GROUPES

Chapitre 1

Ce polycopié est très largement inspiré du polycopié utilisé par mon prédécesseur K. Koufany, que je remercie pour son travail de rédaction.

Table des matières

1. Relations d'équivalence

Dans cette section E désigne un ensemble non vide et $\mathcal{P}(E)$ l'ensemble des parties de E.

Définition 1.1. — *Une* **relation binaire** *sur E est un sous-ensemble $G \subset E \times E$ du produit cartésien $E \times E$. Une telle relation binaire sera notée $\mathcal{R}$. Au lieu de noter $(x, y) \in G$ on notera $x\mathcal{R}y$ et on dira que x est en relation avec y.*

Comme exemples, nous avons :

– *"Egalité"*, sur E :

$$G = \{(x, y) \in E^2 \mid x = y\} \text{ i.e. } x\mathcal{R}y \Leftrightarrow x = y.$$

– *"Inclusion"*, sur $\mathcal{P}(E)$:

$$G = \{(X, Y) \in \mathcal{P}(E)^2 \mid X \subset Y\} \text{ i.e. } X\mathcal{R}Y \Leftrightarrow X \subset Y.$$

– *"Ordre"*, sur $\mathbb{R}$:

$$G = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\} \text{ i.e. } x\mathcal{R}y \Leftrightarrow x \leq y.$$

Définition 1.2. — *Une relation binaire $\mathcal{R}$ sur E est*

1. *réflexive si $\forall x \in E$, $x\mathcal{R}x$,*
2. *symétrique si $\forall x, y \in E$, $x\mathcal{R}y \Rightarrow y\mathcal{R}x$*
3. *transitive si $\forall x, y, z \in E$, $(x\mathcal{R}y$ et $y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.*

On appelle **relation d'équivalence** *sur E toute relation binaire réflexive, symétrique et transitive.*
Une telle relation se note parfois $x \equiv y$ (modulo $\mathcal{R}$).

La relation *"Egalité"* est une relation d'équivalence, par contre *"Inclusion"* et *"Ordre"* ne le sont pas.

Un exemple standard d'une relation d'équivalence est la relation de congruence sur $\mathbb{Z}$: Soit $n \in \mathbb{N}$ non nul et $x, y \in \mathbb{Z}$,

$$x \equiv y\,[n] \Leftrightarrow n \text{ divise } y - x.$$

On vérifie assez facilement que cette relation est réflexive, symétrique et transitive, donc une relation d'équivalence.

Pour un élément $x \in E$, on appelle **classe d'équivalence** (ou classe) de x par rapport à la relation d'équivalence $\mathcal{R}$, l'ensemble

$$\bar{x} := \{y \in E\ ,\ y\mathcal{R}x\},$$

des éléments y de E qui sont en relation avec x. D'après la réflexivité, la classe $\bar{x}$ contient x. Un élément de $\bar{x}$ est appelé *représentant* de la classe $\bar{x}$.

Proposition 1.3. — *Deux classes d'équivalences sont soit confondues, soit disjointes.*

Démonstration. — Soient $x, y \in E$. Si $\bar{x}$ et $\bar{y}$ ne sont pas disjointes, alors il existe $z \in \bar{x} \cap \bar{y}$. D'après la transitivité, $x\mathcal{R}y$ d'où $x \in \bar{y}$ et donc $\bar{x} \subset \bar{y}$. Comme les conditions $y \in \bar{x}$ et $x \in \bar{y}$ sont équivalentes par symétrie, on a de même $\bar{y} \subset \bar{x}$. Par conséquent, $\bar{x} = \bar{y}$. □

L'ensemble des classes d'équivalences est un sous-ensemble de $\mathcal{P}(E)$, appelé *ensemble quotient* de E par $\mathcal{R}$ et on le note $E/\mathcal{R}$:

$$E/\mathcal{R} = \{\bar{x} \mid x \in E\}.$$

Il en résulte que tout élément de E appartient à une et une seule classe d'équivalence. Les classes d'équivalences constituent donc une partition de E, *i.e.*

$$E = \coprod_{\alpha \in E/\mathcal{R}} \alpha.$$

L'application $p : E \to E/\mathcal{R}$ définie par $p(x) = \bar{x}$ est surjective; elle est appelée la **surjection canonique** ou **l'application de passage au quotient**. L'application p n'est pas en général injective, mais elle vérifie

$$\forall x, y \in E, \;\; p(x) = p(y) \Leftrightarrow \bar{x} = \bar{y} \Leftrightarrow x \mathcal{R} y.$$

C'est exactement ce que l'on peut raisonnablement demander à une application de passage au quotient : elle confond deux éléments x, y (ie $p(x) = p(y)$) exactement lorsqu'ils sont en relation (ie $x\mathcal{R}y$).

Exemple 1.4. — Soit $E = \{1, 2, 3\}$ et $\mathcal{R}$ la relation d'équivalence définie sur E par $1\mathcal{R}1, 2\mathcal{R}2, 3\mathcal{R}3, 2\mathcal{R}3$ et $3\mathcal{R}2$ (et aucune autre relation entre ces éléments). On a alors $E/\mathcal{R} = \{\{1\}, \{2, 3\}\}$, et l'application p est donnée par $p(1) = \{1\}$ et $p(2) = p(3) = \{2, 3\}$.

Proposition 1.5. — *Considérons une relation d'équivalence $\mathcal{R}$ sur un ensemble E, une application f de E dans un ensemble F. Alors, il existe une application $\bar{f}$ de $E/\mathcal{R}$ dans F, telle que $\bar{f} \circ p = f$, si et seulement si f est constante sur chaque classe d'équivalence. De plus, si c'est le cas, $\bar{f}$ est unique et on a* $\mathrm{Im}(f) = \mathrm{Im}(\bar{f})$.

Remarque 1.6. — *Il sera parlant visuellement de représenter l'existence de $\bar{f}$ par le "diagramme commutatif" suivant :*

$$\begin{array}{ccc} E & \xrightarrow{\;f\;} & F \\ {\scriptstyle p}\downarrow & \nearrow_{\bar{f}} & \\ E/\mathcal{R} & & \end{array}$$

Les deux flêches en traits pleins indiquent les données du problème, et la flêche en pointillées celle qui est obtenue grâce à la proposition. La "commutativité" du diagramme signifie que quelque soit le chemin choisi pour aller de E à F (directement ou en passant par $E/\mathcal{R}$), le résultat obtenu est le même. Autrement dit, $f = \bar{f} \circ p$.

