc fausse. Autrement dit, $\mathfrak{A}_4$ ne contient aucun sous-groupe d'ordre 6.*

## 4.3 Opération d'un groupe sur un ensemble

**Solution 4.3.1** (Exercice 3.4.1) *L'opération de $G$ sur $\mathrm{Im}(\varphi)$ qu'il faut considérer est donnée par*

$$g \cdot x = x\varphi(g) \quad \text{pour tout } (g,x) \in G \times \mathrm{Im}(\varphi).$$

*Si $x \in \mathrm{Im}(\varphi)$ alors il existe $h \in G$ tel que $x = \varphi(h)$. Ainsi,*

$$\Omega(x) = \{g \cdot x : g \in G\} = \{\varphi(gh) : g \in G\} = \mathrm{Im}(\varphi).$$

*En particulier, il existe une et une seule orbite sous cette action. De plus,*

$$G(x) = \{g \in G : g \cdot x = x\} = \{g \in G : x\varphi(g) = x\} = \ker(\varphi).$$

*D'après* 3.2.4,

$$\mathrm{o}\left(\mathrm{Im}\left(\varphi\right)\right) = \mathrm{card}\left(\Omega\left(x\right)\right) = \left[G : G\left(x\right)\right] = \frac{\mathrm{o}\left(G\right)}{\mathrm{o}\left(\ker\left(\varphi\right)\right)},$$

*ce qui prouve le résultat demandé.*

**Solution 4.3.2** (Exercice 3.4.2)

(**1**) *Comme les déplacements de* $\mathbb{R}^3$ *sont des permutations de* $\mathbb{R}^3$*, nous pouvons prouver que* $G$ *est un sous-groupe de* $\mathfrak{S}\left(\mathbb{R}^3\right)$*, ce qui est immédiat.*

(**2**) *Posons* $\Delta \cap \mathcal{C} = \{A, B\}$*. Autrement dit,* $A$ *et* $B$ *sont deux sommets de* $\mathcal{C}$ *non situés sur une même face de* $\mathcal{C}$*. La distance qui sépare* $A$ *et* $B$ *est la même que celle qui sépare* $g\left(A\right)$ *et* $g\left(B\right)$*. De plus* $g\left(A\right)$ *et* $g\left(B\right)$ *sont situés sur* $\mathcal{C}$*. Donc* $g\left(A\right)$ *et* $g\left(B\right)$ *sont deux sommets de* $\mathcal{C}$ *non situés sur une même face de* $\mathcal{C}$*. En particulier,* $g$ *laisse globalement invariant l'ensemble des sommets de* $\mathcal{C}$*. En outre,* $g$ *conserve l'alignement. En résumé,* $g\left(\Delta\right)$ *est la droite qui passe par* $g\left(A\right)$ *et* $g\left(B\right)$ *et donc* $g\left(\Delta\right)$ *est une diagonale de* $\mathcal{C}$*.*

(**3**) *Soient* $\Delta \in X$ *et* $f, g \in G$*. Alors*

$$\mathrm{id}_{\mathbb{R}^3} \cdot \Delta = \Delta \text{ et } \left(f \circ g\right) \cdot \Delta = \left(f \circ g\right)\left(\Delta\right) = f\left(g\left(\Delta\right)\right) = f \cdot \left(g \cdot \Delta\right).$$

(**4**) *Soit* $g \in G$ *tel que*

$$g \cdot \Delta = \Delta \quad \text{pour tout } \Delta \in X.$$

*Donc toutes les diagonales sont des droites fixes de* $g$*. Or, si* $g \neq \mathrm{id}_{\mathbb{R}^3}$ *alors* $g$ *admet une seule droite fixe, à savoir, son axe. Il vient que* $g = \mathrm{id}_{\mathbb{R}^3}$ *et l'opération considérée est donc fidèle. En d'autres termes, le morphisme canoniquement associé à notre opération, que nous notons* $\gamma$*, est injectif de* $G$ *dans* $\mathfrak{S}\left(X\right)$*. Mais* $X$ *contient quatres diagonales. Par suite,* $\mathfrak{S}\left(X\right)$ *est isomorphe à* $\mathfrak{S}_4$ *et* $G$ *est alors isomorphe à un sous-groupe de* $\mathfrak{S}_4$*. Une transposition de* $\mathfrak{S}_4$ *correspond à un échange entre deux diagonales. Il existe visiblement un déplacement de* $\mathbb{R}^3$ *qui échange deux diagonales données de* $\mathcal{C}$*. Compte tenu du fait que les transpositions engendrent* $\mathfrak{S}_4$*, il vient que* $\gamma$ *est surjectif. Par conséquent,* $G$ *est isomorphe à* $\mathfrak{S}_4$*.*

