**Frank Pacard, Raphaël Danchin, Stéphane Jaffard**
**Université Paris Est-Créteil**

---

# ALGÈBRE

# LICENCE 3

---

# ALGÈBRE

## LICENCE 3

**Frank Pacard, Raphaël Danchin, Stéphane Jaffard**
**Université Paris Est-Créteil**

**Avertissement:** Ces notes de cours viennent en appui du cours de Structures Métriques enseigné en L2-L3 à l'UPEC. Le cours proprement dit peut toutefois légèrement différer de ces notes.

# TABLE DES MATIÈRES

# CHAPITRE 1

# GROUPES

## 1.1. Définition

Soit $G$ un ensemble. Une *loi de composition interne* $*$ sur $G$ est une application de $G \times G$ à valeurs dans $G$. Pour tout $x, y \in G$, on note $x * y \in G$ l'image du couple $(x, y) \in G \times G$.

**Exemples de lois de composition interne:**

- Sur $\mathbb{N}$, l'addition et la multiplication sont des lois de composition internes. Ce n'est pas le cas de la soustraction.
- Sur $\mathbb{R}$, l'addition, la soustraction ou la multiplication sont des lois de composition internes.
- Sur $\mathbb{R}^*$, l'addition n'est pas une lois de composition interne, mais la multiplication en est une.
- Sur $\mathbb{R}^{*,+}$, l'addition, la multiplication et la division sont des lois de composition internes. Mais ce n'est pas le cas de la soustraction.
- Soit $E$ un ensemble et $\mathcal{P}(E)$ l'ensemble des parties de $E$. L'union, l'intersection et la différence symétrique (définie par $A\Delta B = A \cup B - A \cap B$) sont des lois de composition internes.

***Définition 1.1***. — *On dit que l'ensemble $G$, muni de la loi de composition interne $*$, est un* groupe *si les trois propriétés suivantes sont vérifiées :*

(i) *la loi $*$ est* associative*, c'est-à-dire que*

$$\forall (x, y, z) \in G^3, \qquad (x * y) * z = x * (y * z)\,;$$

(ii) *la loi $*$ admet un* élément neutre *(noté $e$) vérifiant*

$$\forall x \in G\,, \qquad x * e = e * x = x\,;$$

(iii) *tout élément de $G$ admet un* symétrique *pour la loi $*$, c'est-à-dire que*

$$\forall x \in G, \quad \exists\, x' \in G, \quad \text{tel que} \qquad x * x' = x' * x = e\,.$$

*Si de plus la loi $*$ est* commutative*, c'est-à-dire que*

$$\forall (x,y) \in G^2,\ x * y = y * x,$$

*on dit que le groupe est* commutatif *ou* abélien.

*On dit que le groupe $(G,*)$ est* fini *si $G$ a un nombre fini d'éléments.*

***Remarque 1.1***. — *En général, le symétrique $x'$ de l'élément $x \in G$ est noté $x^{-1}$. Ainsi on aura $x^{-1} * x = x * x^{-1} = e$.*
*Lorsque la loi $*$ est notée $\cdot$ ou $\times$ (notation multiplicative), le symétrique d'un élément $x$ est noté $x^{-1}$ et appelé* inverse de $x$*, l'élément neutre est noté* $1$*.*
*Lorsque la loi $*$ est notée $+$ (notation additive), le symétrique d'un élément $x$ est noté $-x$ et appelé* opposé de $x$*, l'élément neutre est noté* $0$*. La notation additive est réservée aux groupes commutatifs.*

**Exemples de groupes:**

- Pour l'addition: $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ et $(\mathbb{C},+)$,
- Pour la multiplication: $(]0,+\infty[,\cdot),(\mathbb{Q}^*,\cdot),(\mathbb{R}^*,\cdot),(\mathbb{R}^{*,+},\cdot)$ et $(\mathbb{C}^*,\cdot)$.
- Pour la multiplication: Le cercle unité $U \subset \mathbb{C}$; les racines n-ièmes de l'unité: $U_n = \{e^{2ik\pi/n}\}$ pour $k = 0, \cdots n-1$.
- Pour la composition: L'ensemble des bijections de $E$ dans $E$.
- L'ensemble des matrice $n \times n$ à coefficients réels et inversibles (pour le produit des matrices), noté $GL_n(\mathbb{R})$.

***Proposition 1.1***. — *Soit $(G,*)$ un groupe. L'élément neutre $e$ de $G$ pour la loi $*$ est unique et, pour tout $x \in G$, le symétrique de $x$ dans $G$, pour la loi $*$, est unique.*

*Démonstration.* — Commençons par démontrer que l'élément neutre de $(G,*)$ est unique. On note $e$ un élément neutre de $(G,*)$. Soit $e'$ un élément de $G$ qui vérifie aussi

$$\forall x \in G, \qquad x * e' = e' * x = x\,.$$

En prenant $x = e$ dans l'égalité ci-dessus, on trouve

$$e * e' = e\,.$$

Mais, $e$ étant un élément neutre de $G$, on a aussi $e * e' = e'$. Donc, $e' = e$ ce qui démontre l'unicité de l'élément neutre de $(G,*)$.

Montrons maintenant que le symétrique d'un élement $x$ de $G$ est unique. Soit $x \in G$ et $x', x''$ deux élements de $G$ vérifiant

$$x * x' = x' * x = e \qquad \text{et} \qquad x * x'' = x'' * x = e\,.$$

En utilisant la seconde série d'égalités, on peut écrire

$$x' * (x * x'') = x' * e = x'\,,$$

et, en utilisant la première série d'égalités, on peut aussi écrire

$$(x' * x) * x'' = e * x'' = x'' .$$

La loi $*$ étant associative, on conclut que

$$x' = x' * (x * x'') = (x' * x) * x'' = x'' .$$

D' où l'unicité du symétrique de $x$. □

Le résultat qui suit est une simple conséquence de l'unicité du symétrique d'un élément d'un groupe.

***Proposition 1.2.*** — *Soit $(G, *)$ un groupe. Pour tout $x, y \in G$, on a l'égalité*

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

*Démonstration.* — D'après le résultat de la Proposition précédente, il suffit simplement de vérifier que $y^{-1} * x^{-1}$ est bien *un* symétrique (et donc en fait *le* symétrique) de $x * y$. Pour cela, on calcule en utilisant l'associativité de la loi $*$

$$\begin{aligned} (x * y) * (y^{-1} * x^{-1}) &= ((x * y) * y^{-1}) * x^{-1} \\ &= ((x * (y * y^{-1})) * x^{-1} \\ &= (x * e) * x^{-1} \\ &= x * x^{-1} \\ &= e . \end{aligned}$$

On montre de la même manière que $(y^{-1} * x^{-1}) * (x * y) = e$, ce qui prouve que $y^{-1} * x^{-1}$ est bien le symétrique de $x * y$. □

Soit $(G, *)$ un groupe. La loi $*$ étant associative, pour tout $n \in \mathbb{N} \setminus \{0\}$ et pour tout $x_1, \ldots, x_n \in G$, on peut définir par récurrence sur $n \in \mathbb{N} \setminus \{0\}$

$$x_1 * \ldots * x_n = (x_1 * \ldots * x_{n-1}) * x_n .$$

Ainsi, l'associativité de la loi $*$ permet de s'affranchir de l'utilisation des parenthèses dans l'écriture de $x_1 * (x_2 * (\ldots * x_n))$.

**Notation:** On convient que $x^0 = e$ et on peut définir par récurrence sur $n \in \mathbb{N}$

$$x^{n+1} = x * x^n = x^n * x .$$

Autrement dit, pour tout $n \in \mathbb{N}^*$ et pour tout $x \in G$, on note

$$x^n = \underbrace{x * x * \ldots * x}_{n \text{ fois}} .$$

On vérifie aisément que l'inverse de $x^n$ est donné par $(x^{-1})^n$. Par convention, on note $x^{-n} = (x^n)^{-1} = (x^{-1})^n$. Avec cette notation, on a

$$\forall n, m \in \mathbb{Z}, \quad \forall x \in G \qquad x^n * x^m = x^{n+m}\,.$$

Ces notations sont certainement très pratiques mais il convient de faire un peu attention : si $x, y \in G$, en général $(x * y)^n$ n'est pas égal à $x^n * y^n$. En revanche, on a le résultat suivant :

***Lemme 1.1***. — *Soit $(G, *)$ un groupe et $x, y \in G$. On suppose que $x*y = y*x$ (on dit que $x$ et $y$* commutent*) alors, pour tout $n \in \mathbb{Z}$, on a*

$$(x * y)^n = x^n * y^n = y^n * x^n\,.$$

*Démonstration.* — On commence par démontrer, en utilisant une récurrence sur $n \geq 0$, que

$$x^n * y = y * x^n \qquad \text{et que} \qquad y^n * x = x * y^n\,.$$

Ensuite, on montre que $(x * y)^n = x^n * y^n$ en utilisant une fois de plus une récurrence sur $n \geq 0$. Pour $n < 0$, on peut utiliser le résultat de la Proposition 1.2 pour démontrer le résultat. □

Nous verrons dans la section suivante de nombreux exemples de groupes. Commençons par quelques exemples classiques.

## 1.2. Exercices et exemples

On donne dans cette section quelques exemples de groupes. Ces exemples font l'objet d'exercices qui sont fortement recommandés.

***Exemple 1.1***. — *Un groupe $(G, *)$ à un élement est uniquement composé de l'élement neutre donc $G = \{e\}$.*

***Exemple 1.2***. — *Soit $(G, *)$ un groupe à deux éléments, $G = \{e, x\}$ où $e$ désigne l'élément neutre et $x \neq e$. On a*

$$e * e = e\,, \qquad e * x = x * e = x, \qquad \text{et} \qquad x * x = e\,,$$

*(remarquer que $x$ est nécessairement le symétrique de $x$ pour la loi $*$). On peut rassembler ces informations dans un tableau à deux entrées (la table de composition de la loi $*$)*

| $*$ | $e$ | $x$ |
|---|---|---|
| $e$ | $e$ | $x$ |
| $x$ | $x$ | $e$ |

Il faut encore s'assurer que la loi ainsi obtenue vérifie les axiomes de groupe. Le seule point à vérifier est l'associativité, qui, ici ne pose pas de difficulté. On peut cependant faire la remarque suivante, qui trouve sa pleine utilité dans l'étude des groupes de cardinal plus élevé: On vérifie que le groupe obtenu est celui des racines carrées de l'unité (c'est à dire: $\{1,-1\},\times$, ce qui assure l'associativité de la loi.

En jouant sur la définition d'un groupe, on peut facilement classifier tous les groupes à 3 éléments.

***Exemple 1.3***. — *Soit $(G,*)$ un groupe à trois éléments, $G=\{e,x,y\}$ où $e$ désigne l'élément neutre et $x,y\neq e$ sont deux éléments distincts. Alors, la table de composition de la loi $*$ est donnée par*

| $*$ | $e$ | $x$ | $y$ |
|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ |
| $x$ | $x$ | $y$ | $e$ |
| $y$ | $y$ | $e$ | $x$ |

*Démonstration.* — En utilisant le fait que $e$ est l'élément neutre de $(G,*)$, on trouve déjà que

$$e*e=e\,,\quad e*x=x*e=x\qquad\text{et}\qquad e*y=y*e=y\,,$$

ce qui permet de remplir la première ligne et la première colonne. On peut ensuite utiliser le lemme suivant (qu'on démontrera).

***Lemme 1.2***. — *Tous les éléments du groupe se retrouvent dans chaque ligne et dans chaque colonne.*

Ce lemme permet de dire que $x*y=y*x=e$ et on en déduit aussitôt les deux dernières valeurs manquantes.

ici encore, on vérifie que le groupe obtenu est celui des racines cubiques de l'unité, ce qui assure l'associativité de la loi.

□

***Remarque 1.2***. — *Ces trois premiers exemples montrent que les groupes ayant* 1, 2 *ou* 3 *éléments sont nécessairement commutatifs. Cette propriété est équivalente à la symétrie du tableau de groupe par rapport à la première diagonale.*

***Exemple 1.4***. — *Soit $a\in\mathbb{R}$ fixé. On note*

$$a\,\mathbb{Z}=\{a\,n\,:\,n\in\mathbb{Z}\}\,,$$

*l'ensemble des multiples de $a$. Vérifier que $(a\,\mathbb{Z},+)$ est un groupe (additif).*

***Exemple 1.5***. — *Soient $a, b \in \mathbb{R}$ fixés. On note*

$$a\,\mathbb{Z} + b\,\mathbb{Z} = \{a\,n + b\,m \,:\, n, m \in \mathbb{Z}\}\,.$$

*Vérifier que $(a\,\mathbb{Z} + b\,\mathbb{Z}, +)$ est un groupe (additif).*

***Exemple 1.6***. — *On note*

$$\mathbb{U} = \{z \in \mathbb{C} \,:\, |z| = 1\}\,,$$

*l'ensemble des nombres complexes de module 1. Vérifier que $(\mathbb{U}, \cdot)$ est un groupe (multiplicatif).*

***Exemple 1.7***. — *Soit $\alpha \in \mathbb{R}$. On note*

$$\mathbb{U}_\alpha = \{e^{in\alpha} \in \mathbb{C} \,:\, n \in \mathbb{Z}\}\,.$$

*Vérifier que $(\mathbb{U}_\alpha, \cdot)$ est un groupe (multiplicatif) et que ce groupe est un groupe fini si et seulement si $\alpha \in \pi\,\mathbb{Q}$.*

*Démonstration.* — Vérifions que $G$ est fini si et seulement si $\alpha \in \pi\,\mathbb{Q}$. Supposons que $\mathbb{U}_\alpha$ est fini. Alors, il existe $n \neq m \in \mathbb{Z}$ tels que

$$e^{in\alpha} = e^{im\alpha}\,.$$

En particulier, ceci implique que $(n-m)\,\alpha \in 2\pi\,\mathbb{Z}$, donc que $\alpha = \frac{2\pi k}{n-m}$ pour un certain $k \in \mathbb{Z}$.

Inversement, si $\alpha \in \pi\,\mathbb{Q}$ alors, il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que

$$\alpha = \frac{p}{q}\,\pi\,.$$

Dans ce cas $e^{i2q\alpha} = 1$ donc

$$\mathbb{U}_\alpha \subset \{e^{in\alpha} \in \mathbb{C} \,:\, n = 0, 1, \ldots, q-1\}\,,$$

contient au plus $q$ éléments. Il est donc de cardinal fini. □

***Exemple 1.8***. — *On considère l'ensemble $\mathbb{R}^2 - \{(0,0)\}$ muni de la loi $*$ définie par*

$$(x, y) * (x', y') = (xx' - yy', xy' + yx')\,.$$

*Vérifier que $(\mathbb{R}^2 - \{(0,0)\}, *)$ est un groupe commutatif. Quel est le symétrique de $(x, y)$ ?*

***Exemple 1.9***. — *Soit $E$ un ensemble et $G$ l'ensemble des bijections de $E$ dans $E$. On note $\circ$ la loi de composition d'applications de $E$ dans $E$. Vérifier que $(G, \circ)$ est un groupe (l'élement neutre est $\mathrm{Id}_E$ et le symétrique de $f \in G$ est la bijection réciproque $f^{-1}$).*

***Exemple 1.10***. — *Vérifier que l'ensemble $GL_n(\mathbb{R})$ des matrices $n \times n$ à coefficients dans $\mathbb{R}$ qui sont inversibles, muni de la loi de multiplication des matrices, est un groupe.*

***Exemple 1.11***. — *Soient $a \in \mathbb{R}$. On note*

$$\mathbb{Q}[a] = \{n + a\,m \,:\, n, m \in \mathbb{Q}\}\,.$$

*Vérifier que $(\mathbb{Q}[\sqrt{2}] - \{0\}, .)$ est un groupe (multiplicatif).*

***Exemple 1.12***. — *Soit $(G, *)$ un groupe tel que pour tout $x, y \in G$*

$$(x * y)^2 = x^2 * y^2\,.$$

*Alors $(G, *)$ est abélien. En effet, on a $x*y*x*y = x*x*y*y$. En composant à gauche par $x^{-1}$ et à droite par $y^{-1}$ on trouve $y * x = x * y$. Ce qui montre bien que $(G, *)$ est abélien.*

Un exemple de groupe non abélien est fourni par les matrices $n\times n$ inversibles (pour $n \geq 2$ muni du produit des matrices. Donnons maintenant un exemple d'un groupe fini non abélien.