Démonstration. — Supposons f constante sur toutes les classes d'équivalence. La relation $f = \bar{f} \circ p$ implique que pour $\alpha \in E/\mathcal{R}$ et $x \in \alpha$, on a $\bar{f}(\alpha) = x$. Ceci détermine $\bar{f}$, qui est donc unique si elle existe. Ceci donne de plus une indication pour montrer l'existence de $\bar{f}$: considérons l'application $\bar{f} : E/\mathcal{R} \to F$ définie par $\bar{f}(\alpha) = f(x)$ dès que $x \in \alpha$. Puisque f est constante sur toute classe d'équivalence donc en particulier sur α, la valeur de $f(x)$ ne dépend que de $\alpha \in E/\mathcal{R}$ et non des représentants x de α. On en déduit que l'application $\bar{f}$ est bien définie et vérifie $\bar{f} \circ p = f$. Finalement, il est clair que $\mathrm{Im}(f) = \mathrm{Im}(\bar{f})$.

Réciproquement, si $\overline{f}$ existe, on a pour x, y tels que $\bar{x} = \bar{y}$, les égalités

$$f(x) = \bar{f}(\bar{x}) = \bar{f}(\bar{y}) = f(y)\,,$$

ce qui montre que f est constante sur les classes d'équivalence. □

On dit que $\bar{f}$ se déduit de f par factorisation, ou par passage au quotient.

2. Lois de composition interne

Définition 2.1. — *On appelle* **loi de composition interne** *ou* **opération** *sur un ensemble non vide E toute application définie sur $E \times E$ et à valeurs dans E.*

On désignera par $(E, *)$ l'ensemble E muni de la loi de composition interne

$$(x, y) \mapsto x * y$$

Exemple 2.2. — 1. L'addition et la multiplication usuelles sont des lois de composition interne sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

2. Si E est un ensemble non vide, alors les applications

$$\begin{aligned} (A, B) &\mapsto A \cap B, \\ (A, B) &\mapsto A \cup B, \\ (A, B) &\mapsto A \Delta B = (A \cup B) \setminus (A \cap B) \end{aligned}$$

sont des lois de composition interne sur $\mathcal{P}(E)$.

3. Si E est un ensemble non vide et $\mathcal{F}(E)$ l'ensemble des applications de E dans E, alors

$$(f, g) \mapsto f \circ g$$

est une loi de composition interne sur $\mathcal{F}(E)$.

4. Dans l'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices carrées $n \times n$ à coefficients réels les opérations usuelles d'addition $(A, B) \mapsto A + B$ et de multiplication $(A, B) \mapsto AB$ sont des lois de composition interne.

5. Dans l'ensemble $GL_n(\mathbb{R})$ des matrices carrées $n \times n$ à coefficients réels inversibles, l'addition n'est pas une loi de composition interne, alors que la multiplication en est une.

Définition 2.3. — *Soit E un ensemble non vide muni d'une loi de composition interne $(x, y) \mapsto x * y$.*

– *La loi est* **associative** *si :*

$$\forall x, y, z \in E,\ (x * y) * z = x * (y * z)$$

– *Elle est* **commutative** *si :*

$$\forall x, y \in E,\ x * y = y * x$$

– *S'il existe* $e \in E$ *tel que*

$$\forall x \in E,\ x * e = e * x = x$$

on dit que e *est un* **élément neutre** *pour* $(E, *)$

– *Si* $(E, *)$ *possède un élément neutre* e*, alors un élément* $x \in E$ *est dit* **inversible***, s'il existe* $x' \in E$ *tel que*

$$x * x' = x' * x = e$$

x' *est alors appelé* **inverse** *de* x *dans* $(E, *)$.

Remarque 2.4. — *Si* $(E, *)$ *possède un élément neutre* e*, alors il est unique et il est son propre inverse. Si la loi est associative, alors tout élément a au plus un inverse.*

En effet, supposons que $(E, *)$ possède deux éléments neutre e_1 et e_2. Puisque e_1 est neutre on a $e_1 * e_2 = e_2$ et puisque e_2 est aussi neutre $e_1 * e_2 = e_1$, d'où $e_1 = e_2$.

Soit x_1 et x_2 deux inverses de x dans E, alors

$$x_1 x = e \Rightarrow (x_1 x)x_2 = x_2 \text{ et } x x_2 = e \Rightarrow x_1(x x_2) = x_1\,.$$

La loi étant associative, on a $x_1 = x_2$.

Exemple 2.5. —

1. Les opérations usuelles d'addition et de multiplication sont commutatives et associatives sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. 0 est l'élément neutre pour l'addition et 1 est l'élément neutre pour la multiplication pour chacun des ensembles.
   Dans $(\mathbb{N}, +)$ aucun élément non nul n'est inversible.
   Dans $(\mathbb{N}, \times)$ aucun élément différent de 1 n'est inversible.
   Dans $(\mathbb{Z}, +)$ tout élément est inversible ($-x$ est l'inverse de x)
   Dans $(\mathbb{Z}, \times)$ seuls 1 et -1 sont inversibles.
2. Si E est un ensemble non vide, les opérations $\cap$ et $\cup$ sont commutatives et associatives sur $\mathcal{P}(E)$. L'ensemble vide $\emptyset$ est un élément neutre pour $\cup$ et E est un élément neutre pour $\cap$. Quels sont les éléments inversibles pour ces deux lois ?
3. Si E est un ensemble non vide, la composition des applications dans $\mathcal{F}(E)$ est associative mais non commutative dès que E a plus d'un élément. L'identité Id_E est l'élément neutre pour cette loi.
4. Dans $\mathcal{M}_n(\mathbb{R})$ l'addition est associative et commutative; la multiplication est associative et non commutative.
5. Dans $\mathbb{R}^3$ l'opération produit vectoriel

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \wedge \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} yz' - y'z \\ zx' - z'x \\ xy' - x'y \end{pmatrix}$$

est une loi de composition qui n'est ni associative ni commutative. En effet, si (e_1, e_2, e_3) est la base canonique de $\mathbb{R}^3$, alors

$$e_2 \wedge (e_2 \wedge e_3) = e_2 \wedge e_1 = -e_3, \quad (e_2 \wedge e_2) \wedge e_3 = 0_{\mathbb{R}^3} \wedge e_3 = 0_{\mathbb{R}^3}$$

et

$$e_1 \wedge e_2 = e_3, \quad e_2 \wedge e_1 = -e_3.$$

3. Groupes

Définition 3.1. — *Un groupe $(G, *)$ est un ensemble G muni d'une loi de composition interne $*$ possédant les propriétés suivantes :*

- *la loi $*$ est associative : $\forall x, y, z \in G,\ x * (y * z) = (x * y) * z$;*
- *la loi $*$ possède un un éléments neutre : $\exists e \in G,\ \forall x \in G,\ x*e = e*x = x$;*
- *tout élément de G admet un inverse : $\forall x \in G, \exists x' \in G,\ x*x' = x'*x = e$.*

Remarque 3.2. — En général, s'il n'y a pas de confusion, on dira tout simplement que G est un groupe pour $(G, *)$ est un groupe et on notera parfois xy ou $x + y$ le résultat de l'opération $x * y$.
Avec la première notation, on dit que G est un groupe multiplicatif et on notera 1 ou e l'élément neutre; l'inverse d'un élément $x \in G$ s'écrit x^{-1} et est appelé **inverse** de x.