**Solution 4.3.3** (Exercice 3.4.3) *D'après* 3.3.4*,* $G$ *contient un* $p$*-Sylow* $S$*. En utilisant* 3.2.7*,* $\mathcal{Z}\left(S\right)$ *n'est pas réduit à l'élément neutre. Comme* $\mathrm{o}\left(\mathcal{Z}\left(S\right)\right)$ *divise* $\mathrm{o}\left(S\right)$*,* $\mathcal{Z}\left(S\right)$ *est un* $p$*-groupe abélien. Nous pouvons ainsi appliquer* 3.3.1*. Il existe alors* $g \in \mathcal{Z}\left(S\right)$ *d'ordre* $p$*. L'élément* $g$ *répond à la question.*

**Solution 4.3.4** (Exercice 3.4.4)

(**1**) *Comme $G$ est un $p$-groupe, son centre $\mathcal{Z}(G)$ n'est pas réduit à l'élément neutre (voir* 3.2.7*). Puisque $\mathrm{o}(\mathcal{Z}(G))$ divise $p^2$, nous obtenons $\mathrm{o}(\mathcal{Z}(G)) \in \{p, p^2\}$. Supposons que $\mathrm{o}(\mathcal{Z}(G)) = p$. Ainsi, $[G : \mathcal{Z}(G)] = p^2/p = p$. Mais ceci est impossible compte tenu de* 1.4.4*. Nous en déduisons que $\mathrm{o}(\mathcal{Z}(G)) = p^2$ et donc $G = \mathcal{Z}(G)$. Il vient que $G$ est abélien.*

(**2**) *Si $G$ contient un élément d'ordre $p^2$ alors $G$ est cyclique et est donc isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Sinon, tous les éléments de $G$ autre que l'élément neutre sont d'ordre $p$. De plus,* 3.3.3 *entraîne l'existence d'un sous-groupe $H$ de $G$ d'ordre $p$. Soit $g \in G$ tel que $g \notin H$. Comme $g$ est d'ordre $p$, le sous-groupe cyclique $\langle g \rangle$ de $G$ est également d'ordre $p$ et donc tous ses éléments sont des générateurs. Il s'en suit que $H \cap \langle g \rangle$ est réduit à l'élément neutre. Par conséquent, l'application $\varphi$ définie de $H \times \langle g \rangle$ par*

$$\varphi((h, g^m)) = hg^m \quad \textit{pour tout } (h, m) \in H \times \mathbb{Z}$$

*est un isomorphisme de groupe. Ce qui prouve que $G$ est isomorphe à $H \times \langle g \rangle$ et donc à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

**Solution 4.3.5** (Exercice 3.4.5)

(**1**) *D'après* 3.2.7*, $\mathcal{Z}(G)$ n'est pas réduit à l'élément neutre. De plus, $\mathcal{Z}(G)$ est propre car $G$ est non abélien. Mais comme $\mathcal{Z}(G)$ est distingué dans $G$, $G$ n'est pas simple.*

(**2**) *Si $G$ possède un seul $p$-Sylow $S$ alors $S$ est distingué (voir* 3.3.8*). Ceci contredit la simplicité de $G$.*

**Solution 4.3.6** (Exercice 3.4.6)

(**1**) *Notons $n_p$ le nombre des $p$-Sylows de $G$. D'après* 3.3.9*, $n_p \equiv 1 \pmod{p}$ et $n_p$ divise $q$. Comme $q$ est premier, $n_p \in \{1, q\}$. Si $n_p = q$ alors $q \equiv 1 \pmod{p}$. Ceci contredit l'hypothèse. Donc $n_p = 1$.*

(**2**) *Un $p$-Sylow de $G$ est d'ordre $p$ et donc c'est un sous-groupe propre de $G$. Puisqu'il existe un seul $p$-Sylow de $G$, ce $p$-Sylow est distingué (voir* 3.3.8*). Il vient que $G$ n'est pas simple.*

(**3**) *D'après* (**1**) *et* (**2**)*, $G$ admet un unique $p$-Sylow $H$ et un unique $q$-Sylow $K$ qui sont distingués. Comme $H$ est d'ordre $p$ et $p$ est premier, $H$ est cyclique (voir* 1.1.5*). Il existe alors $h \in H$ tel que $H = \langle h \rangle$. De même, il existe $k \in K$ tel que $K = \langle k \rangle$. En outre, puisque $p \neq q$, nous avons $H \cap K = \{e\}$, où $e$ désigne l'élément neutre de $G$. Observons à présent que*

$$hkh^{-1}k^{-1} = h\left(kh^{-1}k^{-1}\right) \in H$$

*car $H$ est distingué dans $G$. Nous montrons de la même manière que $hkh^{-1}k^{-1} \in K$ et par suite $hkh^{-1}k^{-1} = e$. Il en résulte que $hk = kh$. Ainsi, l'ordre de $hk$ est $pq$. Il vient que $G$ est cyclique et $hk$ en est un générateur.*

(**4**) *Nous écrivons* $35 = 5 \times 7$. *De plus,* 5 *ne divise pas* 6 *et* 7 *ne divise pas* 4. *Compte tenu de* (**3**)*, tout groupe d'ordre* 35 *est cyclique.*