***Exemple 1.13***. — † *On considère dans le plan $\mathbb{R}^2$, le triangle équilatéral de sommets*

$$(1, 0), \quad (-\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}), \qquad \text{et} \qquad (-\tfrac{1}{2}, -\tfrac{\sqrt{3}}{2})$$

*et on considère $G$ le groupe des isométries du plan qui laissent ce triangle invariant.*

*On vérifie que*

$$G = \{I, R_1, R_2, S_1, S_2, S_3\}$$

*où $I = Id_{\mathbb{R}^2}$, $R_1$ (resp. $R_2$) est la rotation d'angle $\frac{2\pi}{3}$ (resp. la rotation d'angle $\frac{4\pi}{3}$) et où $S_1$ (resp. $S_2$, resp. $S_3$) est la symétrie par rapport à la droite $y = 0$ (resp. par rapport à la droite $y = -\sqrt{3}\,x$, resp. par rapport à la droite $y = \sqrt{3}\,x$). On munit $G$ de la loi $\circ$ (loi de composition des applications linéaires du plan).*

*Vérifier que la table de composition de la loi $\circ$ est donnée par*

| $\circ$ | $I$ | $R_1$ | $R_2$ | $S_1$ | $S_2$ | $S_3$ |
|---|---|---|---|---|---|---|
| $I$ | $I$ | $R_1$ | $R_2$ | $S_1$ | $S_2$ | $S_3$ |
| $R_1$ | $R_1$ | $R_2$ | $I$ | $S_3$ | $S_1$ | $S_2$ |
| $R_2$ | $R_2$ | $I$ | $R_1$ | $S_2$ | $S_3$ | $S_1$ |
| $S_1$ | $S_1$ | $S_2$ | $S_3$ | $I$ | $R_1$ | $R_2$ |
| $S_2$ | $S_2$ | $S_3$ | $S_1$ | $R_2$ | $I$ | $R_1$ |
| $S_3$ | $S_3$ | $S_1$ | $S_2$ | $R_1$ | $S_2$ | $I$ |

*Nous retrouverons la table de composition de cette loi plus tard dans le cours.*

***Exemple 1.14***. — *Soit $(G, *)$ un groupe. On suppose que, pour tout $a \in G$, $a^2 = e$. Vérifier que $(G, *)$ est abélien.*

*Démonstration.* — Soient $a, b \in G$. Par hypothèse $a^2 = b^2 = e$ et $(a * b)^2 = e$. Cette dernière égalité s'écrit aussi

$$e = a * b * a * b.$$

On compose alors par $a$ à gauche et par $b$ à droite pour trouver

$$a * b = a * e * b = a * (a * b * a * b) * b = (a * a) * b * a * (b * b) = e * b * a * e = b * a$$

donc $a$ et $b$ commutent. □

**Groupe produit:**

***Définition 1.2***. — *Si $(G_1, *_1), \cdots (G_n, *_n)$ sont $n$ groupes, l'ensemble $G_1 \times \cdots \times G_n$ peut être muni d'une loi de groupe $*$ définie par*

$$(x_1, \cdots x_n) * (y_1, \cdots y_n) = (x_1 *_1 y_1, \cdots x_n *_n y_n).$$

*L'élément neutre est $(e_1, \cdots e_n)$ et le symétrique de $(x_1, \cdots x_n)$ est $((x_1)^{-1}, \cdots (x_n)^{-1})$.*

C'est ainsi que l'on définit $(\mathbb{R}^n, +)$ par exemple.

## 1.3. Sous-groupes

Dans toute cette section, $(G, *)$ désigne un groupe.

***Définition 1.3***. — *Soit $H \subset G$. On dit que $H$ est un* sous-groupe *de $(G, *)$ si $(H, *)$ est un groupe.*

**Exemples:**
$(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, qui est un sous-groupe de $(\mathbb{R}, +)$, qui est un sous-groupe de $(\mathbb{C}, +)$.

$(\mathbb{Q}^{*,+}, \times)$ est un sous-groupe de $(\mathbb{R}^{*,+}, \times)$ qui est un sous-groupe de $(\mathbb{R}^*, \times)$, qui est un sous-groupe de $(\mathbb{C}^*, \times)$. De même, le groupe $U - n$ des racines n-ièmes de l'unité forme un sous-groupe de $(U, \times)$ qui est un sous-groupe de $(\mathbb{C}^*, \times)$.

Les rotations de $\mathbb{R}^2$, c'est-à-dire les matrices $2 \times 2$ de la forme

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

forment un sous-groupe du groupe des matrices $2 \times 2$ inversibles.

Le résultat suivant donne un critère qui permet de vérifier facilement si $H$ est un sous-groupe de $(G, *)$.

***Proposition 1.3***. — *Un sous-ensemble $H \subset G$ est un sous-groupe de $(G, *)$ si et seulement si les trois propriétés suivantes sont vérifiées :*

(i) $e \in H$,
(ii) $\forall x \in H,\ x^{-1} \in H$,
(iii) $\forall x, y \in H,\ x * y \in H$.

On a aussi la caractérisation suivante :

***Proposition 1.4***. — *Un sous-ensemble $H \subset G$ non vide est un sous-groupe de $(G, *)$ si et seulement si*

$$\forall x, y \in H, \qquad x * y^{-1} \in H\,.$$

*Démonstration.* — L'implication est évidente. Regardons plus précisément la réciproque. On suppose donc que $\forall x, y \in H,\ x * y^{-1} \in H$. Etant donné que $H$ est non vide, il existe $x \in H$, donc $x * x^{-1} \in H$. Mais, $x * x^{-1} = e$ (calcul effectué dans $G$) donc $e \in H$, ce qui démontre la propriété (i) dans la Proposition 1.3. On sait maintenant que $e \in H$ et si $x \in H$ alors $e * x^{-1} \in H$, donc $e * x^{-1} = x^{-1} \in H$, ce qui démontre la propriété (ii) dans la Proposition précédente. Enfin, si $x, y \in H$, on vient de démontrer que $y^{-1} \in H$ donc $x * (y^{-1})^{-1} \in H$. Autrement dit $x * y \in H$, ce qui démontre la propriété (iii) dans la Proposition 1.3. Conclusion, (i), (ii) et (iii) sont vérifiés donc, d'après la Proposition 1.3, $H$ est un sous-groupe de $(G, *)$. □

Donnons quelques exemples de sous-groupes.

***Exemple 1.15***. — *Tout groupe $(G, *)$ admet les deux sous-groupes triviaux $\{e\}$ et $G$.*

***Exemple 1.16***. — *Soit $(G, *)$ un groupe et $x \in G$. Le sous-ensemble de $G$ défini par*

$$\{x^n\ :\ n \in \mathbb{Z}\}\,,$$

*est un sous-groupe de $G$; on l'appelle le* sous-groupe engendré par $x$. *L'élément neutre est $e = x^0$ et le symétrique de $x^n$ est $x^{-n}$. Si ce sous-groupe est fini,* son cardinal s'appelle l'ordre de $x$. *Ainsi, si $G$ est le groupe des racines huitièmes de l'unité: $G = (\{e^{ik\pi/4}\}, \times)$, alors $e^{i\pi/4}$ est d'ordre 8, $e^{i\pi/2}$ $(= i)$ est d'ordre 4 et $e^{i\pi}$ $(= -1)$ est d'ordre 2.*

On peut décrire exactement tous les sous-groupes de $\mathbb{Z}$.

***Proposition 1.5***. — *Tout sous-groupe de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$.*
*De plus $a\mathbb{Z} \subset b\mathbb{Z}$ si et seulement si $b$ divise $a$.*

*Démonstration.* — Il est clair que $a\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$ car $0 \in a\mathbb{Z}$ et $an - bn = (a-b)n$; le critère foruni par la proposition 1.4 est donc vérifié.

Soit $H$ un sous groupe de $\mathbb{Z}$ différent de $\{0\}$. On note

$$a = \min\{x \in H \,:\, x > 0\}$$

on vérifie que $a \in H$ et que $a > 0$. Soit $x \in H$, $x > 0$. Effectuons la division euclidienne de $x$ par $a$

$$x = q\,a + r\,,$$

où $q \in \mathbb{N}$ et $r \in \{0, \ldots, a-1\}$. Etant donné que $(H, +)$ est un groupe, on a $q\,a \in H$, donc, on peut conclure que

$$r = x - q\,a \in H\,.$$

Par construction de $a$, nécessairement $r = 0$. Donc $x \in a\,\mathbb{Z}$. Une démonstration semblable montre que si $x \in H$, $x < 0$ alors $x \in a\,\mathbb{Z}$. Conclusion, $H \subset a\,\mathbb{Z}$. Enfin, étant donné que $a \in H$, les multiples de $a$ sont aussi des éléments de $H$, donc $a\,\mathbb{Z} \subset H$. On a donc montré que $H = a\,\mathbb{Z}$.

Le dernier point est immédiat. □

***Exemple 1.17***. — *Soit $a, b \in \mathbb{N}$. Alors $(a\,\mathbb{Z} + b\,\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$. Donc d'après le résultat précédent, il existe $c \in \mathbb{N}$ tel que*

$$a\,\mathbb{Z} + b\,\mathbb{Z} = c\,\mathbb{Z}\,.$$

Le théorème ci-dessous donne la valeur de $c$.

***Théorème 1.1***. — **[Théorème de Bézout]** *Soient $a, b \in \mathbb{N}^*$. Alors on a*

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \quad \textit{avec} \quad d = PGCD(a, b).$$

*En particulier, il existe $u, v \in \mathbb{Z}$ tels que*

$$a\,u + b\,v = d.$$

*Démonstration.* — On sait qu'il existe $c \in \mathbb{N}$ tel que

$$a\,\mathbb{Z} + b\,\mathbb{Z} = c\,\mathbb{Z}\,.$$

En particulier, $c \in a\,\mathbb{Z} + b\,\mathbb{Z}$ donc il existe $u, v \in \mathbb{Z}$ tels que $a\,u + b\,v = c$. Montrons que $c$ est égal à $d$, le pgcd de $a$ et $b$, ce qui terminera la preuve. Clairement

$$a\,\mathbb{Z} \subset d\,\mathbb{Z} \qquad \text{et} \qquad b\,\mathbb{Z} \subset d\,\mathbb{Z}\,,$$

donc $c\,\mathbb{Z} \subset d\,\mathbb{Z}$. On en déduit que $d$ divise $c$. Ensuite, $a \in c\,\mathbb{Z}$ et $b \in c\,\mathbb{Z}$, donc $c$ divise à la fois $a$ et $b$. On en déduit que $c$ divise $d$. Conclusion $d = c$. □

On a donc par exemple $2\,\mathbb{Z} + 3\,\mathbb{Z} = \mathbb{Z}$ et $6\,\mathbb{Z} + 8\,\mathbb{Z} = 2\,\mathbb{Z}$.

***Définition 1.4***. — *Soit $(G,*)$ un groupe. L'ensemble*

$$Z = \{x \in G \,:\, x * y = y * x \qquad \forall y \in G\}\,,$$

*est un sous-groupe de $(G,*)$ qui est appelé le* centre de $(G,*)$.

*Démonstration.* — On vérifie que $e \in Z$, car $e * y = y * e$ pour tout $y \in G$. Vérifions que $Z$ est stable par $*$. Soient $x, x' \in Z$. Pour tout $y \in G$ on peut écrire

$$(x * x') * y = x * (x' * y) = x * (y * x') = (x * y) * x' = y * (x * x')\,,$$

donc $x * x' \in Z$. Enfin, si $x \in Z$ alors $x * y = y * x$ pour tout $y \in G$. On compose à droite et à gauche par $x^{-1}$ pour trouver

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

identité que l'on peut encore écrire sous la forme

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

donc

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

donc $x^{-1} \in Z$. □

**Remarque:** Si $G$ est commutatif, le centre de $G$ est $G$ lui-même.

***Exemple 1.18***. — *Vérifier que le centre du groupe des matrices $2 \times 2$ inversibles (pour le produit) est l'ensemble des matrices de la forme $C \cdot Id$ avec $C \neq 0$.*

***Théorème 1.2***. — *Soit $(G,*)$ un groupe et $H_i$, pour $i \in I$ une famille de sous-groupes de $(G,*)$. Alors, $H = \bigcap_{i \in I} H_i$ est un sous-groupe de $(G,*)$.*

*Démonstration.* — On vérifie que $H$ est non vide car $e \in H_i$ pour tout $i \in I$. Soient $x, y \in H$, alors $x, y \in H_i$, pour tout $i \in I$. Etant donné que $(H_i,*)$ est un groupe, on en déduit que $x * y^{-1} \in H_i$. Donc $x * y^{-1} \in \bigcap_{i \in I} H_i = H$. Le résultat est alors une conséquence de la Proposition 1.4. □

**Remarque:** Attention, en général une union de sous-groupes n'est pas un sous-groupe.

***Définition 1.5***. — *Soit $(G,*)$ un groupe et $X \subset G$. On note $< X >$ le sous-groupe engendré par $X$, c'est-à-dire l'intersection de tous les sous-groupes de $(G,*)$ qui contiennent $X$ (autrement dit $< X >$ est le plus petit sous-groupe de $G$ qui contient $X$).*

**Remarque:** Si $X = \{x\}$ est réduit à un singleton, le sous-groupe engendré par $\{x\}$ est $\{x^n\}$ (avec $n \in \mathbb{N}$ si ce groupe est infini, et sinon, $n = 0, \dots k-1$, où $k$ est l'ordre de $x$. On note $< x >$ ce groupe.

***Définition 1.6***. — *Soient $(e_1, \cdots e_d)$ $d$ vecteurs de $\mathbb{R}^d$ formant une base de $\mathbb{R}^d$. On appelle réseau engendré par $(e_1, \cdots e_d)$ l'ensemble*

$$\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_d.$$

*C'est un sous-groupe de $(\mathbb{R}^d, +)$.*

***Proposition 1.6***. — *Soit $(G, *)$ un groupe et $x \in G$. Alors*

$$< x >= \{x^n \, : \, n \in \mathbb{Z}\}\,.$$

*Démonstration.* — Etant donné que $< x >$ est un groupe qui contient $x$, il contient aussi $x^n$, pour tout $n \in \mathbb{Z}$. On peut donc affirmer que

$$\{x^n \, : \, n \in \mathbb{Z}\} \subset < x > \ .$$

D'autre part, on sait que $(\{x^n \, : \, n \in \mathbb{Z}\}, *)$ est un groupe (voir exemple 1.16), c'est donc un sous-groupe de $G$ qui contient $x$. On a donc l'inclusion

$$< x > \subset \{x^n \, : \, n \in \mathbb{Z}\}\,.$$

Ce qui termine la démonstration. □

On montre de la même façon que

***Proposition 1.7***. — † *Soit $(G, *)$ un groupe et $X \subset G$. Alors*

$$< X >= \{y \in G \, : \, \exists\, n \in \mathbb{N}, \quad y = x_1 * \ldots * x_n \\ \text{où} \quad (x_i \in X \quad ou \quad x_i^{-1} \in X), \quad \forall i = 1, \ldots, n\}\ .$$

# CHAPITRE 2

# GROUPES QUOTIENTS ET MORPHISMES

## 2.1. Relations d'équivalence

***Définition 2.1***. — *Soit $E$ un ensemble. Une relation entre les éléments de $E$ est un sous-ensemble $R$ de $E \times E$. On note $a \mathcal{R} b$ si le couple $(a, b)$ appartient à $R$, et on dit que $a$ est en relation avec $b$.*

Soit $\mathcal{R}$ une relation définie sur un ensemble $E$.
Les propriétés usuelles que peut vérifier une relation sont les suivantes:

- $\mathcal{R}$ est *réflexive* si
$$\forall x \in E\,, \quad x \mathcal{R} x\,.$$
- $\mathcal{R}$ est *symétrique* si
$$\forall x, y \in E\,, \quad x \mathcal{R}\, y \quad \Longrightarrow \quad y \mathcal{R}\, x\,.$$
- $\mathcal{R}$ est *antisymétrique* si
$$\forall x, y \in E\,, \text{ si } \quad x \mathcal{R}\, y \text{ et } \quad y \mathcal{R}\, x \quad \text{ alors } x = y.$$
- $\mathcal{R}$ est *transitive* si
$$\forall x, y, z \in E\,, \quad (x \mathcal{R}\, y \quad \text{et} \quad y \mathcal{R}\, z) \quad \Longrightarrow x \mathcal{R}\, z\,.$$

Deux classes de relations jouent un rôle particulièrement important.