La seconde notation ne s'emploie par convention que pour des groupes commutatifs, on notera dans ce cas 0 l'élément neutre et $-x$ l'inverse de x (il sera sage de parler d'opposé plutôt que d'inverse dans ce cas).
Attention : *Il y a ici une source de confusion et donc d'erreur, car pour parler de l'inverse d'un élément, il faut savoir de quel groupe on parle (et de quelle loi de groupe). Ainsi, l'inverse de* 2 *dans* $(\mathbb{Q}, +)$ *est* -2*, et l'inverse de* 2 *dans le groupe* $(\mathbb{Q}^*, \times)$ *est* $\frac{1}{2}$.

C'est la notation multiplicative que nous adopterons pour énoncer et démontrer les propriétés générales des groupes. Cependant, selon l'usage, c'est la notation additive qui sera employée pour l'étude des groupes abéliens.

Définition 3.3. — *1. Un groupe G est dit est* **commutatif** *ou* **abélien** *si pour tout $x, y \in G$ on a $xy = yx$, autrement dit, si sa loi est commutative.*

*2. Un groupe G est dit fini s'il n'a qu'un nombre fini d'éléments. Dans ce cas le cardinal de G s'appelle l'***ordre** *du groupe G; il est noté $o(G)$ ou $|G|$.*

Exemples 3.4. —

1. $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, et $\mathbb{C}$ munis de l'addition sont des groupes abéliens.
2. $\mathbb{Q}^\times$, $\mathbb{R}^\times$ et $\mathbb{C}^\times$ munis de la multiplication sont des groupes abéliens. Plus généralement, si $(A, +, \times)$ est un anneau unitaire, alors l'ensemble des éléments inversibles $A^\times$ muni de la loi $\times$ est un groupe. Par exemple, $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ est un groupe multiplicatif.

3. $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition des classes est un groupe abélien fini d'ordre n, sont élément neutre est $\bar{0}$.
4. Le groupe $(\mathbb{Z}/5\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ muni de la multiplication, est un groupe abélien d'ordre 4. Son élément neutre est $\bar{1}$. On peut remarquer que $(\bar{2})^{-1} = \bar{3}$, $(\bar{3})^{-1} = \bar{2}$ et $(\bar{4})^{-1} = \bar{4}$.
5. Le groupe symétrique $\mathfrak{S}_n$ muni de la composition des applications est un groupe fini d'ordre $n!$. Pour $n \geq 3$, $\mathfrak{S}_n$ n'est pas abélien.
6. L'ensemble
$$Q_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \right\}$$
muni de la multiplication est un groupe fini d'ordre 8, non abélien, appelé groupe des quaternions.
7. $\mathrm{GL}(n, \mathbb{R})$ muni de la multiplication des matrices est un groupe non abélien.

Proposition 3.5. — *Dans un groupe G,*
(a) l'élément neutre est unique,
(b) tout élément possède un unique inverse,
(c) tout élément $a \in G$ est régulier (ou simplifiable) à droite et à gauche,

$$\forall x, y \in G,\ (xa = ya \Rightarrow x = y) \text{ et } (ax = ay \Rightarrow x = y).$$

(d) Le produit dans G de n éléments, $x_1, x_2, \ldots, x_n$ pris dans cet ordre ($n \geq 2$ dans $\mathbb{N}$) est défini par $x_1 x_2 \cdots x_n$ (définition par récurrence) .
En particulier, si $x \in G$, alors la puissance n-ième de x est

$$x^n = xx \cdots x, \text{ produit de } x, n \text{ fois} \tag{1}$$

Pour tous les entiers positifs m et n on a

$$x^n x^m = x^{n+m} = x^m x^n \tag{2}$$

et

$$(x^m)^n = x^{mn} = (x^n)^m \tag{3}$$

Si G n'est pas abélien, pour $x, y \in G$ on a en général $(xy)^n \neq x^n y^n$. Cependant, si x et y commutent, alors $(xy)^n = x^n y^n$.
(e) Pour tout $x, y \in G$, $(x^{-1})^{-1} = x$ et $(xy)^{-1} = y^{-1}x^{-1}$.

Démonstration. — D'après la remarque 2.4, un groupe G a un unique élément neutre e et tout élément a un unique inverse. Le reste de la proposition est laissé au soin de l'étudiant. □

Remarque 3.6. — En notation additive les formules (1), (2) et (3) s'écrivent

$$\begin{aligned} nx &= x + x + \cdots x \\ nx + mx &= (n+m)x \\ n(mx) &= nmx \end{aligned}$$

4. Sous-groupes

Sauf mention contraire, G désigne toujours un groupe d'élément neutre e.

Définition 4.1. — *G étant un groupe, une partie non vide H de G est un* **sous-groupe** *de G, si*

1. $\forall x, y \in H$, $xy \in H$ *(H est stable par la loi de G)*
2. $\forall x \in H$, $x^{-1} \in H$ *(H est stable par passage à l'inverse).*

On écrira $H \leq G$ pour exprimer que H est un sous-groupe de G et $H < G$ si $H \leq G$ et $H \neq G$.

Remarque 4.2. — 1. Les conditions (1) et (2) de la définition impliquent que $e \in H$. En effet puisque H est non vide il contient un élément x, donc $x^{-1} \in H$ et $e = xx^{-1} \in H$. On en déduit que dans la définition la condition $H \neq \emptyset$ peut être remplacée par $e \in H$.

2. Si H est un sous-groupe de $(G, *)$, alors la loi de groupe $*$ sur G se restreint à H (par définition), et on vérifie que $(H, *)$ est un groupe.

3. Tous les sous-groupes d'un groupe G ont le même élément neutre e que G. En effet, $e \in H$ et est élément neutre pour la loi induite sur H.

4. Tout groupe G ayant plus d'un élément a au moins deux sous-groupes, G et $\{e\}$.

Remarque 4.3. — Insistons sur le premier point de la remarque précédente. La manière la plus simple de montrer que $(G, *)$ est un groupe est de souvent voir G comme un sous-groupe d'un groupe standard. Les groupes standard sont $(\mathbb{C}, +), (\mathbb{C}^\times, \times)$ et l'ensemble $\mathcal{S}(E)$ des bijections d'un ensemble quelconque E dans lui-même.

Par exemple, l'ensemble des automorphismes d'un espace vectoriel E est un sous-groupe de $\mathcal{F}(E)$.

Proposition 4.4. — *Soit H une partie de G. Pour que H soit un sous-groupe de G, il faut et il suffit que*

$$\begin{cases} e \in H\,; \\ \forall x, y \in H,\ \ xy^{-1} \in H\,. \end{cases} \tag{4}$$

Démonstration. — Supposons $H \leq G$, soit $(x, y) \in H \times H$, comme $y \in H$, $y^{-1} \in H$ d'après (2) de la définition 4.1; par suite $xy^{-1} \in H$ d'après (1) de la même définition.