**Solution 4.3.7** (Exercice 3.4.7)

(**1**) *D'après* 3.3.8*, les p-Sylows* $S_1, S_2, ...$ *et* $S_n$ *sont distingués. Nous déduisons que* $H = S_1 S_2 \cdots S_n$ *est un sous-groupe distingué de* $G$[1]*. Nous vérifions aisément que* $H$ *est isomorphe au groupe produit* $S_1 \times S_2 \times \cdots \times S_n$*. En particulier,*

$$\mathrm{o}(H) = \mathrm{o}(S_1)\,\mathrm{o}(S_2) \cdots \mathrm{o}(S_n) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} = \mathrm{o}(G).$$

*Ainsi,* $G = H$ *et* $G$ *est donc isomorphe à* $S_1 \times S_2 \times \cdots \times S_n$*.*

(**2**) *Comme* $G$ *est abélien, tout sous-groupe de* $G$ *est distingué. Il vient, d'après* 3.3.8*, que pour tout diviseur* $p$ *premier de* $G$*, il existe un unique p-Sylow de* $G$*. Le reste se déduit de* (**1**)*.*

**Solution 4.3.8** (Exercice 3.4.8) *Notons* $n_2 = \mathrm{card}(\mathcal{S}(2))$.

(**1**) *Ecrivons* $48 = 2^4 \times 3$*. D'après* 3.3.4*,* $n_2 \geq 1$ *et d'après* 3.3.9*,* $n_2$ *divise* 3 *et* 2 *divise* $n_2 - 1$*. Par suite,* $n_2 \in \{1, 3\}$*.*

(**2**) *Il suffit d'appliquer* 3.3.8*.*

(**3**) *C'est une conséquence immédiate de* 3.3.5*.*

(**4**) *Notons* $\gamma$ *le morphisme de groupes de* $G$ *vers* $\mathfrak{S}(\mathcal{S}(2))$ *canoniquement associé à l'opération définie dans* (**3**)*. Il est clair que* $\mathrm{o}(\mathfrak{S}(\mathcal{S}(2))) = 6$ *car* $\mathrm{card}(\mathcal{S}(2)) = 3$*. Comme* $\mathrm{o}(G) = 48$*,* $\gamma$ *n'est pas injectif et donc* $\ker(\gamma)$ *n'est pas réduit à l'élément neutre. En outre, il est clair que* $\ker(\gamma) \subsetneq G$*. Il vient que* $G$ *n'est pas simple car* $\ker(\gamma)$ *est un sous-groupe propre disintgué dans* $G$*.*

**Solution 4.3.9** (Exercice 3.4.9) *Le théorème de Lagrange assure que si* $G$ *est* $p$*-groupe alors l'ordre de tout élément de* $G$ *est une puissance de* $p$*. Inversement, supposons que l'ordre de tout élément de* $G$ *est une puissance de* $p$*. Soit* $q$ *un diviseur premier de* $\mathrm{o}(G)$*. D'après* 3.3.4*, il existe un* $q$*-Sylow dans* $G$*. Compte tenu de* 3.4.3*, il existe un élément de* $G$ *d'ordre* $q$*. Il s'en suit* $q$ *est une puissance de* $p$ *et donc que* $q = p$*. Nous déduisons que* $G$ *est un* $p$*-groupe.*

[1]Il est bien connu que *si* $G$ *est groupe,* $H, K$ *sont deux sous-groupes de* $G$ *et si* $H$ *est distingué dans* $G$ *alors* $HK$ *est un sous-groupe de* $G$ *et* $HK = KH$*. Si, de plus,* $K$ *est distingué dans* $G$ *alors* $HK$ *est distingué dans* $G$*.*

# Bibliographie


[1] A. Ben Kilani & S. Msallem Ghorbel, *Groupes. Anneaux. Corps. Exemples et Applications*, Centre de Publication Universitaire, Tunis, 2006

[2] J. Calais, *Eléments de Théorie de Groupes*, Presses Universitaires de France, Paris, 1998

[3] C. Deschamps, A. Miquel, F. Moulin, J. F. Ruaud, J. C. Sifre & A. Warusfel, *Mathématiques 2$^{e}$ année Cours et Exercices Corrigés*, Dunod Paris, 2001

[4] S. Lang, *Algèbre*, Dunod, Paris, 2002

[5] M. P. Malliavin, *Les Groupes Finis et leurs Représentations Complexes*, Masson, Paris, 1985

[6] R. Mneimne & F. Testard, *Introduction à la Théorie des Groupes de Lie Classiques*, Hermann, Paris, 1986

[7] D. Perrin, *Cours d'Algèbre*, Ellipses, Paris, 1996

[8] J. Querré, *Cours d'Algèbre*, Masson, 1976

[9] P. Tauvel, *Cours d'Algèbre*, Dunod, Paris, 1999