***Définition 2.2***. — *On dit que $\mathcal{R}$ est une* relation d'équivalence *si $\mathcal{R}$ est* réflexive*,* symétrique *et* transitive*.*

*On dit que $\mathcal{R}$ est une* relation d'ordre *si $\mathcal{R}$ est* réflexive*,* antisymétrique *et* transitive*.*

**Exemples:**

- Si $E$ est un ensemble, la relation $A \mathcal{R}\, B$ si $A \subset B$ est une relation d'ordre sur $\mathcal{P}(E)$.
- Soit $a \in \mathbb{N}^*$; sur $\mathbb{Z}$, la relation $n \mathcal{R}\, m$ si $n - m \in a\mathbb{Z}$ est une relation d'équivalence.

– Sur $\mathbb{C}$ la relation $z \mathcal{R} z'$ si $|z| = |z'|$ est une relation d'équivalence.

***Définition 2.3***. — *Si $\mathcal{R}$ est une relation d'équivalence sur $E$ alors la* classe d'équivalence *de $x$ est le sous ensemble de $E$ défini par*

$$\dot{x} := \{y \in X \, : \, x \mathcal{R} y\}.$$

On rappelle la définition d'une partition d'un ensemble $X$.

***Définition 2.4***. — *Soit $I$ une famille d'indices, et $(X_i)_{i\in I}$ une famille de sous-ensemble de $E$ indexée par $I$ (c'est-à-dire que l'on se donne une application de $I$ dans $\mathcal{P}(E)$). On dit que $(X_i)_{i\in I}$ forme une partition de $X$ si*

$$X = \bigcup_{i\in I} X_i$$

*et si*

$$\forall i \neq j \, , \qquad X_i \cap X_j = \emptyset.$$

***Proposition 2.1***. — *Les classes d'équivalence d'une relation d'équivalence sur $X$ forment une partition de $X$.*

**Démonstration:** Pour tout $x \in E$, $x \in \dot{x}$, d' où la première propriété. Et si $\dot{x}$, et $\dot{y}$ ont un élément $z$ en commun, alors $x\mathcal{R}z$ et $z\mathcal{R}y$, donc $x\mathcal{R}y$ et donc $\dot{x} = \dot{y}$, d' où la deuxième propriété.

On note $X/\mathcal{R}$ l'ensemble des classes d'équivalence de la relation $\mathcal{R}$ sur $X$.

**Remarque:** On vérifie facilement que, réciproquement, pour toute partition de $E$, il existe une relation d'équivalence dont les classes d'équivalence sont les éléments de cette partition.

**Exemples:** Reprenons les deux exemples déjà mentionnés:
Tout d'abord, sur $\mathbb{Z}$, la relation $n \ \mathcal{R} \ m$ si $n-m \in a\mathbb{Z}$; les classes d'équivalence sont les $a$ sous-ensembles de $\mathbb{Z}$ suivants:

$$\forall k = 0, \cdots a-1, \qquad \dot{k} = k + a\mathbb{Z}.$$

Sur $\mathbb{C}$ la relation $z \mathcal{R} z'$ si $|z| = |z'|$ : les classes d'équivalence sont les cercles centrés en 0.

## 2.2. Théorème de Lagrange

***Proposition 2.2***. — *Soient $(G, *)$ un groupe et $H$ un sous-groupe de $G$. On considère la relation $\mathcal{R}$ sur $G$ par*

$$x \mathcal{R} y \quad \Longleftrightarrow \quad x * y^{-1} \in H$$

*La relation $\mathcal{R}$ est une relation d'équivalence sur $G$.*

*Démonstration.* — Pour tout $x \in G$ on a $x * x^{-1} = e$ qui appartient à $H$ donc $\forall x \in G$, $x \mathcal{R} x$. La relation est donc réflexive.

Si $x * y^{-1} \in H$, alors son inverse appartient aussi à $H$, mais cet inverse est $y * x^{-1}$, donc $y * x^{-1} \in H$. La relation est donc symétrique.

Si $x \mathcal{R} y$ et $y \mathcal{R} z$, alors $x*y^{-1} \in H$ et $y*z^{-1} \in H$. Donc $(x*y^{-1})*(y*z^{-1}) = x * z^{-1} \in H$, c'est-à-dire $x \mathcal{R} z$. La relation est donc transitive. □

On notera $\dot{x}$ la classe d'équivalence de $x$ pour la relation $\mathcal{R}$ et on notera $G/H$ l'ensemble des classes d'équivalence pour la relation $\mathcal{R}$ (l'intérêt d'utiliser cette notation plutôt que la notation précédente $G/\mathcal{R}$ est qu'elle fait apparaitre explicitement le sous-groupe utilisé dans le quotient).

***Théorème 2.1* (de Lagrange).** — *Soit $(G, *)$ un groupe fini et $H$ un sous-groupe. Alors, le cardinal de $H$ divise le cardinal de $G$. De plus*

$$\mathrm{Card}(G) = \mathrm{Card}(G/H)\,\mathrm{Card}(H)$$

*Démonstration.* — On a une partition de $G$ en classes d'équivalence de la relation $\mathcal{R}$.

Etudions la classe d'équivalence d'un élément $x$. On a

$$\dot{x} = \{y \in G : \quad x * y^{-1} \in H\}.$$

Mais $x*y^{-1} \in H$ signifie qu'il existe $a \in H$ tel que $y = a^{-1}x$, donc $\dot{x}$ est l'image de $H$ par l'application $a \to a^{-1}x$, qui est clairement injective. Cette image a donc $Card(H)$ éléments. Donc toutes les classes d'équivalence ont le même nombre d'éléments, à savoir $Card(H)$. Ces classes d'équivalence formant une partition de $G$, on a bien le théorème.

□

***Définition 2.5***. — *Soit $(G, *)$ un groupe fini, et $H$ un sous-groupe de $G$.* L'indice de $H$ dans $G$, *noté $[G : H]$, est le cardinal de $G/H$.*

Voici quelques conséquences du Théorème de Lagrange.

***Proposition 2.3***. — *Soit $(G, *)$ un groupe fini et $x \in G$. Alors l'ordre de $x$ divise le cardinal de $G$.*

*Démonstration.* — On remarque que $< x >$ est un sous-groupe de $(G, *)$ dont le cardinal est égal à l'ordre de $x$. Le résultat est alors une conséquence directe du Théorème de Lagrange. □

***Exemple 2.1***. — *Soit $(G, *)$ un groupe non abélien de cardinal égal à 8. Alors $G$ admet un élément d'ordre 4.*

*Démonstration.* — Soit $a \in G$. Grâce au théorème de Lagrange, on sait que l'ordre de $a$ divise 8. Donc, l'ordre de $a$ est égal à $1, 2, 4$ ou 8. Si l'ordre de $a$ est égal à 1, c'est que $a = e$. Maintenant, si l'ordre de $a$ est égal à 8 alors nécessairement $G =< a >$ et $(G, *)$ serait abélien, ce qui est contraire à l'hypothèse. Conclusion, si $a \neq e$, l'ordre de $a$ est soit égal à 2 soit égal à 4.

Si l'ordre de tous les éléments de $G \setminus \{e\}$ était égal à 2 alors $(G, *)$ serait abélien (voir exemple 1.14). Conclusion, il existe au moins un élément de $G$ qui est d'ordre 4. □

## 2.3. Compatibilité d'une relation avec une loi de composition interne

***Définition 2.6***. — *Soit $E$ un ensemble muni d'une loi de composition interne $*$. Une relation d'équivalence $\mathcal{R}$ sur $E$ est compatible avec la loi $*$ si*

$$\forall a, b \in E, \quad a \,\mathcal{R}\, b \quad \Rightarrow \quad \forall x \in E, \begin{cases} (a * x) \;\mathcal{R}\; (b * x) \\ (x * a) \;\mathcal{R}\; (x * b) \end{cases}$$

***Exemple 2.2***. — *La relation sur $\mathbb{C}$ définie par $z \,\mathcal{R}\, z'$ si $|z| = |z'|$ est compatible avec la multiplication, mais pas avec l'addition.*

***Proposition 2.4***. — *Soit $E$ un ensemble muni d'une loi de composition interne $*$ et $\mathcal{R}$ une relation d'équivalence sur $E$ compatible avec la loi $*$. On peut définir une loi de composition interne $\dot{*}$ sur $E/\mathcal{R}$ de la façon suivante:*

$$\dot{a} \dot{*} \dot{b} = \overline{a * b}.$$

*Démonstration.* — Pour que $\dot{*}$ soit bien défini, il faut vérifier que la définition ne dépend pas des représentants choisis dans $\dot{a}$ et $\dot{b}$. Soient donc $a' \in \dot{a}$ et $b' \in \dot{b}$. Alors

$$\overline{a' * b'} = \overline{a' * b} \quad \text{car } b \,\mathcal{R}\, b'$$

et

$$\overline{a' * b} = \overline{a * b} \quad \text{car } a \,\mathcal{R}\, a'$$

□

***Proposition 2.5***. — *Soit $(G, *)$ un groupe et $\mathcal{R}$ une relation d'équivalence sur $G$ compatible avec $*$. Alors $(G/\mathcal{R}, \dot{*})$ est un groupe.*

Montrons l'associativité. On a

$$(a * b) * c = a * (b * c)$$

donc

$$(\overline{a * b}) \dot{*} \dot{c} = \dot{a} \dot{*} (\overline{b * c})$$

donc

$$(\dot{a} \dot{*} \dot{b}) \dot{*} \dot{c} = \dot{a} \dot{*} (\dot{b} \dot{*} \dot{c})$$

Le reste de la démonstration est est similaire et laissé en exercice. On remarquera que l'élément neutre est $\dot{e}$ et le symétrique de $\dot{a}$ est $\overline{a^{-1}}$.

**Remarque :** De même, si $*$ est commutative, alors $\dot{*}$ est également commutative.

**Exemple: Construction de $\mathbb{R}$**

On ne donne que le schéma général de construction. Certains calculs un peu fastidieux sont laissés en exercice.

On suppose construit $\mathbb{Q}$. Une suite de rationnels $(a_n)_{n\in\mathbb{N}}$ est *de Cauchy* si, pour tout rationnel $\varepsilon > 0$ il existe $N$ tel que

$$\forall n, m \geq N, \qquad |a_n - a_m| \leq \varepsilon.$$

On dit qu'une suite $(r_n)$ de rationnels tend vers 0 si, pour tout rationnel $\varepsilon > 0$ il existe $N$ tel que

$$\forall n \geq N, \qquad |r_n| \leq \varepsilon.$$

On introduit alors une relation d'équivalence entre suites de Cauchy de rationnels: Deux suites $(a_n)$ et $(b_n)$ sont équivalentes si $a_n - b_n \to 0$. On vérifie alors que l'addition et la multiplication (terme à terme) des suites sont compatibles avec cette relation d'équivalence. L'ensemble quotient, est donc ainsi muni de deux lois de composition internes, $+$ et $\times$, qui héritent des propriétés de ces lois sur $\mathbb{Q}$. On "identifie" le rationnel $q$ à la classe d'équivalence de la suite constante égale à $q$.

## 2.4. Compléments sur $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. On considère maintenant la relation sur $\mathbb{Z}$:

$$a \mathcal{R} b \quad \text{si} \quad a - b \quad \text{est multiple de} \quad n.$$

C'est clairement une relation d'équivalence sur $\mathbb{Z}$ appelée *congruence modulo* $n$. Si $a \mathcal{R} b$, on notera:

$$a \equiv b \quad [n].$$

On a alors

$$\dot{a} = a + n\mathbb{Z}.$$

et

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \ldots, \overline{n-1}\},$$

On remarque que l'on a quotienté $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$. L'ensemble des classes d'équivalence pour cette relation est donc noté $\mathbb{Z}/n\mathbb{Z}$.

La relation d'équivalence est compatible avec la somme et le produit usuels des entiers. En effet, si $a-b$ est multiple de $n$ , pour tout $c$, $(a+c)-(b+c)$ est multiple de $n$, et $ac - bc$ est multiple de $n$. On en déduit que $\mathbb{Z}/n\mathbb{Z}$ est muni

de deux lois de compositions internes $\dot{+}$ et $\dot{\times}$, que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif, et que $\dot{\times}$ est commutative.

***Exemple 2.3.*** — *Prenons $n = 3$, alors $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$ et la table d'addition dans $\mathbb{Z}/3\mathbb{Z}$ est donnée par*

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

*On pourra comparer cette table à celle obtenue dans l'exemple 1.3.*

**Remarque:** Attention, certains résultats vrais sur $\mathbb{Z}$ deviennent faux dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, il peut y avoir des *diviseurs de 0*: Par exemple, dans $\mathbb{Z}/6\mathbb{Z}$, $\dot{2}\dot{\times}\dot{3} = \dot{6} = \dot{0}$. Ou encore certains éléments de $\mathbb{Z}/n\mathbb{Z}$ peuvent diviser 1; ainsi, dans $\mathbb{Z}/8\mathbb{Z}$, $\dot{3}\dot{\times}\dot{3} = \dot{9} = \dot{1}$.

La prochaine proposition utilise une idée qui revient constamment dans l'étude des groupes finis (on laisse la démonstration du lemme en exercice).

***Lemme 2.1.*** — *Soit $E$ un ensemble fini, et $\sigma$ une application de $E$ dans $E$. Alors, on a l'équivalence:*

$$\sigma \text{ injective} \iff \sigma \text{ surjective} \iff \sigma \text{ bijective.}$$

***Proposition 2.6.*** — *Soit $p \geq 2$ un nombre premier. L'ensemble $(\mathbb{Z}/p\mathbb{Z})^*$ muni de la loi $\dot{\times}$ est un groupe commutatif.*

*Démonstration.* — En effet, la multiplication est associative (conséquence de l'associativité dans $\mathbb{Z}$), et l'élément neutre est donné par $\dot{1}$. Montrons maintenant que chaque élément $\dot{a}$ est inversible; pour cela, on considére l'application $\sigma_a$ de $(\mathbb{Z}/p\mathbb{Z})^*$ dans lui-même définie par $\dot{k} \to \dot{a} \times \dot{k}$. On remarque que, si $1 \leq k < k' \leq p-1$, les éléments $\dot{k} \dot{\times} \dot{a}$ et $\dot{k'} \dot{\times} \dot{a}$ sont distincts; en effet, si tel n'était pas le cas, $(k' - k)\, a$ serait un multiple de $p$. Or $k' - k < p$ et nous avons supposé que $p$ est un nombre premier, donc nécessairement, $p$ devrait diviser $a$, donc $\dot{a} = \dot{0}$, ce qui est contraire à l'hypothèse.