Supposons maintenant (4) vérifiée et appliquons la pour e et un élément quelconque $x \in H$. On a et $x^{-1} = ex^{-1} \in H$. D'où la stabilité par passage à l'inverse. soit $(x, y) \in H \times H$, on a $(x, y^{-1}) \in H \times H$ et $xy = x(y^{-1})^{-1} \in H$, d'où la stabilité par la loi de G. □

Remarque 4.5. — En notation additive, la deuxième partie de la condition (4) s'écrit

$$\forall x, y \in H, \quad x - y \in H. \tag{5}$$

Exemples 4.6. — *1. Les ensembles $m\mathbb{Z}$, $m \in \mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$ et $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.*
2. G et $\{e\}$ sont des sous-groupes triviaux de G.
3. Si G est un groupe et H et K deux sous-groupes de G, alors le produit cartésien $H \times K$ est un sous-groupe du groupe $G \times G$.
4. L'ensemble $Z(G) = \{x \in G \ : \ \forall y \in G, \ xy = yx\}$ est un sous-groupe de G appelé **centre** *de G.*
5. L'ensemble $\mathbb{U} = \{z \in \mathbb{C}, \ |z| = 1\}$ des nombres complexes de module 1 est un sous-groupe de $\mathbb{C}^*$.
6. L'ensemble $\mathbb{U}_n = \{z \in \mathbb{C}, \ z^n = 1\}$ des racines nième de l'unité est un sous-groupe de $\mathbb{U}$ et donc de $\mathbb{C}^*$.
7. $\{e, \tau_{1,2}\}$ est un sous-groupe de $\mathfrak{S}_3$.

Définition 4.7. — *Soit H un sous-groupe d'un groupe G. On dit que H est un sous-groupe* **distingué** *(ou* **normal** *) de G et on note $H \triangleleft G$, si pour tout $x \in G$, $xHx^{-1} = H$ ou encore $xH = Hx$. Une autre formulation est encore :*

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H \, .$$

Exemples 4.8. — *1. Dans un groupe abélien, tout sous-groupe est distingué.*
2. Dans un groupe G, le centre $Z(G)$ est distingué.
3. $SO(n)$ est distingué dans $O(n)$.

5. Sous-groupes de $(\mathbb{Z}, +)$

Théorème 5.1 **(division euclidienne)**. — *Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que*

1. $a = bq + r$,
2. $0 \leq r < |b|$.

Démonstration. — On suppose que $b > 0$ et on pose

$$A = \{k \in \mathbb{Z}, \ bk \leq a\}.$$

Cet ensemble est non vide (pour $a \geq 0$, $0 \in A$ et pour $a < 0$, $a \in A$) et majoré (pour $a \geq 0$, a majore A et pour $a < 0$, 0 majore A). Il admet donc un plus grand élément a qui vérifie

$$qb \leq a < (q+1)b.$$

Il suffit alors de poser $r = a - bq$.

Pour $b < 0$ on travaille avec $-b$ et on a l'existence de (q', r') vérifiant $a = -bq' + r'$ et $0 \leq r' < -b$. Il suffit alors de poser $q = -q'$, $r = -r'$.

Pour l'unicité, supposons qu'il existe deux couples d'entiers (q, r) et (q', r') vérifiants 1. et 2. avec $q \neq q'$ On a alors

$$|r - r'| = |b(q - q')| \geq |b|$$

avec r et r' dans $]-|b|, |b|[$, ce qui est impossible. On a donc $q = q'$ et puis $r = r'$. □

Proposition 5.2. — *Les sous-groupes du groupe additif $(\mathbb{Z}, +)$ sont les sous-ensembles $m\mathbb{Z}$, où $m \in \mathbb{N}$.*

Démonstration. — Il est clair que les ensembles $m\mathbb{Z}$ pour $m \in \mathbb{N}$ sont des sous-groupes de $\mathbb{Z}$. Inversement, soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$; sinon, il existe dans H un entier a non nul et l'un des entiers a ou $-a$ est dans $H^+ = H \cap \mathbb{N}^*$. L'ensemble H^+ est donc une partie non vide de $\mathbb{N}^*$ et en conséquence admet un plus petit élément $m \geq 1$. Comme $m \in H$ et H est un groupe additif, on a $m\mathbb{Z} \subset H$. D'autre part, pour tout $x \in H$, la division euclidienne par m donne $x = qm + r$ avec $r = x - mq \in H^+$ (car $x, mq \in H$) et $r \leq m - 1$, ce qui impose $r = 0$ par définition de m. On a donc $H \subset m\mathbb{Z}$ et $H = m\mathbb{Z}$. □

6. Sous-groupe engendré par une partie

Proposition 6.1. — *Soit G un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes (resp. de sous-groupes distingués) de G. Alors $H = \cap_{i \in I} H_i$ est un sous-groupe (resp. sous-groupe distingué) de G.*

Démonstration. — On $e \in H = \cap_{i \in I} H_i$ et pour tout $x, y \in G$,

$$\begin{aligned} x, y \in H &\Rightarrow \forall i \in I,\ x, y \in H_i \\ &\Rightarrow \forall i \in I,\ xy^{-1} \in H_i \quad \text{car } H_i \leq G \\ &\Rightarrow xy^{-1} \in H. \end{aligned}$$

Donc H est un sous-groupe de G. Supposons H_i distingué dans G pour tout $i \in I$. Alors, pour tout $x \in G$,

$$xHx^{-1} = x(\cap_{i \in I} H_i)x^{-1} = \cap_{i \in I} xH_ix^{-1} = \cap_{i \in I} H_i = H.$$

Ainsi H est distingué dans G. □

Remarque 6.2. — La réunion de deux groupes de G n'est pas nécessairement un sous-groupe de G.
Par exemple $2\mathbb{Z}$ et $3\mathbb{Z}$ sont deux sous-groupes de $(\mathbb{Z}, +)$, mais la réunion ne l'est pas puisque 2 et 3 sont dans $2\mathbb{Z} \cup 3\mathbb{Z}$ alors que $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Corollaire 6.3. — *Si X est une partie d'un groupe G, l'intersection de tous les sous-groupes de G qui contiennent X est un sous-groupe de G (qui contient X).*

Définition 6.4. — *Si X est une partie d'un groupe G, le sous-groupe de G engendré par X est l'intersection de tous les sous-groupes de G qui contiennent X. C'est le plus petit (pour l'inclusion) sous-groupe de G contenant X. On le note $\langle X \rangle$.*

Si X est réduit un seul élément, $X = \{a\}$, alors

$$\langle X \rangle = \langle a \rangle = \{a^k \ , \ k \in \mathbb{Z}\}$$

où $a^k := aa \cdots a$, k-fois. En notation additive,

$$\langle X \rangle = \langle a \rangle = \{ka \ , \ k \in \mathbb{Z}\}$$

où $ka := a + \cdots + a \cdots a$, k-fois.

Si $\langle X \rangle = G$, on dit que X est un **système de générateurs** de G ou que X **engendre** G.

Si G est engendré par un élément $a \in G$, on dit que G est un groupe **monogène**. Un groupe monogène fini est appelé **groupe cyclique**.
Les groupes monogènes et en particulier les groupes cycliques seront étudiées en détails au chapitre 3.

Proposition 6.5. — *Soient G un groupe et X, Y deux parties de G.*

(a) On a $X \subset \langle X \rangle$ et l'égalité est réalisée si, et seulement si, X est un sous-groupe de G.

(b) Si $X \subset Y$, alors $\langle X \rangle \subset \langle Y \rangle$.

(c) En notant, pour X non vide, X^{-1} l'ensemble des inverses des éléments de X, soit $X^{-1} = \{x^{-1}, \ x \in X\}$, les éléments de $\langle X \rangle$ sont de la forme $x_1 x_2 \cdots x_n$ où $n \in \mathbb{N}^*$ et les x_k sont dans $X \cup X^{-1}$ pour tout k, $1 \leq k \leq n$.

Démonstration. — Les points (a) et (b) se déduisent immédiatement de la définition.

Pour (c), posons

$$H = \{x_1 x_2 \cdots x_n \ : n \in \mathbb{N} \text{ et } x_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq n\}$$

Il est clair que cet ensemble est un sous-groupe de G; il contient bien évidemment X. De plus, si H' est un sous-groupe de G quelconque contenant X, il doit contenir tous les éléments de X, tous leurs inverses, et tous les produits d'éléments de X et leurs inverses, donc il doit contenir H. Ainsi

H est bien le plus petit sous-groupe de G contenant X. On a donc $H = \langle X \rangle$. □

Du point (c) de la Proposition 6.5, il découle que si les éléments de X commutent deux à deux, alors le sous-groupe engendré par X est abélien.

Exemples 6.6. — 1. Le sous-groupe de $\mathbb{Z}$ engendré par $X = \{n\}$ est $n\mathbb{Z}$.
2. Le sous-groupe de $\mathbb{Z}$ engendré par $X = \{n, m\}$ est $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, où $d = \text{pgcd}(n, m)$.
3. Le sous-groupe de $\mathbb{C}^*$ engendré par $\xi = e^{2i\pi/n}$ est $\mathbb{U}_n$.

7. Quotient par un sous-groupe

Proposition 7.1. — *Soit G un groupe et H un sous-groupe de G. La relation $\mathcal{R}$ définie par $x\mathcal{R}y \iff y^{-1}x \in H$ est une relation d'équivalence sur G. Si $x \in G$, la classe d'équivalence de x (dite la classe à gauche de x) est l'ensemble $xH = \{xh \ : \ h \in H\}$ (en particulier la classe de e est H). L'ensemble quotient $G/\mathcal{R}$ est noté G/H.*

Démonstration. — Soit $x \in H$, on a $x^{-1}x = e \in H$, donc $x\mathcal{R}x$ d'où la réflexivité de la relation. Soient $x, y \in H$. Si $x\mathcal{R}y$ alors $y^{-1}x \in H$ et $x^{-1}y = (y^{-1}x)^{-1} \in H$, autrement dit $y\mathcal{R}x$, d'où la symétrie de la relation. Soient $x, y, z \in H$. Si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $z^{-1}x = z^{-1}yy^{-1}x \in H$, donc $x\mathcal{R}z$, d'où la transitivité de la relation. □

On montre de même

Proposition 7.2. — *La relation $\mathcal{R}'$ définie par $x\mathcal{R}'y \iff xy^{-1} \in H$ est une relation d'équivalence sur G. Si $x \in G$, la classe d'équivalence de x (dite la classe à droite de x) est l'ensemble $Hx = \{hx \ : \ h \in H\}$ (en particulier la classe de e est H). L'ensemble quotient $G/\mathcal{R}'$ est noté $H\backslash G$.*

L'application $\Phi : x \mapsto x^{-1}$ est une bijection de G sur G. Elle vérifie $\Phi \circ \Phi = \text{Id}_G$ et $\Phi(H) = H$. On a $\Phi(xH) = Hx^{-1}$ donc Φ induit une bijection de l'ensemble des classes à gauche G/H sur l'ensemble des classes à droite $H\backslash G$. Ces deux ensembles ont donc le même cardinal.

Si $H = \{e\}$, alors $G/H = H\backslash G = G$.

Définition 7.3. — *Le cardinal commun aux ensembles G/H et $H\backslash G$ s'appelle* **indice** *de H dans G. Nous le noterons $[G : H]$.*

***Théorème 7.4* (de Lagrange).** — *Soit G un groupe fini et H un sous-groupe de G. Alors on a*

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

et en particulier $|H|$ divise $|G|$.

Démonstration. — Les éléments de G/H sont les classes d'équivalences xH; elles sont toutes de cardinal $|H|$ (cardinal de H), car l'application $H \to xH$, $h \mapsto xh$ est bijective, elles forment une partition de G et sont au nombre de $\mathrm{Card}(G/H) = [G : H]$. Donc

$$|G| = \mathrm{Card}(\cup_{xH \in G/H}(xH)) = \textstyle\sum_{xH \in G/H} \mathrm{Card}(xH) = \sum_{xH \in G/H} |H| = \mathrm{Card}(G/H) \times |H|.$$

D'où la formule de Lagrange. □

La réciproque du théorème de Lagrange est fausse, à savoir, si G est un groupe d'ordre n et si d est un diviseur de n, alors G n'admet pas nécessairement un sous-groupe d'ordre d.

Définition 7.5. — *Soit $\mathcal{R}$ une relation d'équivalence sur un groupe G. On dit que $\mathcal{R}$ est* **compatible** *avec la loi de groupe si on a l'implication :*

$$\forall g, g', h, h' \in G,\ g\mathcal{R}g' \text{ et } h\mathcal{R}h' \Rightarrow gh\,\mathcal{R}\,g'h'\,.$$

Proposition 7.6. — *Considérons un groupe G, un sous-groupe H de G et les relations d'équivalences $\mathcal{R}$ et $\mathcal{R}'$ introduites dans les propositions 7.1 et 7.2. Les conditions suivantes sont équivalentes*

1. *$\mathcal{R}$ est compatible avec la loi de G.*
2. *$\mathcal{R}'$ est compatible avec la loi de G.*
3. *$\mathcal{R} = \mathcal{R}'$.*
4. *$xH = Hx$ pour tout $x \in G$.*
5. *H est distingué dans G.*

Si l'une de ces conditions est vérifiée, le quotient G/H muni de la loi quotient $(xH)(yH) = (xy)H$, est un groupe.