Donc, quand $k$ varie de 1 à $p-1$, les éléments $\dot{k} \dot{\times} \dot{a}$ sont deux à deux distincts et $\sigma_a$ est donc injective, donc surjective. En particulier, il existe $\dot{k}$ tel que $\dot{k} \dot{\times} \dot{a} = \dot{1}$. □

Une conséquence du théorème de Lagrange et de la proposition précédente est une démonstration très simple du "petit théorème de Fermat".

***Théorème 2.2* (Petit Théorème de Fermat).** — *Soit $p \geq 2$ un nombre premier et $\dot{a} \in (\mathbb{Z}/p\mathbb{Z})^*$. Alors $\dot{a}^{p-1} = \dot{1}$.*

*Démonstration.* — Puisque $p$ est premier, $((\mathbb{Z}/p\mathbb{Z})^*, \dot{\times})$ est un groupe à $p-1$ éléments. Ensuite, il suffit d'utiliser que l'ordre d'un élément $\dot{a}$ divise $p-1$, donc $\dot{a}^{p-1} = \dot{1}$. □

## 2.5. Morphismes

Nous avons déjà remarqué que certains groupes ont la même table de composition. C'est par exemple le cas pour $(\mathbb{Z}/3\mathbb{Z}, +)$ et du groupe des racines cubiques de l'unité, muni de la multiplication (ce qui n'est d'ailleurs pas étonnant puisque nous avons par ailleurs montré qu'il n'y a qu'une seule loi de composition possible sur un ensemble à trois éléments qui en fasse un groupe). C'est la notion de morphisme qui fournit le bon cadre pour expliquer ces similitudes.

***Définition 2.7.*** — *Soient $(G, *)$ et $(G', *')$ deux groupes et $f : G \longrightarrow G'$ une application. On dit que $f$ est un* morphisme de groupes *si*

$$\forall x, y \in G \qquad f(x * y) = f(x) *' f(y)\,.$$

*Un* endomorphisme *de groupes est un morphisme d'un groupe dans lui même.*

***Exemple 2.4.*** — *Vérifier que* $\exp : \mathbb{R} \longrightarrow ]0, +\infty[$ *est un morphisme de groupes de* $(\mathbb{R}, +)$ *dans* $(]0, \infty[\,, \cdot\,)$.

***Exemple 2.5.*** — *Vérifier que l'application* $\theta \to e^{i\theta}$ *est un morphisme de groupes de* $(\mathbb{R}, +)$ *dans* $(U\,, \cdot\,)$.

***Exemple 2.6.*** — *Vérifier que l'application de* $\mathbb{C}^*$ *dans* $GL_2(\mathbb{R})$ *(ensemble des matrices* $2 \times 2$ *à coefficients réels et inversibles) définie par*

$$a + ib \to \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

*est un morphisme de groupes.*

Soit $f : G \longrightarrow G'$ un morphisme de groupes. On note $e$ l'élément neutre de $(G, *)$ et $e'$ l'élément neutre de $(G', *')$.

***Proposition 2.7.*** — *Les propriétés suivantes sont vérifiées :*

(i) $f(e) = e'$,

(ii) *Pour tout* $x \in G$ *et pour tout* $n \in \mathbb{Z}$, $f(x^n) = (f(x))^n$. *En particulier,*

$$f(x^{-1}) = (f(x))^{-1}\,.$$

*Démonstration.* — En utilisant le fait que $f$ est un morphisme de groupes, on peut écrire

$$f(e) = f(e * e) = f(e) *' f(e)\,.$$

On compose par $f(e)^{-1}$, le symétrique de $f(e)$ pour la loi $*'$. On trouve

$$\begin{aligned} e' = f(e)^{-1} *' f(e) &= f(e)^{-1} *' (f(e) *' f(e)) \\ &= (f(e)^{-1} *' f(e)) *' f(e) = e' *' f(e) = f(e)\,. \end{aligned}$$

Ce qui montre que $f(e) = e'$.

Soit $x \in G$, on calcule

$$e' = f(e) = f(x * x^{-1}) = f(x) *' f(x^{-1})\,,$$

donc $f(x^{-1})$ est le symétrique de $f(x)$ pour la loi $*'$. Conclusion :

$$f(x^{-1}) = (f(x))^{-1}\,.$$

On démontre par récurrence sur $n \in \mathbb{N}$, que

$$f(x^n) = (f(x))^n\,.$$

Enfin, pour tout $n \in \mathbb{N}$, on peut écrire

$$f(x^{-n}) = f((x^n)^{-1}) = (f(x^n))^{-1} = (f(x)^n)^{-1} = f(x)^{-n}\,.$$

Ce qui termine la démonstration. □

***Proposition 2.8***. — *Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors*

(i) *Pour tout sous-groupe $H$ de $(G, *)$,*

$$f(H) = \{f(x) \in G' \,:\, x \in H\}$$

*est un sous-groupe de $(G', *')$.*

(ii) *Pour tout sous-groupe $H'$ de $(G', *')$,*

$$f^{-1}(H') = \{x \in G \,:\, f(x) \in H'\}$$

*est un sous-groupe de $(G, *)$.*

*Démonstration.* — Vérifions la première assertion. On a $e \in H$ donc, $e' = f(e) \in f(H)$. Soient $x', y' \in f(H)$. Alors il existe $x, y \in H$ tels que

$$x' = f(x) \quad \text{et} \quad y' = f(y)$$

Alors

$$x' *' y'^{-1} = f(x) *' (f(y))^{-1} = f(x) *' f(y^{-1}) = f(x * y^{-1}) \in f(H)\,,$$

car $H$ est un sous-groupe de $(G, *)$. Ce qui termine la démonstration de (i).

Vérifions maintenant la deuxième assertion. On a $e' \in H$ et $f(e) = e'$ donc $e \in f^{-1}(H')$. Soient $x, y \in f^{-1}(H')$, alors

$$f(x * y^{-1}) = f(x) *' f(y^{-1}) = f(x) *' (f(y))^{-1} \in H'\,,$$

car $H'$ est un sous-groupe de $(G', *')$. Ce qui termine la démonstration de (ii). □

***Définition 2.8***. — *Soit $f : G \longrightarrow G'$ un morphisme de groupes. On note*

$$\mathrm{Ker}\,(f) = f^{-1}(\{e'\}) := \{x \in H \,:\, f(x) = e'\}\,,$$

le noyau *de $f$ et on note*

$$\mathrm{Im}\,(f) = f(G) := \{f(x) \in G' \,:\, x \in G\}\,,$$

l'image *de $f$.*

***Proposition 2.9***. — *Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors $f$ est injectif si et seulement si* $\mathrm{Ker}\,(f) = \{e\}$.

*Démonstration.* — On suppose $f$ injectif et soit $x \in f^{-1}(\{e'\})$. Par définition, $f(x) = e' = f(e)$ donc $x = e$ et par conséquent $\mathrm{Ker}\,(f) = \{e\}$.

Inversement, supposons que $\mathrm{Ker}\,(f) = \{e\}$. Soient $x, y \in G$ tels que $f(x) = f(y)$. Alors, $f(x * y^{-1}) = f(x) *' (f(y))^{-1} = f(x) *' (f(x))^{-1} = e'$. Donc $x * y^{-1} \in \mathrm{Ker}\,(f)$ donc $x * y^{-1} = e$ et par conséquent $x = y$. Ce qui prouve bien que $f$ est injectif. □

***Proposition 2.10***. — *Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors,* $(\mathrm{Ker}\,(f), *)$ *est un sous-groupe de* $(G, *)$ *et* $(\mathrm{Im}\,(f), *')$ *est un sous-groupe de* $(G', *')$.

*Démonstration.* — C'est une conséquence facile de la proposition 2.8.

□

***Exemple 2.7***. — *Soit $H$ un sous-groupe de $(G, *)$. Vérifier que l'application $f : H \longrightarrow G$ définie par $f(x) = x$ est un morphisme de groupes (ce morphisme de groupe est appelé* injection canonique*).*

***Exemple 2.8***. — *L'application déterminant définie sur $GL_n(\mathbb{R})$, l'ensemble des matrices $n \times n$ à coefficients dans $\mathbb{R}$ qui sont inversibles est un morphisme de groupe (le groupe d'arrivée étant $(\mathbb{R}^*, .)$). En effet, si $A, B \in M_n(\mathbb{R})$ on a*

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

***Exemple 2.9***. — *Soit $(G, *)$ un groupe et $x$ un élément de $G$. L'application*

$$k \in \mathbb{Z} \longmapsto x^k \in G\,,$$

*est un morphisme de groupes.*

On démontre immédiatement le résultat suivant :

***Proposition 2.11***. — *La composée de morphismes de groupes est un morphisme de groupes.*

***Exemple 2.10***. — *On appelle groupe de Moebius les fractions rationnelles du type* $\dfrac{ax+b}{cx+d}$ *avec* $ad-bc \neq 0$. *On vérifie que la composition est une loi de composition interne et qui en fait bien un groupe, et que l'application de* $(GL_2(\mathbb{R}), \times)$ *dans le groupe de Moebius définie par*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \frac{ax+b}{cx+d}$$

*est un morphisme de groupe.*

Nous nous intéressons maintenant aux morphismes bijectifs.

***Définition 2.9***. — *Un* isomorphisme de groupes *est un morphisme de groupes bijectif. Un* automorphisme *est un isomorphisme d'un groupe dans lui même. On dit que deux groupes* $(G, *)$ *et* $(G', *')$ *sont isomorphes s'il existe un isomorphisme de* $(G, *)$ *dans* $(G', *')$. *On note alors* $(G, *) \simeq (G', *')$.

Si $G$ et $G'$ sont finis, cela signifie qu'ils ont la même table de composition (à une permutation des éléments près).

**Exemple:** $(\mathbb{Z}/n\mathbb{Z}, +)$ et le groupe $(U_n, \times)$ des racines n-ièmes de l'unité sont isomorphes, le morphisme étant l'application $\dot{k} \to e^{2ik\pi/n}$.

***Proposition 2.12***. — *Soit* $f$ *un isomorphisme de groupes, alors* $f^{-1}$ *est un isomorphisme de groupes.*

*Démonstration.* — Soient $x', y' \in G'$. On calcule en utilisant le fait que $f$ est un morphisme de groupes

$$f\left(f^{-1}(x') * f^{-1}(y')\right) = f(f^{-1}(x')) *' f(f^{-1}(y')) = x' *' y'$$

On compose par $f^{-1}$ pour conclure que

$$f^{-1}(x') * f^{-1}(y') = f^{-1}(x' *' y')$$

Ce qui montre que $f^{-1}$ est un morphisme de groupes. □

***Théorème 2.3***. — *L'ensemble* $\mathrm{Aut}\,(G)$ *des automorphismes du groupe* $(G, *)$ *muni de la loi de composition des applications* $\circ$ *est un groupe.*

*Démonstration.* — Laissé à titre d'exercice. □

***Exemple 2.11***. — *Soit* $(G, *)$ *un groupe. Pour tout* $a \in G$, *on note* $\sigma_a : G \longrightarrow G$ *l'application définie par*

$$\sigma_a(x) = a * x * a^{-1}$$

*C'est un automorphisme de* $G$ *appellé* automorphisme interne.

*L'application $\sigma : G \longrightarrow \mathrm{Aut}\,(G)$ définie par $\sigma(a) = \sigma_a$ est un morphisme de groupes. On vérifie que $\mathrm{Ker}\,\sigma$ est le centre de $G$ (voir Définition 1.4).*

***Exemple 2.12***. — *Soit $E$ un ensemble de cardinal $n$. Soit $f : E \longrightarrow \{1, \ldots, n\}$ une application bijective. On note $S_E$ l'ensemble des bijections de $E$ dans $E$, muni de $\circ$, la loi de composition des applications et on note*

$$F : S_E \longrightarrow S_n$$

*l'application définie par*

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

*pour tout $\sigma \in S_E$. Alors $F$ est un isomorphisme de groupes.*

***Proposition 2.13***. — *Soit $f : G \longrightarrow G'$ un morphisme de groupes. On suppose que $(G, *)$ et $(G', *')$ sont deux groupes finis de même cardinal. Si $f$ est injectif, alors $f$ est un isomorphisme de groupes.*

*Démonstration.* — Il faut montrer que $f$ est surjectif. Remarquons que $f$ étant injectif, le cardinal de l'image de $f$ est égal au cardinal de $G$ qui par hypothèse est égal au cardinal de $G'$. Donc $\mathrm{Im}\,(f) = G'$ ce qui montre que $f$ est surjectif. □

***Proposition 2.14***. — *Soit $f$ un isomorphisme du groupe $(G, *)$ dans le groupe $(G', *')$. On suppose que $(G, *)$ est abélien, alors $(G', *')$ est abélien.*

*Démonstration.* — Soient $x', y' \in G'$. On note $x = f^{-1}(x')$ et $y = f^{-1}(y')$. Le groupe $(G, *)$ étant abélien, on a $x * y = y * x$ donc, on peut écrire

$$x' *' y' = f(x) *' f(y) = f(x * y) = f(y * x) = f(y) *' f(x) = y' *' x'$$

Ce qui montre que $(G', *')$ est abélien. □

***Exemple 2.13***. — *Grâce à la proposition précédente, on peut vérifier que $(\mathbb{Z}/6\mathbb{Z}, \overline{+})$ et $(S_3, \circ)$ ne sont pas isomorphes. En effet, le premier groupe est abélien alors que le deuxième ne l'est pas (voir l'exemple 3.4).*

## 2.6. Sous-groupes distingués

Dans la démonstration du théorème de Lagrange, nous avons vu que, si $H$ est un sous-groupe de $G$, on peut considérer la relation d'équivalence

$$x \,\mathcal{R}\, y \quad \Longleftrightarrow \quad x * y^{-1} \in H$$

Une question naturelle est de savoir si cette relation est compatible avec la loi $*$; en effet, nous avons vu que c'est est une condition nécessaire pour pouvoir en déduire une loi de composition interne sur $G/H$. Rappelons qu'il faut vérifier que

$$\forall x, y, z, \qquad x \,\mathcal{R}\, y \quad \Longrightarrow \qquad x * a \;\mathcal{R}\; y * a \quad \text{et } a * x \;\mathcal{R}\; a * y.$$

En ce qui concerne le premier point, $x \mathcal{R} y$ s'écrit $x * y^{-1} \in H$ et donc

$$x * a * (y * a)^{-1} = x * y^{-1} \in H,$$

donc $x * a \ \mathcal{R} \ y * a$. La condition $a * x \ \mathcal{R} \ a * y$ s'écrit

$$a * x * y^{-1} * a^{-1} \in H;$$

cette condition n'a, en général, pas de raison de se déduire de la condition $x * y^{-1} \in H$. On notera toutefois qu'elle est trivialement vérifiée si $*$ est commutative.

Si $*$ n'est pas commutative, on introduit la définition suivante qui est donc motivée par le fait que l'on puisse quotienter $G$ par son sous-groupe $H$.

***Définition 2.10***. — *On dit qu'un sous-groupe $H$ de $(G, *)$ est* distingué *s'il est* stable par conjugaison*, c'est-à-dire si*

$$\forall x \in G, \quad \forall y \in H, \qquad x * y * x^{-1} \in H$$

*On notera $H \lhd G$.*

La motivation que nous avons donnée montre donc que, si $H$ est distingué, on en déduit une loi de composition interne sur $G/H$ qui en fait un groupe.