Démonstration. — 1. $\Rightarrow$ 3. Supposons $\mathcal{R}$ compatible avec la loi de G. Alors $x\mathcal{R}y \iff y^{-1}x \in H \iff y^{-1}x\mathcal{R}e \Rightarrow y(y^{-1}x)y^{-1}\mathcal{R}yey^{-1} \iff xy^{-1}\mathcal{R}e \iff xy^{-1} \in H \iff x\mathcal{R}'y$. De manière analogue, on montre que $x\mathcal{R}'y \Rightarrow x\mathcal{R}y$ et donc $\mathcal{R} = \mathcal{R}'$.
2. $\Rightarrow$ 3. se montre de la même façon.
3. $\iff$ 4. car pour chaque $x \in G$, la classe xH modulo $\mathcal{R}$ est égale à la classe Hx modulo $\mathcal{R}'$.
4. $\iff$ 5. Évident.
5. $\Rightarrow$ 1. Si $x\mathcal{R}x'$ et $y\mathcal{R}y'$, alors il existe $h, h' \in H$ tels que $x = x'h$ et $y = y'h'$.

Donc $xy = x'hy'h' = x'y'(y'^{-1}hy')h'$ et par suite $xy \in x'y'H$, d'où $xy\mathcal{R}x'y'$. Enfin nous vérifions facilement que muni de la loi quotient, G/H est un groupe. □

8. Homomorphismes de groupes

Définition 8.1. — *Soient G et G' deux groupes. On appelle* **homomorphisme** *(ou* **morphisme***) de groupes de G dans G', une application f de G dans G' telle que,*

$$\forall x, y \in G,\ f(xy) = f(x)f(y).$$

On note $\mathrm{Hom}(G, G')$ l'ensemble des homomorphismes de G dans G'. Il existe au moins un homomorphisme de G dans G', l'homomorphisme trivial $f_0 : x \mapsto e'$ où e' est l'élément neutre de G'.

Un homomorphisme de G dans G est un **endomorphisme** de G. On note $\mathrm{End}(G)$ l'ensemble des endomorphismes de G.

On dit que $f \in \mathrm{Hom}(G, G')$ est un **isomorphisme** si f est bijectif; dans ce cas la bijection réciproque f^{-1} est un isomomorphisme de G' sur G. S'il existe un isomorphisme de G sur G' on dit que les groupes G et G' sont **isomorphes**. Nous écrivons $G \simeq G'$.

On appelle **automorphisme** de G, un isomorphisme de G sur G. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. On montre que $\mathrm{Aut}(G)$ muni de la composition des applications est un groupe d'élément neutre Id_G.

Pour tout $x \in G$, l'application $\tau_x : y \mapsto xyx^{-1}$ est bijective de G sur G, d'application réciproque $\tau_{x^{-1}} : y \mapsto x^{-1}yx$. C'est aussi un homomorphisme, donc un automorphisme de G. On l'appelle **automorphisme intérieur**. On note $\mathrm{Int}(G)$ ou $\mathrm{Ad}(G)$ l'ensemble $\{\tau_x\ :\ x \in G\}$ des automorphismes intérieurs de G.

Exemple 8.2. —
1. La fonction exponentielle est un isomorphisme des groupes de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$.
2. La fonction logarithme népérien est un isomorphisme de groupes de $(\mathbb{R}_+^*, \times)$ sur $(\mathbb{R}, +)$.
3. La fonction trace est un morphisme de groupes de $(\mathcal{M}_n(\mathbb{R}), +)$ dans $(\mathbb{R}, +)$.
4. La fonction déterminant est un morphisme de groupes de $(GL_n(\mathbb{R}), \times)$ dans $(\mathbb{R}^*, \times)$.

Remarque 8.3. — Une bijection f d'un groupe G sur un ensemble X permet de transporter la structure de G sur X : on définit une loi de composition interne $*$ sur X en posant pour tout $x, y \in X$

$$x * y = f\Big(f^{-1}(x)f^{-1}(y)\Big).$$

Muni de cette opération, X est un groupe et f est un isomorphisme de G sur X. Nous donnons ici quelques applications de cette propriété :

1. La loi $x\star y = \frac{x+y}{1+xy}$ définit une structure de groupe sur $X =]-1,1[$. En effet, la fonction $f(x) = \tanh(x) = \frac{e^x-e^{-x}}{e^x+e^{-x}}$ réalise une bijection du groupe additif $\mathbb{R}$ sur l'ensemble $X =]-1,1[$, de bijection réciproque argtanh et on a
$$\begin{aligned} x\star y &= f(f^{-1}(x)+f^{-1}(y)) \\ &= \tanh(\operatorname{argtanh}(x)+\operatorname{argtanh}(y)) \\ &= \frac{\tanh(\operatorname{argtanh}(x))+\tanh(\operatorname{argtanh}(y))}{1+\tanh(\operatorname{argtanh}(x))\tanh(\operatorname{argtanh}(y))} \\ &= \frac{x+y}{1+xy}. \end{aligned}$$
2. La loi $x\star y = \arctan(\tan(x)+\tan(y))$ définit une structure de groupe sur $]-\frac{\pi}{2},\frac{\pi}{2}[$. En effet la fonction $f(x) = \arctan(x)$ réalise une bijection du groupe additif $\mathbb{R}$ sur l'ensemble $X =]-\frac{\pi}{2},\frac{\pi}{2}[$, de bijection réciproque tan et on a
$$\begin{aligned} x\star y &= f(f^{-1}(x)+f^{-1}(y)) \\ &= \arctan(\tan(x)+\tan(y)). \end{aligned}$$
3. Pour tout entier $n \geq 1$ impair, la loi $x\star y = \sqrt[n]{x^n+y^n}$ définit une structure de groupe abélien sur $\mathbb{R}$. En effet, la fonction $f : x \mapsto \sqrt[n]{x}$ est une bijection du groupe additif $\mathbb{R}$ sur l'ensemble $\mathbb{R}$ pour n impair, son inverse étant la fonction $x \mapsto x^n$ et on a
$$x\star y = \sqrt[n]{x^n+y^n} = f(f^{-1}(x)+f^{-1}(y)).$$

Proposition 8.4. — *Soient G, G' deux groupes, d'éléments neutres e, e' et soit $f \in Hom(G,G')$. On a*

1. *$f(e) = e'$.*
2. *Pour tout $x \in G$ on a $f(x^{-1}) = f(x)^{-1}$.*
3. *Pour tout $x \in G$ et pour tout $k \in \mathbb{Z}$, $f(x^k) = f(x)^k$.*

Démonstration. — 1. On a $f(e)^2 = f(e^2) = f(e) = f(e)e'$, donc $f(e) = e'$ puisque dans un groupe tout élément est régulier.

2. Pour tout $x \in G$, $xx^{-1} = x^{-1}x = e$, donc $f(x)f(x^{-1}) = f(x^{-1})f(x) = f(e) = e'$, d'où $f(x^{-1}) = f(x)^{-1}$.

3. On montre par récurrence, que $f(x^k) = f(x)^k$ pour tout $k \in \mathbb{N}$, puis pour tout $k \in \mathbb{Z}$. □

Proposition 8.5. — *Soient G, G' deux groupes, d'éléments neutres e, e' et soit $f \in Hom(G,G')$.*

1. *Si H est un sous-groupe de G, alors $f(H)$ est un sous-groupe de G'. En particulier, l'ensemble* $\operatorname{Im}(f) = f(G)$ *appelé* **image de** *f est un sous-groupe de G'.*

2. *Si H' est un sous-groupe de G', alors $f^{-1}(H') = \{x \in G \ : \ f(x) \in H'\}$ est un sous-groupe de G. Si H' est distingué dans G', alors $f^{-1}(H')$ est distingué dans G.*
   En particulier, l'ensemble $\mathrm{Ker}(f) = \{x \in G \ : \ f(x) = e'\}$ *appelé* **noyau** *de f est un sous-groupe distingué de G.*
3. *Pour que f soit injectif, il faut et il suffit que* $\mathrm{Ker}(f) = \{e\}$.

Démonstration. — 1. On a $e' = f(e) \in f(H)$. D'autre part, soit $y, y' \in f(H)$, alors il existe $x, x' \in H$ tels que $f(x) = y$ et $f(x') = y'$. D'où $yy'^{-1} = f(x)f(x')^{-1} = f(xx'^{-1}) \in f(H)$ puisque $xx'^{-1} \in H$ car H est un sous-groupe de G. On en déduit que $f(H)$ est un sous-groupe de G'.

Le deuxième point de la proposition est laissé comme exercice aux étudiants.

Pour le troisième point, on remarque qu'indépendemment du fait que f soit injectif, $f(e) = e'$ donc $\{e\} \subset \mathrm{Ker}(f)$. Si f est injectif, alors l'équation $f(x) = e' = f(e)$ implique $x = e$, de sorte qu'on a l'autre inclusion $\mathrm{Ker}(f) \subset \{e\}$. Si on a $\mathrm{Ker}(f) \subset \{e\}$, soit $x, y \in G$ tels que $f(x) = f(y)$. Alors $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e'$. Ainsi, $xy^{-1} \in \mathrm{Ker}(f)$, l'hypothèse donne donc $xy^{-1} = e$ et ainsi $x = y$. Ceci montre l'injectivité de f. □

Exemple 8.6. — 1. L'application $\det : A \mapsto \det(A)$ est morphisme de groupes de $(GL_n(\mathbb{R}), \times)$ dans $(\mathbb{R}^*, \times)$. Son noyau $\mathrm{Ker}(\det) = SL_n(\mathbb{R})$ est un sous-groupe distingué de $(GL_n(\mathbb{R}), \times)$.

2. L'application $\varphi : \theta \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(SL_2(\mathbb{R}), \times)$. Son image $\mathrm{Im}(\varphi) = SO_2(\mathbb{R})$ est un sous-groupe abélien de $(SL_2(\mathbb{R}), \times)$.

Proposition 8.7. — *Soient G, G' deux groupes et $f \in Hom(G, G')$. Pour toute partie non vide A de G, on a*

$$f^{-1}(f(A)) = A\,\mathrm{Ker}(f) = \mathrm{Ker}(f)A. \tag{6}$$

Démonstration. — On a $x \in f^{-1}(f(A)) \iff f(x) \in f(A) \iff \exists a \in A,\ f(a) = f(x) \iff \exists a \in A,\ f(a^{-1}x) = e \iff \exists a \in A,\ a^{-1}x \in \mathrm{Ker}(f) \iff \exists a \in A,\ x \in a\,\mathrm{Ker}(f) \iff x \in A\,\mathrm{Ker}(f)$. Donc $f^{-1}(f(A)) = A\,\mathrm{Ker}(f)$.
□

En notation additive, (6) s'écrit

$$f^{-1}(f(A)) = A + \mathrm{Ker}(f) = \mathrm{Ker}(f) + A.$$

Proposition 8.8. — *Soient G et G' deux groupes et soit $f \in Hom(G, G')$. Soit $H \leq G$ un sous-groupe de G. Alors, f passe au quotient en une application $\bar{f} : G/H \to G'$ si et seulement si $H \subset \mathrm{Ker}(f)$.*

Si, de plus, H est distingué, alors $\bar{f}$ est un morphisme de groupes pour la structure de groupe sur G/H définie par la Proposition 7.6.

Démonstration. — La proposition 1.5 nous assure qu'il existe une application $\bar{f} : G/H \to G'$ telle que $\bar{f} \circ p = f$ si et seulement si f est constante sur toutes les classes $\bar{x} = xH$ modulo H. Cette condition est équivalente à la condition de l'énoncé $H \subset \mathrm{Ker}(f)$. En effet, si elle est vérifiée, alors elle l'est pour $x = e$, donc f est constante sur $eH = H$. On en déduit que pour tout $h \in H$, on a $f(h) = f(e) = e'$, de sorte que $h \in \mathrm{Ker}(f)$. Si réciproquement, $H \subset \mathrm{Ker}(f)$, alors pour $g, g' \in \overline{x} = xH$, on a l'existence de $h \in H$ tel que $g' = gh$. On a alors $f(g') = f(gh) = f(g)f(h) = f(g)$, car $h \in \mathrm{Ker}(f)$. La première partie de la proposition est donc démontrée.

Si la condition est vérifiée et que H est distingué dans G, on a par définition de la structure de groupe sur G/H,

$$\bar{f}(\bar{x}\bar{y}) = \bar{f}(\overline{xy}) = f(xy) = f(x)f(y) = \bar{f}(\bar{x})\bar{f}(\bar{y}).$$

Ceci montre que $\bar{f}$ est un morphisme de groupes. □

***Théorème 8.9* (Factorisation canonique).** — *Soient G et G' deux groupes et soit $f \in Hom(G, G')$. Alors il existe une unique application*

$$\bar{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$$

vérifiant $\forall x \in G$, $\bar{f}(x\,\mathrm{Ker}(f)) = f(x)$. L'application $\bar{f}$ est un isomorphisme de groupes. On a alors $G/\mathrm{Ker}(f) \simeq f(G)$. Si G est fini, on a

$$|G| = |\mathrm{Ker}(f)| \cdot |f(G)|.$$

En particulier, si G est fini, alors l'ordre de $f(G)$ et l'ordre de $\mathrm{Ker}(f)$ divisent $|G|$. Si G' est fini, alors $|f(G)|$ divise $|G'|$, par le théorème de Lagrange (Théorème 7.4).

Démonstration. — Comme $\mathrm{Ker}(f) \triangleleft G$, la Proposition 8.8 nous assure qu'il existe un morphisme de groupes $\bar{f} : G/\mathrm{Ker}(f) \to G'$ unique, tel que $\bar{f} \circ p = f$ et $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$. La surjectivité de $\bar{f}$ est évidente par construction et $\mathrm{Ker}(\bar{f}) = p(\mathrm{Ker}(f)) = \{\bar{e}\}$, d'où l'injectivité.