***Exemple 2.14***. — *On vérifie que $\{e\}$ et $G$ sont des sous-groupes distingués de $(G, *)$.*

***Exemple 2.15***. — *Si $*$ est commutative, tout sous-groupe de $G$ est distingué. Ainsi, l'ensemble $\mathbb{U} := \{z \in \mathbb{C} : |z| = 1\}$ des nombres complexes de module un est un sous-groupe distingué de $(\mathbb{C}^*, \cdot)$. Soit $n \in \mathbb{N}^*$. L'ensemble $\mathbb{U}_n := \{z \in \mathbb{C} : z^n = 1\}$ des racines n-ièmes de l'unité est un sous-groupe distingué de $(\mathbb{U}, \cdot)$.*

***Proposition 2.15***. — *L'intersection d'une famille de sous-groupes distingués de $(G, *)$ est un sous-groupe distingué de $(G, *)$.*

*Démonstration.* — Soient $(H_i)_{i \in I}$ une famille de sous-groupes distingués de $(G, *)$. On note $H = \cap_{i \in I} H_i$. On sait déjà que $H$ est un sous-groupe de $(G, *)$. Soit $x \in G$ et $y \in H$, pour tout $i \in I$, $y \in H_i$ donc $x * y * x^{-1} \in H_i$. Donc, $x * y * x^{-1} \in H$. Ce qui montre que $H$ est distingué. □

Rappelons que, d'après la Proposition 2.10, si $f : G \longrightarrow G'$ est un morphisme de groupe alors $(\mathrm{Im}\,(f), *')$ est un sous-groupe de $(G', *')$. Nous avons la proposition suivante, qui fournit une motivation supplémentaire pour l'étude des sous-groupes distingués, puisque ceux-ci apparaissent naturellement comme les noyaux des morphismes de groupes.

***Proposition 2.16***. — *Soit $f : G \longmapsto G'$ un morphisme du groupe $(G, *)$ dans le groupe $(G', *')$. Alors les propriétés suivantes sont vérifiées :*

(i) $\mathrm{Ker}\,(f) \lhd G$.
(ii) *Si* $H \lhd G$ *alors* $f(H) \lhd \mathrm{Im}\,(f) := \{f(x) \,:\, x \in G\}$.
(iii) *Si* $H' \lhd G'$ *alors* $f^{-1}(H') \lhd G$.

*Démonstration.* — Vérifions la première propriété. Soit $x \in \mathrm{Ker}\,(f)$ et $y \in G$. Calculons

$$\begin{aligned} f(y * x * y^{-1}) = f(y) *' f(x) *' f(y^{-1}) &= f(y) *' e' *' f(y^{-1}) \\ &= f(y) *' (f(y))^{-1} = e' \end{aligned}$$

donc $y * x * y^{-1} \in \mathrm{Ker}\,(f)$ ce qui montre que $\mathrm{Ker}\,(f)$ est un sous-groupe distingué de $(G, *)$.

Vérifions maintenant la deuxième propriété. On suppose que $H$ est un sous-groupe distingué de $(G, *)$. Soit $x' \in f(H)$ et $y' \in \mathrm{Im}\,(f)$. Il existe $x \in H$ tel que $x' = f(x)$ et $y \in G$ tel que $y' = f(y)$. Calculons

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

Étant donné que $H$ est un sous-groupe distingué de $(G, *)$, nous en déduisons que $y * x * y^{-1} \in H$. Donc $y' *' x *' y'^{-1} \in f(H)$. Ce qui montre que $f(H)$ est un sous-groupe distingué de $(\mathrm{Im}\,(f), *')$.

Enfin, vérifions la dernière propriété. On suppose que $H'$ est un sous-groupe distingué de $(G', *')$. Soit $x \in f^{-1}(H')$ et $y \in G$. Il existe un unique $x' \in H'$ tel que $f(x) = x'$. Calculons

$$f(y * x * y^{-1}) = f(y) *' f(x) *' (f(y^{-1})) = f(y) *' x' *' (f(y))^{-1} \in H'$$

car $H'$ est un sous-groupe distingué de $(G', *')$. Nous en déduisons que $y * x * y^{-1} \in f^{-1}(H')$, ce qui montre que $f^{-1}(H')$ est un sous-groupe distingué de $(G, *)$. □

***Exemple 2.16.*** — *L'ensemble* $SL_n(\mathbb{R})$ *des matrices* $n \times n$ *à coefficients dans* $\mathbb{R}$ *dont le déterminant est égal à* 1*, est un sous-groupe distingué de* $(GL_n(\mathbb{R}), .)$.

***Théorème 2.4.*** — *L'application* $\overline{f} : G/\mathrm{Ker}\, f \longrightarrow \mathrm{Im}\, f$ *est un isomorphisme de groupes.*

*Démonstration.* — On vérifie dans un premier temps que $\overline{f}$ est un morphisme de groupes (laissé en exercice). Ensuite, $\overline{f}$ est injective. En effet, si $\overline{x} = x\,\mathrm{Ker} f$ vérifie $\overline{f}(\overline{x}) = e'$ alors, $f(x) = e'$ donc $x \in \mathrm{Ker} f$. En particulier $x\,\mathrm{Ker} f = \mathrm{Ker}\, f = \overline{e}$. Enfin, on vérifie que $\overline{f}$ est surjective. En effet, si $y \in \mathrm{Im}\, f$ alors, il existe $x \in G$ tel que $f(x) = y$. Si $\overline{x} = x\,\mathrm{Ker} f$, on peut écrire, $\overline{f}(\overline{x}) = f(x) = y$. Ce qui termine la démonstration. □

On résume cela avec le schéma suivant:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \downarrow & & \uparrow i \\ G/\operatorname{Ker} f & \xrightarrow{\overline{f}} & \operatorname{Im} f \end{array}$$

où $i$ est l'injection canonique de $\operatorname{Im} f$ dans $G'$ définie tout simplement par $i(x) = x$, est un diagramme commutatif, c'est-à-dire que $\overline{f}$ est l'unique isomorphisme de groupes tel que

$$f = i \circ \overline{f} \circ \pi$$

***Corollaire 2.1***. — *Si $(G, *)$ et $(G', *')$ sont des groupes finis et $f : G \to G'$ est un morphisme alors*

$$|G| = |\ker f|\,|\operatorname{Im} f|.$$

*Démonstration.* — Comme $\overline{f}$ est un isomorphisme, on a

$$|G/\ker f| = |\operatorname{Im} f|.$$

D'après le théorème de Lagrange, le membre de gauche vaut $|G|/|\ker f|$, ce qui donne le résultat voulu. □

# CHAPITRE 3

# QUELQUES EXEMPLES DE GROUPES

## 3.1. Groupes monogènes et groupes cycliques

***Définition 3.1***. — *On dit qu'un groupe* $(G, *)$ *est* monogène *s'il existe* $x \in G$ *tel que* $G =< x >$. *On dit alors que* $G$ *est engendré par* $x$ *ou bien que* $x$ *est un générateur de* $G$.

On remarque qu'un groupe monogène est abélien.

***Exemple 3.1***. — *Le groupe* $(\mathbb{Z}, +)$ *est monogène. Il a exactement deux générateurs, qui sont* $1$ *et* $-1$.

***Définition 3.2***. — *On dit qu'un groupe* $(G, *)$ *est* cyclique *s'il est monogène et fini, autrement dit, si* $G$ *est fini et s'il existe* $x \in G$ *tel que* $G =< x >$.

***Exemple 3.2***. — *Soit* $n \geq 1$. *Le groupe* $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ *un groupe cyclique, engendré par* $\dot{1}$.

***Définition 3.3***. — *Soit* $(G, *)$ *un groupe et* $x \in G$. *On dit que* $x$ *est* d'ordre fini *si* $< x >$ *est fini (donc cyclique) et si tel est le cas, le cardinal de* $< x >$ *est appelé* ordre de $x$.

***Exemple 3.3***. — *Soit* $n \in \mathbb{N}^*$. *Vérifier que* $(\mathbb{U}_n, \cdot)$ *où*

$$\mathbb{U}_n = \{e^{2i\pi \frac{k}{n}} \in \mathbb{C} : k \in \mathbb{Z}\},$$

*est l'ensemble des racines* $n^{ièmes}$ *de l'unité, est un groupe cyclique.*

Voici maintenant une conséquence directe du théorème de Lagrange.

***Proposition 3.1***. — *Soit* $(G, *)$ *un groupe fini de cardinal* $p$ *où* $p$ *est un nombre premier. Alors* $G$ *est cyclique.*

*Démonstration*. — Soit $x \in G$ tel que $x \neq e$. Alors, l'ordre de $x$ divise $p$ et est $\geq 2$. Donc l'ordre de $x$ est égal à $p$. □

***Proposition 3.2.*** — *Soit $(G,*)$ un groupe et $x$ un élément de $G$. Alors l'ensemble $H$ des entiers relatifs $m$ tels que $x^m = e$ est un sous-groupe de $\mathbb{Z}$. Plus précisément:*

- *Si $x$ est d'ordre infini, alors $H = \{0\}$.*
- *Si $x$ est d'ordre fini $n$ alors $H = n\mathbb{Z}$ et $n$ est aussi le plus petit entier de $\mathbb{N}^*$ tel que $x^n = e$. On a alors $< x >= \{e, x, \ldots, x^{n-1}\}$.*

*Démonstration.* — On considère le morphisme

$$\Phi \ : \ \left\{ \begin{array}{ccc} (\mathbb{Z},+) & \longrightarrow & (< x >, *) \\ k & \longmapsto & x^k. \end{array} \right.$$

On sait que $\ker \Phi$ est un sous-groupe de $(\mathbb{Z},+)$, donc il existe $k \in \mathbb{N}$ tel que $\ker \Phi = k\mathbb{Z}$.

Premier cas : $k = 0$. Alors $\Phi$ est injective et $x$ est donc d'ordre infini. Deuxième cas : $k > 0$. Alors tout entier $m$ tel que $x^m = e$ est multiple de $k$. Donc $k$ est bien le plus petit entier strictement positif ayant cette propriété. Montrons que

$$< x >= \{e, x, \ldots, x^{k-1}\}. \tag{1}$$

En effet, si $y \in < x >$ alors il existe $m$ tel que $y = x^m$. En effectuant la division euclidienne par $k$: $m = ak + r$ avec $r \in \{0, \cdots, k-1\}$, on trouve

$$x^m = x^{ak+r} = (x^k)^a * x^r = e * x^r = x^r.$$

Finalement les éléments de $= \{e, x, \ldots, x^{k-1}\}$ sont bien deux à deux distincts car si l'on considère deux éléments $x^p$ et $x^q$ dans cet ensemble avec, par exemple $p \leq q$, tels que $x^p = x^q$, alors on a $x^{q-p} = e$, et donc $k$ divise $q - p$. Mais comme $0 \leq q - p < k$, on doit avoir $q = p$. On obtient donc (1) et le fait que card $< x >= k$. On en conclut que $k = n$. □

Donnons une conséquence importante de la proposition ci-dessus, pour les groupes monogènes.

***Corollaire 3.1.*** — *Soit $G$ un groupe monogène de générateur $x$.*

- *Si $G$ est infini alors $G = \{x^n, n \in \mathbb{Z}\}$ et les éléments de l'ensemble de droite sont deux à deux distincts.*
- *Si $G$ est fini alors $G = \{e, x, \ldots, x^{n-1}\}$ où $n$ est l'ordre de $x$. En particulier l'ordre de tout générateur de $(G,*)$ est égal au cardinal de $G$.*

***Corollaire 3.2.*** — *Soit $(G,*)$ un groupe monogène engendré par $x \in G$.*

(i) *Si $G$ est infini, alors l'application $\Phi : n \in \mathbb{Z} \longmapsto x^n \in G$ est un isomorphisme de groupes. En particulier, $(G,*)$ est isomorphe à $(\mathbb{Z},+)$.*

(ii) *Si $G$ est cyclique de cardinal $n$, l'application*

$$\dot{k} \in \mathbb{Z}/n\mathbb{Z} \longmapsto x^k \in G\,,$$

*( où $k \in \dot{k}$) est un isomorphisme de groupes. En particulier $(G, *)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$.*

*Démonstration.* — Dans le cas où $G$ est infini, la proposition ci-dessus assure que $\ker \Phi = \{0\}$, et la surjectivité découle du fait que $x$ engendre $G$. En conséquence, $\Phi$ est un isomorphisme de $(\mathbb{Z}, +)$ dans $(G, *)$.

Si $G$ est cyclique d'ordre $n$ alors $\ker \Phi = n\mathbb{Z}$. On considère alors l'application $f$ définie par $f(\dot{k}) = x^k$ où $k \in \dot{k}$. Il faut vérifier que cette application est bien définie. Or si $k, k' \in \dot{k}$, on peut écrire $k' = k + q\,n$ où $q \in \mathbb{Z}$. En particulier

$$x^{k'} = x^k * (x^n)^q = x^k$$

Donc $f(\dot{k})$ ne dépend pas du représentant choisi dans $\dot{k}$. On vérifie que c'est un morphisme de groupes (le faire). L'application $f$ est surjective car $x$ engendre $G$. Comme $G$ et $\mathbb{Z}/n\mathbb{Z}$ ont même cardinal, le lemme 2.1 implique que $f$ est bijective, et est donc un isomorphisme. □

***Proposition 3.3.*** — *Soit $n \in \mathbb{N}^*$. Les générateurs de $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ sont de la forme $\dot{a}$ où $a$ et $n$ sont premiers entre eux.*

*Démonstration.* — Soit $\dot{a} \in \mathbb{Z}/n\mathbb{Z}$ un générateur de $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$. Alors, il existe $u \in \mathbb{N}$ tel que

$$u\,\dot{+} = \dot{1}$$

Autrement dit, $1 - u\,a$ est un multiple de $n$. Donc, il existe $v \in \mathbb{Z}$ tel que

$$a\,u + n\,v = 1\,,$$

on en déduit que $a$ et $n$ sont premiers entre eux. Inversement, si $a$ et $n$ sont premiers entre eux, le Théorème de Bézout nous assure qu'il existe $u, v \in \mathbb{Z}$ tels que

$$a\,u + n\,v = 1.$$

Alors, $u\,\dot{a} = \dot{1}$ dans $\mathbb{Z}/n\mathbb{Z}$. On vérifie alors que $\dot{a}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$. □

L'exemple 3.1 et la Proposition 3.3 sont des cas particuliers du résultat général suivant :

***Théorème 3.1.*** — *Soit $(G, *)$ un groupe monogène de générateur $x$. Alors :*

(i) *si $G$ est infini, les générateurs de $G$ sont $x$ et $x^{-1}$ ,*
(ii) *si $G$ est fini de cardinal $n$ (donc $G$ est cyclique), les générateurs de $G$ sont de la forme $x^k$ où $k$ et $n$ sont premiers entre eux.*

*Démonstration.* — Soit $x'$ un générateur de $G$. On a $x' \in G =< x >$ donc, il existe $k \in \mathbb{Z}$ tel que

$$x' = x^k \, .$$

Inversement, $x \in G =< x' >$ donc, il existe $k' \in \mathbb{Z}$ tel que

$$x = x'^{\,k'} \, .$$

En particulier

$$x = x^{k\,k'} \, ,$$

autrement dit

$$x^{k\,k'-1} = e \, .$$

On suppose que $G$ est infini. Remarquons que, pour tout $\ell \in \mathbb{Z}^*$, $x^\ell \neq e$ (autrement $< x >$ n'aurait qu'un nombre fini d'éléments). Donc dans ce cas on a nécessairement $k\,k' - 1 = 0$ donc $k, k' \in \{\pm 1\}$.