Lorsque G et G' sont finis, l'isomorphisme donne $\frac{|G|}{|\mathrm{Ker}(f)|} = |f(G)|$, soit $|G| = |\mathrm{Ker}(f)| \cdot |f(G)|$, d'où le fait que $|G|$ soit divisible par $|\mathrm{Ker}(f)|$ et par $|f(G)|$. □

Le Théorème 8.9 permet de retrouver le Théorème de Lagrange (Théorème 7.4) dans le cas où H est distingué : on l'applique au morphisme quotient canonique $p : G \longrightarrow G/H$, dont le noyau est exactement H et l'image G/H.

Exemples 8.10. — (a) Soit $n \geq 2$ un entier. $SO_n(\mathbb{R})$ est un sous-groupe distingué de $O_n(\mathbb{R})$ comme noyau du morphisme de groupes det : $O_n(\mathbb{R}) \to \{-1, 1\}$. Comme cette application est surjective, on a

$$O_n(\mathbb{R})/SO_n(\mathbb{R}) \simeq \{-1, 1\}$$

On en déduit que $SO_n(\mathbb{R})$ est un sous-groupe distingué de $O_n(\mathbb{R})$ d'indice 2.

(b) L'application $f = x \mapsto e^{2i\pi x}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$. Son image est $\mathrm{Im}(f) = \mathbb{U}$ et son noyeau est $\mathrm{Ker}(f) = \mathbb{Z}$. On en déduit que le groupe $\mathbb{R}/\mathbb{Z}$ est isomorphe à $\mathbb{U}$:

$$\mathbb{R}/\mathbb{Z} \simeq \mathbb{U}.$$

Proposition 8.11. — *Soient G un groupe, H et K deux sous-groupes distingués de G tels que $K \subset H$. Alors*

(a) H/K est un sous-groupe distingué de G/K.

(b) Les deux groupes quotient $(G/K)/(H/K)$ et G/H sont isomorphes.

Démonstration. — Soient $x \in G$. Notons $\bar{x} = xH$ la classe de x modulo H, et $\dot{x} = xK$ la classe de x modulo K. Considérons la surjection canonique $f : G \to G/H$, $x \mapsto \bar{x}$. On a $K \subset H = \mathrm{Ker}(f)$, donc il existe un morphisme $\bar{f} : G/K \to G/H$ tel que $\bar{f}(\dot{x}) = \bar{x}$ pour tout $x \in G$. f est surjectif, puisque $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f) = G/H$. De plus $\mathrm{Ker}(\bar{f}) = \{\dot{x},\ x \in H\} = H/K$, (c'est donc un sous-groupe distingué de G/H). Par conséquent, d'après le théorème 8.9 $(G/H)/\mathrm{Ker}(\bar{f})$ est isomorphe $\mathrm{Im}(\bar{f})$, d'où l'isomorphisme demandé. □

9. Ordre d'un élément

Proposition 9.1. — *Soit G un groupe $a \in G$.*

1. *Si $|\langle a\rangle| = \infty$, alors $\langle a\rangle \simeq \mathbb{Z}$.*
2. *Si $|\langle a\rangle| = n \in \mathbb{N}$, alors:*
   - *(a) $\langle a\rangle \simeq \mathbb{Z}/n\mathbb{Z}$;*
   - *(b) $\langle a\rangle = \{a^k \mid k = 0, \ldots, n-1\}$;*
   - *(c) $\{k \mid a^k = e\} = n\mathbb{Z}$.*
   - *(d) n est le plus petit entier k strictement positif tel que $a^k = e$.*

Le cardinal de $\langle a\rangle$ est appelé ordre de a. *Il est donc infini dans le cas* 1., *et égal à n dans le cas* 2.

Démonstration. — L'application $f : \mathbb{Z} \to G$, $k \mapsto a^k$ est un homomorphisme de groupes, car $f(k+k') = a^{k+k'} = a^k a^{k'} = f(k)f(k')$. De plus $\mathrm{Im}(f) = \{a^k : k \in \mathbb{Z}\} = \langle a\rangle$. On en déduit que f est un morphisme de groupes surjectif de $\mathbb{Z}$ sur $\langle a\rangle$.

Le noyau $\mathrm{Ker}(f)$ est un sous-groupe de $\mathbb{Z}$, donc d'après la proposition 5.2, il existe $n \in \mathbb{N}$ tel que $\mathrm{Ker}(f) = n\mathbb{Z}$. Si $n = 0$, alors f est injective, et par

suite un isomorphisme de $\mathbb{Z}$ sur $\langle a\rangle$. Si $n \neq 0$, par factorisation canonique de f à travers son noyau $n\mathbb{Z}$, on obtient un isomorphisme $\bar{f}$ de $\mathbb{Z}/n\mathbb{Z}$ sur $\langle a\rangle$. On obtient le diagramme commutatif $\begin{array}{ccc} \mathbb{Z} & & \\ \downarrow p & \searrow^{f} & \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\bar{f}} & \langle a\rangle \end{array}$ Puisque $\bar{f}$ est un isomomorphisme, le noyau de f coïncide avec le noyau de p, soit $n\mathbb{Z}$, c'est à dire l'ensemble des multiples de n. Finalement, comme $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f) = \langle a\rangle$, on a $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. □

Corollaire 9.2. — *Soit G un groupe, $a \in G$, et m un entier. Alors l'ordre de a divise m si et seulement si $a^m = e$.*

Démonstration. — Notant n l'ordre de a, on utilise le point (c) de la Proposition 9.1 sous la forme

$$\{k : a^k = e\} = n\mathbb{Z}\,.$$

Or, m est dans l'ensemble de gauche lorsque $a^m = e$ et dans l'ensemble de droite lorsque n divise m. Ces deux conditions sont donc bien équivalentes. □

Corollaire 9.3. — *Soit p un nombre premier et G un groupe d'ordre p. Alors $G \simeq \mathbb{Z}/p\mathbb{Z}$.*

Démonstration. — Soit $x \in G$ avec $x \neq e$. Alors $o(x) \neq 1$. De plus, par le théorème de Lagrange, $o(x)|p$. Donc $o(x) = p$. On a alors $G = \langle x\rangle \simeq \mathbb{Z}/p\mathbb{Z}$ par la Proposition 9.1. □

Corollaire 9.4. — *Dire que $a \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que $a^n = e$ et $a^k \neq e$ pour tout entier k, $1 \leq k \leq n-1$.*

Corollaire 9.5. — *Soit G un groupe fini. Alors tout élément de G est d'ordre fini divisant l'ordre de G. En particulier, $\forall a \in G$, $a^{|G|} = e$.*

Démonstration. — Soit $a \in G$, l'ordre de a est l'ordre du sous-groupe $\langle a\rangle$ engendré par a. Donc d'après le théorème de Lagrange l'ordre de ce sous-groupe divise l'ordre de G. D'où le corollaire.
□

Exemple 9.6. —
1. Dans tout groupe G, l'élément neutre est le seul élément d'ordre 1.
2. Dans $(\mathbb{Z}, +)$, tout élément $x \neq 0$ est d'ordre infini.
3. Dans le groupe symétrique S_3, $\tau_{2,3}$ est d'ordre 2.