On suppose maintenant que $G$ est fini. Dans ce cas, $k\,k' - 1$ est un multiple de $n$, le cardinal de $G$ (qui est aussi l'ordre de $x$). Donc, $k$ et $n$ sont premiers entre eux. Inversement, si $k$ et $n$ sont premiers entre eux, on peut appliquer le Théorème de Bézout : il existe $u, v \in \mathbb{Z}$ tels que

$$k\,u + n\,v = 1$$

alors

$$x'^u = x^{k\,u} = x^{k\,u+n\,v} = x$$

donc $< x'^u >=< x >$ et $x'$ est donc un générateur de $G$. □

Enfin, démontrons la :

***Proposition 3.4.*** — † *Soit $(G, *)$ un groupe cyclique. Alors, tous les sous-groupes de $(G, *)$ sont cycliques.*

*Démonstration.* — Soit $x$ un générateur de $(G, *)$. On a vu que

$$G = \{e, x, x^2, \ldots, x^{n-1}\} \, ,$$

où $n$ est le cardinal de $G$. Soit $H$ un sous-groupe de $G$. On note

$$m = \min\{p \in \{1, \ldots, n-1\} \, : \, x^p \in H\} \, ,$$

et

$$h = x^m \in H \, .$$

Soit $y \in H$, il existe $p \in \{0, 1, \ldots, n-1\}$ tel que $y = x^p$. Effectuons la division euclidienne de $p$ par $m$

$$p = q\,m + r$$

où $r \in \{0, \ldots, m-1\}$. On constate que

$$x^r = x^{p-q\,m} = x^p * (x^m)^{-q} = y * h^q \in H \, ,$$

comme produit d'éléments de $H$. Par définition de $m$, nécessairement $r = 0$ et par conséquent $y = h^q$. On a donc montré que $H =< h >$, ce qui termine la démonstration du résultat. □

## 3.2. Le groupe des permutations

Soit $n \in \mathbb{N}^*$. On note $S_n$ l'ensemble des bijections de $\{1, \ldots, n\}$ dans lui même. On munit $S_n$ de la loi $\circ$ de composition des applications. On vérifie que la loi $\circ$ est associative, que l'application identité est l'élément neutre et que le symétrique d'un élément de $S_n$ est la bijection réciproque.

***Définition 3.4***. — *On dit que* $(S_n, \circ)$ *est le* groupe des permutations *de l'ensemble* $\{1, \ldots, n\}$*, on dit aussi que c'est le* groupe symétrique d'ordre $n$*.*

***Proposition 3.5***. — *Le cardinal de* $S_n$ *est égal à* $n!$*.*

*Démonstration.* — Pour définir un élément de $S_n$, il faut déterminer l'image de 1 pour laquelle on a $n$ choix possibles, puis, l'image de 2 pour laquelle on a $n-1$ choix possibles, ... et enfin l'image de $n$ pour laquelle on a un seul choix. Donc au total $n!$ choix possibles. □

Soit $\sigma \in S_n$. On pourra représenter l'application $k \longmapsto \sigma(k)$ sous la forme d'une matrice à 2 lignes.

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

Cette notation est utile pour calculer la composition de deux éléments de $S_n$. Donnons un exemple quand $n = 4$. Considérons $\sigma, \sigma' \in S_4$ données par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \qquad \text{et} \qquad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Alors

$$\sigma \circ \sigma' = \begin{pmatrix} \mathbf{1} & 2 & 3 & 4 \\ \mathbf{2} & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{2} & 3 & 4 \\ 2 & \mathbf{1} & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{2} & 3 & 4 \\ 3 & \mathbf{2} & 4 & 1 \end{pmatrix}.$$

Pour déterminer l'image de 2 par $\sigma \circ \sigma'$ on détermine l'image de 2 par $\sigma'$ en regardant la deuxième matrice, on trouve 1, ensuite on détermine l'image de 1 par $\sigma$ en regardant la première matrice.

***Exemple 3.4***. — *On considère* $S_3$*, dont les éléments sont notés*

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

*et*

$$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

*Donc* $S_3 = \{e, r_1, r_2, s_1, s_2, s_3\}$. *Vérifier que la table de composition de la loi* $\circ$ *est donnée par*

| $\circ$ | $e$ | $r_1$ | $r_2$ | $s_1$ | $s_2$ | $s_3$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r_1$ | $r_2$ | $s_1$ | $s_2$ | $s_3$ |
| $r_1$ | $r_1$ | $r_2$ | $e$ | $s_3$ | $s_1$ | $s_2$ |
| $r_2$ | $r_2$ | $e$ | $r_1$ | $s_2$ | $s_3$ | $s_1$ |
| $s_1$ | $s_1$ | $s_2$ | $s_3$ | $e$ | $r_1$ | $r_2$ |
| $s_2$ | $s_2$ | $s_3$ | $s_1$ | $r_2$ | $e$ | $r_1$ |
| $s_3$ | $s_3$ | $s_1$ | $s_2$ | $r_1$ | $r_2$ | $e$ |

*Remarquer que* $(S_3, \circ)$ *n'est pas abélien. On retrouve la table que nous avons déjà trouvée dans l'exemple 1.13.*

***Définition 3.5***. — *On suppose que* $n \geq 2$. *On dit que* $\sigma \in S_n$ *est une* transposition *s'il existe* $i \neq j$ *tels que*

$$\sigma(i) = j\,, \qquad \sigma(j) = i\,, \qquad \text{et} \qquad \sigma(k) = k\,,$$

*pour tout* $k \neq i, j$.

*La transposition de* $S_n$ *qui échange* $i$ *et* $j$ *est parfois notée* $\tau_{i,j}$.

***Remarque 3.1***. — *Une transposition est une* involution, *c'est-à-dire qu'elle est égale à sa bijection réciproque.*

***Théorème 3.2***. — *Toute permutation de* $S_n$ *est le produit d'au plus* $n-1$ *transpositions.*

*Démonstration.* — La démonstration repose sur une récurrence sur $n \geq 2$. Pour $n = 2$, le résultat est vrai car $S_2$ ne contient que deux éléments : l'application identité et la transposition qui échange 1 et 2.

On suppose que le résultat est vrai pour $S_n$, autrement dit que que toute permutation de $S_n$ est le produit d'au plus $n-1$ transpositions. Soit $\sigma \in S_{n+1}$. On distingue deux cas.

Premièrement, supposons que $\sigma(n+1) = n+1$. Dans ce cas on peut définir $\overline{\sigma} \in S_n$ de la manière suivante

$$\overline{\sigma}(k) = \sigma(k) \quad \text{pour} \quad k \in \{1, \cdots, n\}.$$

On vérifie que $\overline{\sigma}$ est bien une bijection de $\{1,\dots,n\}$ sur lui même. On peut alors appliquer l'hypothèse de récurrence et écrire $\overline{\sigma}$ comme la composée d'au plus $n-1$ transpositions de $S_n$.

$$\overline{\sigma} = \overline{\tau}_1 \circ \ldots \circ \overline{\tau}_k$$

où $k \leq n-1$ et où les $\overline{\tau}_i$ sont des transpositions de $S_n$. Pour tout $i = 1,\dots,k$, on note $\tau_i$ la transposition de $S_{n+1}$ définie par

$$\tau_i(j) = \overline{\tau}_i(j)\,,$$

pour tout $j = 1,\dots,n$ et

$$\tau_i(n+1) = n+1\,.$$

Alors on vérifie que

$$\sigma = \tau_1 \circ \ldots \circ \tau_k$$

Conclusion, $\sigma$ est la composée d'au plus $n-1$ transpositions.

Supposons maintenant que $\sigma(n+1) \neq n+1$. On note $\tau$ la transposition de $S_{n+1}$ définie par

$$\tau(\sigma(n+1)) = n+1$$

et

$$\tau(i) = i \quad \text{si} \quad i \notin \{\sigma(n+1), n+1\}.$$

Alors $\sigma' = \tau \circ \sigma$ est une permutation de $S_{n+1}$ qui vérifie $\sigma'(n+1) = n+1$. D'après ce que l'on vient de voir, on peut l'écrire comme la composée d'au plus $n-1$ transpositions

$$\sigma' = \tau_1 \circ \ldots \circ \tau_k$$

où $k \leq n-1$ et où les $\tau_i$ sont des transpositions de $S_{n+1}$. Conclusion,

$$\sigma = \tau^2 \circ \sigma = \tau \circ \tau_1 \circ \ldots \circ \tau_k$$

et $\sigma$ est bien la composée d'au plus $n$ transpositions. Le principe de récurrence nous permet d'affirmer que le résultat est vrai pour tout $n \geq 2$. □

Pour tout $i = 1,\dots,n-1$, on note $\tau_i$ la transposition de $S_n$ telle que

$$\tau_i(i) = i+1 \qquad \tau_i(i+1) = i \qquad \text{et} \qquad \tau_i(k) = k$$

pour tout $k \notin \{i, i+1\}$. On démontre la :

***Proposition 3.6***. — † *Toute permutation de $S_n$ est le produit de transpositions de la forme $\tau_i$, pour $i = 1,\dots,n-1$. Autrement dit, si $X = \{\tau_1,\dots,\tau_{n-1}\}$, alors $S_n =< X >$.*

### 3.3. $k$-cycles †

On a la définition suivante qui généralise la notion de transposition :

***Définition 3.6***. — *On suppose que $n \geq 2$ et $k \in \{1, \dots, n\}$. On dit que $\sigma \in S_n$ est un* $k$-cycle *s'il existe $i_1, i_2, \dots, i_k$ deux à deux distincts, tels que*

$$\sigma(i_1) = i_2\,, \qquad \sigma(i_2) = i_3\,, \qquad \dots \qquad \sigma(i_{k-1}) = i_k\,, \qquad \sigma(i_k) = i_1\,,$$

*et*

$$\forall j \notin \{i_1, \dots, i_k\}, \qquad \sigma(j) = j\,.$$

*On dit que $\{i_1, \dots, i_k\}$ est le* support *du $k$-cycle $\sigma$.*

*Le $k$-cycle décrit ci-dessus est parfois noté $(i_1\ i_2\ \dots\ i_k)$.*

***Remarque 3.2***. — *Un 2-cycle est une transposition.*

Voici quelques propriétés élémentaires des $k$-cycles.

***Lemme 3.1***. — *Si $\sigma \in S_n$ est un $k$-cycle alors $\sigma^k = Id$.*

***Lemme 3.2***. — *Deux cycles de $S_n$, dont les supports sont disjoints, commutent.*

On souhaite maintenant démontrer le :

***Théorème 3.3***. — *Une permutation de $S_n$ peut s'écrire comme le produit de cycles de supports disjoints.*

La démonstration de ce résultat repose sur la notion d'orbite d'un point sous l'action d'un élement de $S_n$ :

***Définition 3.7***. — *Soit $s \in \{1, \dots, n\}$ et $\sigma \in S_n$. On note*

$$O_s = \{\sigma^k(s) \,:\, k \in \mathbb{Z}\}\,,$$

l'orbite de $s$ sous l'action de $\sigma$.

***Lemme 3.3***. — *Soit $\sigma \in S_n$. Les orbites des points de $\{1, \dots, n\}$ sous l'action de $\sigma$ forment une partition de $\{1, \dots, n\}$. Autrement dit, il existe $s_1, \dots, s_k \in \{1, \dots, n\}$, distincts tels que*

$$O_{s_1} \cup \dots \cup O_{s_k} = \{1, \dots, n\}$$

*et*

$$\forall i \neq j, \qquad O_{s_i} \cap O_{s_j} = \emptyset.$$

*Démonstration.* — On remarque que deux orbites sont soit égales soit disjointes. En effet, si $O_s \cap O_{s'} \neq \emptyset$, alors il existe $k, k' \in \mathbb{N}$ tels que

$$\sigma^k(s) = \sigma^{k'}(s')$$

En composant par $\sigma^{-k}$ on conclut que

$$s = \sigma^{k'-k}(s')$$

donc que $s \in O_{s'}$. En particulier, pour tout $\ell \in \mathbb{Z}$, les images de $s$ par $\sigma^\ell$ sont aussi dans $O_{s'}$ donc $O_s \subset O_{s'}$. On montre de la même façon que $O_{s'} \subset O_s$, conclusion, $O_s = O_{s'}$.

Enfin, remarquons que tout élément $s$ de $\{1, \ldots, n\}$ appartient au moins à une orbite sous l'action de $\sigma$ : l'orbite de $s$ sous l'action de $\sigma$. Les orbites des élements de $\{1, \ldots, n\}$ sous l'action de $\sigma$ forment bien une partition de $\{1, \ldots, n\}$. □

*Démonstration du Théorème 3.3.* — Soit $\sigma \in S_n$. On considère une partition de $\{1, \ldots, n\}$ en orbites sous l'action de $\sigma$, deux à deux disjointes

$$\{1, \ldots, n\} = O_1 \cup \ldots \cup O_k \,.$$

Pour tout $j \in \{1, \ldots, k\}$, on note $\phi_j$ le cycle défini par

$$\phi_j(s) = \sigma(s) \qquad \text{si} \quad s \in O_j$$

et

$$\phi_j(s) = s \qquad \text{si} \quad s \notin O_j$$

Les cycles $\phi_1, \ldots, \phi_k$ ayant des supports disjoints, ils commutent et, par construction, si $s \in O_j$ alors $\phi_j(s) = \sigma(s)$ et $\phi_i(s) = s$ si $i \neq j$. Donc

$$\phi_1 \circ \ldots \circ \phi_j(s) = \sigma(s).$$

On a donc démontré que $\sigma$ était le produit de cycles dont les supports sont deux à deux disjoints. □

***Exemple 3.5***. — *Considérons $\sigma \in S_6$ donnée par*

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

*Les orbites des éléments de $\{1, \ldots, 6\}$ sous l'action de $\sigma$ sont*

$$O_1 = \{1, 3, 5\}, \qquad O_2 = \{2\} \qquad \text{et} \qquad O_4 = \{4, 6\}.$$

*Donc $\sigma$ est le produit d'un 2-cycle et d'un 3-cycle comme suit :*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 6 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}.$$

### 3.4. Signature d'une permutation

Rappelons qu'une paire est un ensemble à deux éléments.

***Définition 3.8.*** — *Soit $\sigma \in S_n$, la* signature *de $\sigma$ est définie par la formule*

$$\mathrm{sign}(\sigma) = \prod_{1\le i<j\le n} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(j)-\sigma(i)}{j-i}\,,$$

*où $\mathcal{P}$ est l'ensemble des* paires *de $\{1,\cdots,n\}$.*

***Proposition 3.7.*** — *L'application* sign *est un homomorphisme du groupe $(S_n,\circ)$ dans $(\{-1,1\},\times)$. Autrement dit, pour tout $\sigma\in S_n$, on a $\mathrm{sign}(\sigma)\in\{\pm1\}$, et pour tout $\sigma,\sigma'\in S_n$*

$$\mathrm{sign}(\sigma\circ\sigma') = \mathrm{sign}(\sigma)\,\mathrm{sign}(\sigma')\,.$$

*De plus, si $\tau\in S_n$ est une transposition alors*

$$\mathrm{sign}(\tau) = -1\,.$$

*Démonstration.* — Dans la formule définissant $\mathrm{sign}(\sigma)$ les termes du numérateur et du dénominateur sont les mêmes au signe près, car l'application $(i,j)\mapsto(\sigma(i),\sigma(j))$ est une bijection de l'ensemble $\mathcal{P}$ dans lui-même. Donc $\sigma$ est à valeurs dans $\{-1,1\}$. Pour calculer $\mathrm{sign}(\sigma\circ\sigma')$, on écrit

$$\begin{aligned}\mathrm{sign}(\sigma\circ\sigma') &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma\circ\sigma'(j)-\sigma\circ\sigma'(i)}{j-i}\\ &= \Big(\prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma\circ\sigma'(j)-\sigma\circ\sigma'(i)}{\sigma'(j)-\sigma'(i)}\Big)\Big(\prod_{\{k,\ell\}\in\mathcal{P}} \frac{\sigma'(\ell)-\sigma'(k)}{\ell-k}\Big).\end{aligned}$$

Comme l'ensemble $\mathcal{P}$ est invariant par l'action de $\sigma$, on en déduit en posant $i'=\sigma(i)$ et $j'=\sigma(j)$ dans le premier produit, que

$$\begin{aligned}\mathrm{sign}(\sigma\circ\sigma') &= \Big(\prod_{\{i',j'\}\in\mathcal{P}} \frac{\sigma(j')-\sigma(i')}{j'-i'}\Big)\Big(\prod_{\{k,\ell\}\in\mathcal{P}} \frac{\sigma'(\ell)-\sigma'(k)}{\ell-k}\Big)\\ &= \mathrm{sign}(\sigma)\,\mathrm{sign}(\sigma')\end{aligned}$$

Enfin, si $\tau$ est une transposition (par exemple telle que $\tau(i_0)=j_0$ et $\tau(j_0)=i_0$ pour un couple $i_0<j_0$) on remarque que dans la formule qui donne $\mathrm{sign}(\tau)$ les termes du dénominateur sont tous positifs alors que les termes du numérateur sont tous positifs sauf $\tau(j_0)-\tau(i_0)$ et les termes de la forme

$$\tau(j_0)-\tau(k) \qquad \text{et} \qquad \tau(k)-\tau(i_0) \qquad \text{pour} \qquad k=i_0+1,\ldots,j_0-1$$

Il y a $2(j_0-i_0)-1$ tels termes donc $\mathrm{sign}(\tau)$, qui est le produit d'un nombre impair de $-1$, est égal à $-1$. □

***Remarque 3.3***. — *L'ensemble des* $\sigma$ *de* $S_n$ *de signature* 1 *est un sous-groupe distingué (car noyau d'un morphisme de groupe) de* $(S_n, \circ)$, *appelé* groupe alterné.

# CHAPITRE 4

# ANNEAUX ET CORPS

## 4.1. Définition et exemples

Soit $A$ un ensemble muni de deux lois de composition internes $+$ et $\times$ (on utilisera donc les notations usuelles pour $\mathbb{R}$).

***Définition 4.1***. — *On dit que* $(A, +, \times)$ *est un* anneau *si les propriétés suivantes sont vérifiées :*

(i) $(A, +)$ *est un groupe additif (i.e. commutatif) d'élément neutre* $0_A$.
(ii) *Il existe un élément neutre* $1_A$ *pour la loi* $\times$.
(iii) *La loi* $\times$ *est associative:*

$$\forall x, y, z \in A\,, \qquad x \times (y \times z) = (x \times y) \times z\,.$$

(iv) *La loi* $\times$ *est* distributive *par rapport à la loi* $+$*:*

$$\forall x, y, z \in A\,, \qquad x \times (y+z) = x \times y + x \times z \quad \text{et} \quad (x+y) \times z = x \times z + y \times z\,.$$

*Si de plus la loi* $\times$ *est commutative, on dit que l'anneau est* commutatif.

La distributivité de la loi $\times$ par rapport à la loi $+$ permet de démontrer quelques propriétés élémentaires des anneaux :

***Proposition 4.1***. — *Soit* $(A, +, \times)$ *un anneau, alors :*

(i) $\forall a \in A$, $0_A \times a = a \times 0_A = 0_A$.
(ii) $\forall a, b \in A$, $-(a \times b) = (-a) \times b = a \times (-b)$.
(iii) *Si* $1_A = 0_A$ *alors* $A = \{0_A\}$.

*Démonstration.* — Pour démontrer la première propriété, il suffit d'utiliser la distributivité de $\times$ par rapport à la loi $+$, pour écrire

$$a = a \times 1_A = a \times (1_A + 0_A) = a \times 1_A + a \times 0_A = a + a \times 0_A\,,$$

donc $a \times 0_A = 0_A$.

Pour démontrer la deuxième propriété, on utilise une fois de plus la distributivité de $\times$ par rapport à $+$, on peut alors écrire

$$0_A = (a + (-a)) \times b = a \times b + (-a) \times b\,,$$

donc $(-a) \times b = -(a \times b)$. On montre de même que $a \times (-b) = -(a \times b)$.

Enfin, si $1_A = 0_A$, on peut utiliser la propriété (i) qui permet décrire

$$a = 1_A \times a = 0_A \times a = 0_A\,,$$

donc $A$ est réduit à un élément. □

***Exemple 4.1***. — *Vérifier que les ensembles suivants sont munis d'une structure d'anneau commutatif*

$$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), \qquad (\mathbb{C}, +, \cdot) \qquad \text{et} (\mathbb{Z}/n\mathbb{Z}, +, \cdot).$$

*(pour ce dernier exemple, on vérifiera que la propriété de distributivité est conservée par passage au quotient)*

***Exemple 4.2***. — *Soit $E$ un ensemble et $\mathcal{P}(E)$ l'ensemble des parties de $E$ muni de la différence symétrique $\Delta$ et de de l'intresection. Alors $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif. L'élement neutre pour "l'addition" ($\Delta$) est $\emptyset$ et l'élement neutre pour "la multiplication" ($\cap$) est $E$.*

***Exemple 4.3***. — *Soit $n \geq 2$. Vérifier que $(M_n(\mathbb{R}), +, \times)$ est un anneau non commutatif.*

***Exemple 4.4***. — **Polynômes:** *On rappelle que, formellement, un polynôme à coefficients dans un anneau $A$ est un élément de $A^{\mathbb{N}}$ (c'est à-dire est une suite infinie d'éléments de $A$) nul à partir d'un certain rang. Cette suite s'écrit donc $(a_0, a_1, a_2, \cdots a_n, 0, 0, \cdots)$. Le plus petit $n$ tel que $\forall m > n, a_m = 0$ s'appelle le degré du polynôme. Par convention, on dit que le degré du polynôme nul est -$\infty$. Les polynômes sont munis d'une addition (l'addition usuelle des suites, terme à terme) et d'un produit défini de la façon suivante:*

$$si \quad a = (a_0, a_1, a_2, \cdots a_n, 0, 0, \cdots) \quad et \quad b = (b_0, b_1, b_2, \cdots b_l, 0, 0, \cdots),$$

*le produit $c = a \times b$ est la suite $c = (c_0, c_1, c_2, \cdots c_m, 0, 0, \cdots)$ (définie par*

$$\forall k, \qquad c_k = \sum_{p=0}^{k} a_p b_{k-p}.$$

*(on vérifie facilement que cette suite est effectivement nulle au delà du rang $m = n + l$).*

*L'élément neutre pour la multiplication est la suite $(1, 0, 0, 0 \cdots)$ que l'on note donc $1$. On note traditionnellement $X$ la suite $(0, 1, 0, 0, 0 \cdots)$. On vérifie que $X^n = X \times X...$ (n fois) est la suite*

$$X^n = (0, 0, \cdots 0, 1, 0, \cdots),$$

*où le 1 est à la n+1 ième position. Tout polynôme peut donc s'écrire* $\sum_{k=0}^{n} a_k X^k$. *On évitera de confondre un polynôme avec son évaluation en* $x \in A$ *qui est l'application de* $A$ *dans* $A$ *définie par* $P(x) = \sum_{k=0}^{n} a_k x^k$ *(vérifier que cette application est injective si* $A = \mathbb{R}$ *ou* $\mathbb{C}$ *mais que ce n'est plus la cas si* $A$ *est fini.*

*L'ensemble* $\mathbb{A}[X]$ *des polynômes à une indéterminée à coefficients dans un anneau commutatif* $A$*, muni des lois d'addition et de multiplication des polynômes, est un anneau commutatif.*

***Exemple 4.5***. — *Soit* $k \geq 2$. *On peut définir par récurrence l'anneau des polynômes à* $k$ *indéterminées par*

$$\mathbb{R}[X_1, \ldots, X_k] = \mathbb{R}[X_1, \ldots, X_{k-1}][X_k]\,.$$

*qui, muni de l'addition et de la multiplication naturelles, est un anneau.*

***Exemple 4.6***. — *Soit* $O$ *un intervalle de* $\mathbb{R}$ *et* $\mathcal{C}(O)$ *l'ensemble des fonctions continues sur* $O$*, muni de l'addition et du produit usuels des fonctions. Alors* $\mathcal{C}(O)$ *est un anneau.*

***Exemple 4.7***. — *Soit* $D$ *le disque unité ouvert de* $\mathbb{C}$ *(*$D = \{z : \quad |z| < 1\}$*). Alors l'ensemble* $A$ *des séries entières*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n$$

*dont le rayon de convergence est 1, et telles que* $f$ *se prolonge en une fonction continue sur* $\overline{D}$ *(muni de l'addition et de la multiplication), est un anneau.*

Dans les anneaux, on a la *formule du binôme de Newton* :

***Proposition 4.2*** **(Formule du binôme)**. — *Soit* $(A, +, \times)$ *un anneau et* $a, b \in A$ *deux éléments qui commutent*

$$a \times b = b \times a$$

*Alors, pour tout* $n \in \mathbb{N}$*, on a*

$$(a+b)^n = \sum_{k=0}^{n} C_n^k\, a^k \times b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^k \times b^{n-k}$$

*avec* $C_n^k = \binom{n}{k} = \dfrac{n!}{k!\,(n-k)!}$.

*Démonstration.* — La démonstration repose sur une récurrence sur $n$. Pour $n = 0$ et $n = 1$, la formule est clairement vraie. On suppose que la formule est vraie pour $n$. Calculons, en utilisant l'hypothèse de récurrence et la distributivité de la loi $\times$ par rapport à $+$

$$(a+b)^{n+1} = (a+b) \times (a+b)^n = \sum_{k=0}^{n} C_n^k \, a^{k+1} \times b^{n-k} + \sum_{k=0}^{n} C_n^k \, a^k \times b^{n+1-k} \, .$$

On effectue un changement d'indices

$$(a+b)^{n+1} = \sum_{k=1}^{n+1} C_n^{k-1} \, a^k \times b^{n+1-k} + \sum_{k=0}^{n} C_n^k \, a^k \times b^{n+1-k} \, .$$

Il suffit maintenant d'utiliser la *formule du triangle de Pascal* :

$$C_n^{k-1} + C_n^k = C_{n+1}^k \, ,$$

pour tout $k = 1, \ldots, n$. □

***Exemple 4.8.*** — † *La formule du binôme se généralise comme suit. Soit $(A, +, \times)$ un anneau, $a_1, \ldots, a_m \in A$ des éléments qui commutent deux à deux, autrement dit*

$$a_i \times a_j = a_j \times a_i \, ,$$

*pour tout $i, j \in \{1, \ldots, m\}$. Alors, pour tout $n \in \mathbb{N}$, on a*

$$(a_1 + \ldots + a_m)^n = \sum_{k_1 + \ldots + k_m = n} \frac{n!}{k_1! \, \ldots \, k_m!} \, a_1^{k_1} \times \ldots \times a_m^{k_m} \, .$$

***Définition 4.2.*** — *Soit $(A, +, \times)$ un anneau. On dit que $a \in A$ est* inversible *s'il existe $b \in A$ tel que*

$$a \times b = b \times a = 1_A \, .$$

*On notera alors $b = a^{-1}$. On notera $A^\bullet$ l'ensemble des éléments inversibles de $A$.*

***Proposition 4.3.*** — *$(A^\bullet, \times)$ est un groupe.*

*Démonstration.* — Clairement, $1_A \in A^\bullet$. Soient $a, b \in A^\bullet$, alors $a \times b$ est bien inversible, d'inverse $b^{-1} \times a^{-1}$, donc $\times$ est un loi interne sur $A^\bullet$. Le reste est évident et laissé au lecteur. □

***Exemple 4.9.*** — *Vérifier que $\mathbb{Z}^\bullet = \{-1, 1\}$ dans $(\mathbb{Z}, +, \cdot)$.*

***Exemple 4.10.*** — *Vérifier que $\mathbb{Q}^\bullet = \mathbb{Q} - \{0\}$ dans $(\mathbb{Q}, +, \cdot)$.*

***Exemple 4.11.*** — *Soit $(A, +, \times)$ un anneau. Vérifier que $A[X]^\bullet = \{P(X) = a \in A[X] \, : \, a \in A - \{0_A\}\}$ (ensemble des polynômes constants non nuls) dans $(A[X], +, \times)$.*

***Exemple 4.12***. — *Soit $n \geq 2$. Vérifier que $\dot{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$, si et seulement si $k$ et $n$ sont premiers entre eux.*

*Démonstration.* — On suppose que $\dot{k}$ est inversible. Alors, il existe $\dot{k'} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\dot{k'} \dot{\times} \dot{k'} = \dot{1}$. Autrement dit, $k\,k' - 1$ est un multiple de $n$. Donc, il existe $m \in \mathbb{Z}$ tel que $k\,k' + n\,m = 1$. Ce qui montre que $k$ et $n$ sont premiers en eux (Théorème de Bézout).

Inversement, si $k$ et $n$ sont premiers entre eux, le Théorème de Bézout nous assure qu'il existe $u, v \in \mathbb{Z}$ tels que $k\,u + n\,v = 1$. Dans ce cas $\dot{k}$
$dot\times \dot{u} \dot{+} \dot{n} \dot{\times} \dot{v} = \dot{1}$. Autrement dit $\dot{k} \dot{\times}$
$dotu = \dot{1}$, ce qui montre que $\dot{k}$ est inversible. □

***Définition 4.3***. — *Soit $(A, +, \times)$ un anneau commutatif. On dit que $a \in A - \{0_A\}$ est un* diviseur de 0 *si*

$$\exists b \in A - \{0_A\} \qquad a \times b = 0_A\,.$$

***Proposition 4.4***. — *Soit $(A, +, \times)$ un anneau commutatif et $a \in A$. Alors*

$$a \text{ est inversible} \quad \Longrightarrow \quad a \text{ n'est pas un diviseur de } 0\,,$$

*ou, de manière équivalente,*

$$a \text{ est un diviseur de } 0 \quad \Longrightarrow \quad a \text{ n'est pas inversible.}$$

*Démonstration.* — Supposons que $a \in A$ est inversible. Soit $b \in A$ tel que $a \times b = 0_A$. On multiplie à gauche par $a^{-1}$ pour trouver $b = 0_A$. Donc $a$ n'est pas un diviseur de 0. □

***Définition 4.4***. — *On dit qu'un anneau commutatif $(A, +, \times)$ est* intègre *si*

$$\forall a, b \in A\,, \qquad (a \times b = 0_A \quad \Longrightarrow \quad (a = 0_A \quad \text{ou} \quad b = 0_A))$$

Autrement dit, un anneau commutatif est intègre s'il ne contient aucun diviseur de 0.

***Exemple 4.13***. — *Soit $n \geq 2$. Vérifier que l'anneau $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau intègre, si et seulement si $n$ est un nombre premier.*

***Exemple 4.14***. — *Vérifier que $(\mathbb{Q} + \sqrt{2}\,\mathbb{Q}, +, \cdot)$ est un anneau intègre (utiliser le fait que $\sqrt{2}$ n'est pas un rationnel).*

***Exemple 4.15***. — *$(\mathbb{R}[X], +, \times)$ et $(\mathbb{C}[X], +, \times)$ sont des anneaux intègres (raisonner sur le degré des polynômes).*

## 4.2. Corps

***Définition 4.5***. — *Un* corps $(K, +, \times)$ *est un anneau non réduit à* $\{0_K\}$ *dont tous les éléments non nuls sont inversibles. On dit que* $(K, +, \times)$ *est un corps commutatif, si la loi* $\times$ *est commutative.*

***Exemple 4.16***. — *Vérifier que les ensembles suivants sont munis d'une structure de corps commutatif*

$$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot) \qquad \text{et} \qquad (\mathbb{C}, +, \cdot)\,.$$

***Exemple 4.17***. — *Vérifier que* $(\mathbb{Q} + \sqrt{2}\,\mathbb{Q}, +, \cdot)$ *est un corps (on remarquera que, pour tout* $x, y \in \mathbb{Q}$*,*

$$(x + \sqrt{2}\,y)^{-1} = \frac{x}{x^2 - 2\,y^2} - \sqrt{2}\,\frac{y}{x^2 - 2\,y^2}\,,$$

*si* $x + \sqrt{2}\,y \neq 0$*).*

***Exemple 4.18***. — *Soit* $(A, +, \times)$ *un anneau intègre fini. Alors* $(A, +, \times)$ *est un corps.*

*Démonstration.* — Soit $a \in A - \{0_A\}$. On considère l'application

$$\begin{array}{rcl} f_a \ : A & \longrightarrow & A \\ b & \longmapsto & a \times b \end{array}$$

Dans un premier temps, on vérifie que cette application est injective. En effet, si $f_a(b) = f_A(b')$ alors $f_a(b - b') = 0_A$ donc $a \times (b - b') = 0$. Or, $a$ n'est pas un diviseur de 0, donc $b - b' = 0_A$. Autrement dit $b = b'$. Comme $A$ est fini, le lemme 2.1 implique que que $f_a$ est surjective. En particulier, il existe $b \in A$ tel que $f_a(b) = 1_A$, donc $a$ admet un inverse pour la loi $\times$. □

Nous allons maintenant construire le corps des fractions d'un anneau intègre commutatif. Soit $(A, +, \times)$ un anneau intègre commutatif. On note $A^* = A \setminus \{0_A\}$.

***Lemme 4.1***. — *La relation* $\sim$ *définie sur* $A \times A^*$ *par*

$$(a, b) \sim (c, d) \quad \Longleftrightarrow \quad a \times d = b \times c$$

*est une relation d'équivalence.*

*Démonstration.* — La relation est clairement réflexive et symétrique. Montrons qu'elle est transitive. Supposons que $(a, b) \sim (c, d)$ et que $(c, d) \sim (e, f)$. Alors $a \times d = b \times c$ et $c \times f = d \times e$. Calculons

$$a \times d \times c \times f = b \times c \times d \times e$$

donc

$$(a \times f - b \times e) \times c \times d = 0$$

L'anneau étant intègre et sachant que par hypothèse, $d \neq 0$, on en déduit que

$$a \times f = b \times e \quad \text{ou} \quad c = 0.$$

1er cas : La première égalité est vérifiée. Alors on a bien $(a, b) \sim (e, f)$.
2ème cas : $c = 0$. Alors $(a, b) \sim (c, d)$ entraîne $a = 0$ et $(c, d) \sim (e, f)$ entraîne $e = 0$. Donc on a encore $(a, b) \sim (e, f)$.
Cela prouve que $(a, b) \sim (e, f)$ dans tous les cas. □

On note $\dot{\overline{(a, b)}}$ ou encore $\dfrac{a}{b}$ la classe d'équivalence de $(a, b) \in A \times A^*$ et $K := (A \times A^*)/\sim$ l'ensemble des classes d'équivalence pour la relation $\sim$. La démonstration de la proposition qui suit (un peu fastidieuse, mais sans difficulté) est laissée en exercice.

***Proposition 4.5***. — *Soit $A$ un anneau commutatif intègre. Les lois $+$ et $\times$ définies sur $A$ par:*

$$(a, b) + (c, d) = (a \times d + b \times c, b \times d)$$

*et*

$$(a, b) \times (c, d) = (a \times c, b \times d)$$

*sont des lois de composition internes qui sont bien définies sur $A$ et qui munissent $A$ d'une structure d'anneau. De plus elles sont compatibles avec la relation d'équivalence $\sim$. L'ensemble quotient $K := (A \times A^*)/\sim$ est donc un anneau. De plus, si $a \neq 0_A$, $\dot{\overline{(a, b)}}$ est inversible, d'inverse $\dot{\overline{(b, a)}}$; $K$ est donc un corps, appelé "corps des fractions de $A$".*

De la même façon que nous avons défini la notion de sous-groupe d'un groupe, nous avons la

***Définition 4.6***. — *Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que $B$ est un* sous-anneau *de $(A, +, \times)$ si*

(i) $\forall a, b \in B$, $a - b \in B$.
(ii) $\forall a, b \in B, a \times b \in B$.
(iii) $1_A \in B$.

***Exemple 4.19***. — *$\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ qui est un sous-anneau de $\mathbb{R}$ qui est un sous-anneau de $\mathbb{C}$. Mais $\mathbb{Z}$ n'a pas de sous-anneau strict, car ce serait un sous-groupe de $\mathbb{Z}$ contenant 1, et ce serait donc $\mathbb{Z}$ tout entier.*

Dans le cas des corps, nous avons la

***Définition 4.7***. — *Soit $(K, +, \times)$ un corps et $B \subset K$. On dit que $B$ est un* sous-corps *de $(K, +, \times)$ si*

(i) *$B$ est un sous-anneau de $(B, +, \times)$.*
(ii) $\forall a \in B - \{0_K\}$, $a^{-1} \in B$.

***Exemple 4.20***. — *Soit $(A,+,\times)$ un anneau et $X \subset A$. Le sous-anneau engendré par $X$ est le plus petit sous anneau de $(A,+,\times)$ qui contient $X$. Il peut aussi être défini comme l'intersection de tous les sous-anneaux de $(A,+,\times)$ qui contiennent $X$. On laisse au lecteur le soin de définir ce qu'est un sous-corps engendré.*

***Définition 4.8***. — *Une application $f : A \longrightarrow B$ est un morphisme de l'anneau $(A,+,\times)$ dans l'anneau $(B,+',\times')$ si*

(i) $\forall a,b \in A,\ f(a+b) = f(a) +' f(b)$.
(ii) $\forall a,b \in A,\ f(a\times b) = f(a) \times' f(b)$.
(iii) $f(1_A) = 1_B$.

**Remarque***: Il est important de vérifier la dernière condition qui n'est pas conséquence des précédentes (contrairement à la propriété $f(e) = e'$ pour un morphisme de groupe).*

*On dira que $f$ est un isomorphisme d'anneaux si $f$ est un morphisme d'anneaux bijectif. Dans le cas où les anneaux sont des corps, on parlera de morphisme de corps.*

***Exemple 4.21***. — *L'image d'un morphisme d'anneaux de $(A,+,\times)$ dans $(B,+,\times)$ est un sous-anneau de $(B,+',\times')$.*

***Exemple 4.22***. — *Vérifier qu'un morphisme de corps $f : A \longrightarrow B$ est toujours injectif.*

*Démonstration.* — Si $a' \neq a$, alors $a'-a$ est inversible dans $A$ et $1_B = f(1_A) = f((a'-a)\times(a'-a)^{-1}) = (f(a')-f(a))\times'(f(a'-a))^{-1}$. Donc $f(a') \neq f(a)$. □

## 4.3. Idéaux d'un anneau

***Définition 4.9***. — *Soit $(A,+,\times)$ un anneau et $I \subset A$; $I$ est un* idéal *si :*

(i) *$(I,+)$ est un sous-groupe de $(A,+)$,*
(ii) *Pour tout $x \in I$ et pour tout $y \in A$, $x \times y \in I$,*
(iii) *Pour tout $x \in I$ et pour tout $y \in A$, $y \times x \in I$.*

L'importance des idéaux vient du fait qu'ils jouent, pour les anneaux, un rôle similaire à celui des sous-groupes distingués pour les groupes: Nous verrons que sont les noyaux des morphismes, et également la "bonne" structure avec laquelle on peut quotienter un anneau, et obtenir ainsi un anneau quotient. Donnons quelques exemples d'idéaux.

***Exemple 4.23***. — *$\{0_A\}$ et $A$ sont des idéaux de $(A,+,\times)$.*

***Exemple 4.24***. — *Les idéaux de $(\mathbb{Z},+,\times)$ sont les sous-ensembles de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}$.*

*Démonstration.* — Soit $I$ un idéal de $(\mathbb{Z}, +, \times)$. Par définition $I$ est sous-groupe de $(\mathbb{Z}, +)$. On a vu que dans ce cas, il existe $n \in \mathbb{N}$ tel que $I = n\,\mathbb{Z}$. Inversement, $n\,\mathbb{Z}$ est stable par multiplication par un entier, donc est un idéal de $(\mathbb{Z}, +, \cdot)$. □

***Exemple 4.25.*** — *les matrices $n \times n$ de déterminant nul forment un idéal de l'anneau des matrices $n \times n$.*

***Exemple 4.26.*** — *On considère l'anneau $\mathcal{C}(O)$ des fonctions continues sur un intervalle $O \subset \mathbb{R}$. Si $K$ est un compact inclus dans $O$, les fonctions de $\mathcal{C}(O)$ nulles sur $K$ forment un idéal de $\mathcal{C}(O)$.*

***Exemple 4.27.*** — *Soit $P(X)$ un polynôme de $\mathbb{R}[X]$. Les polynômes $Q(X)$ qui s'écrivent sous la forme $Q(X) = P(X)R(X)$ (polynômes divisibles par $P$) forment un idéal.*

***Exemple 4.28.*** — *Les polynômes de $\mathbb{R}[X, Y]$ qui s'écrivent sous la forme*

$$P(X, Y) = X^2 Q(X, Y) + Y^2 R(X, Y)$$

*forment un idéal.*

***Exemple 4.29.*** — *Si $I$ est un idéal de $(A, +, \times)$ et si $1_A \in I$ alors $I = A$.*

*Démonstration.* — En effet, pour tout $a \in A$ on a $1_A \times a = a \in I$. □

***Exemple 4.30.*** — *Soit $(A, +, \times)$ un anneau commutatif. On dit que $x \in A$ est* nilpotent *s'il existe $n \in \mathbb{N}$ tel que $x^n = 0_A$. On note $I$ l'ensemble des éléments nilpotents de $A$. Alors $I$ est un idéal de $(A, +, \times)$ (ainsi, par exemple, dans $\mathbb{Z}/8\mathbb{Z}$, l'ensemble $I = \{\dot{0}, \dot{2}, \dot{4}, \dot{6}\}$ est un idéal).*

*Démonstration.* — On commence par vérifier que $I$ est un groupe additif. Soient $a, b \in I$. Il existe $n, m \in \mathbb{N}$ tels que $a^n = b^m = 0_A$. On utilise la formule du binôme

$$(a + b)^{n+m} = \sum_{k=0}^{n+m} C_k^{n+m}\, a^k \times b^{n+m-k}$$

(on utilise ici le fait que l'anneau est commutatif). Il suffit maintenant de remarquer que, pour tout $k \in \{1, \ldots, n + m\}$ on a $n \geq n$ ou $n + m - k \geq m$ et par conséquent $a^k\, b^{n+m-k} = 0_A$. Conclusion $(a + b) \in I$. Clairement, si $0_A \in I$ et, si $a \in I$ alors $-a \in I$.

Enfin, remarquons que si $a \in I$, $a^n = 0_A$ et $b \in A$ alors $(a \times b)^n = a^n \times b^n = 0$, donc $a \times b \in I$. □

***Proposition 4.6.*** — *Soit $f : A \longmapsto A'$ un morphisme d'anneaux. Alors* Ker $f$ *est un idéal.*

Ce résultat explique pourquoi les idéaux tiennent une place importante dans l'étude des anneaux (contrairement aux sous-anneaux qui sont peu utilisés).

*Démonstration.* — On sait déjà que $\operatorname{Ker} f$ est un sous-groupe de $(A,+)$. Maintenant, si $a \in \operatorname{Ker} f$ et si $b \in A$, alors

$$f(a \times b) = f(a) \times' f(b) = 0_{A'} \times' f(b) = 0_{A'}\,,$$

donc $a \times b \in \operatorname{Ker} f$. On montre de même que $b \times a \in \operatorname{Ker} f$. Ce qui montre que $\operatorname{Ker} f$ est un idéal de $A$. □

***Proposition 4.7.*** — *Soit $f : A \longmapsto A'$ un morphisme d'anneaux. Alors, l'image réciproque d'un idéal de $A'$ est un idéal de $A$.*

*Si $f$ est surjective, alors l'image d'un idéal de $A$ est un idéal de $A'$.*

*Démonstration.* — Soit $I'$ un idéal de $A'$; $I'$ est un sous-groupe, donc on sait déjà que $f^{-1}(I')$ est un sous-groupe de $(A,+)$. Maintenant, si $a \in f^{-1}(I')$ et si $b \in A$, alors $f(a \times b) = f(a) \times f(b)$, mais $f(a) \in I'$ qui est un idéal, donc $f(a) \times f(b) \in I'$.

On montre de même que $f(b) \times f(a) \in I'$. Ce qui montre que $f^{-1}(I')$ est un idéal de $A$.

Supposons maintenant $f$ surjective. Soit $I$ un idéal de $A$; $I$ est un sous-groupe, donc on sait déjà que $f(I)$ est un sous-groupe de $(A',+)$. Maintenant, si $a' \in f(I)$ et si $b' \in A'$, alors $a' = f(a)$ avec $a \in I$, et, comme $f$ est surjective, $b' = f(b)$ avec $b \in A$. Donc

$$a' \times b' = f(a) \times f(b) = f(a \times b);$$

mais $a \in I$ donc $a \times b \in I$ donc $a' \times b' \in f(I)$.

On raisonne de la même façon pour $b' \times a'$.

□

***Exemple 4.31.*** — *Soient $I$ et $J$ deux idéaux de $(A,+,\times)$. Alors*

$$I + J := \{a + b \,:\, a \in I\,, \quad b \in J\}\,,$$

*est un idéal de $(A,+,\times)$.*

***Exemple 4.32.*** — *L'intersection d'une famille quelconque d'idéaux de $(A,+,\times)$ est un idéal de $(A,+,\times)$.*

***Exemple 4.33.*** — *Soit $(A,+,\times)$ un anneau commutatif. On note*

$$a\,A := \{a \times x \,:\, x \in A\}.$$

*Alors $a\,A$ est un idéal de $(A,+,\times)$.*

***Exemple 4.34.*** — *Vérifier que $\mathbb{Z}$ n'est pas un idéal de $(\mathbb{Q},+,\times)$.*

***Proposition 4.8***. — *Soit $(K,+,\times)$ un corps, alors les seuls idéaux de $(K,+,\times)$ sont $\{0_K\}$ et $K$. Si un anneau commutatif possède exactement deux idéaux, alors c'est un corps.*

*Démonstration.* — On suppose que $(K,+,\times)$ est un corps. Soit $I$ un idéal, $I \neq \{0_K\}$. Soit $a \in I - \{0_K\}$. Alors $a^{-1} \times a \in I$ donc $1_K \in I$ et d'après un exercice précédent, $I = K$.

Supposons maintenant que $(A,+,\times)$ ait exactement deux idéaux $\{0_A\}$ et $A$. Soit $a \in A - \{0_A\}$. On sait que $a\,A$ est un idéal et il est non réduit à $\{0_A\}$. Donc $a\,A = A$. Conclusion, il existe $x \in A$ tel que $a \times x = 1_A$. Donc tout élément non nul de $A$ est inversible, et $A$ est un corps. □

***Exemple 4.35***. — *Soit $(K,+,\times)$ un corps, $(A,+,\times)$ un anneau non réduit à $\{0_A\}$, et $f : K \longrightarrow A$ un morphisme d'anneaux. Alors $f$ est injectif.*

*Démonstration.* — On sait que $\operatorname{Ker} f$ est un idéal de $(K,+,\times)$. Donc deux possibilités, soit $\operatorname{Ker} f = \{0_K\}$ soit $\operatorname{Ker} f = K$. Remarquons que, par définition, $f(1_K) = 1_A$, donc $\operatorname{Ker} f \neq K$. C'est donc que $\operatorname{Ker} f = \{0_K\}$, ce qui termine la démonstration. □

## 4.4. Anneau quotient

Soit $(A,+,\times)$ un anneau commutatif et $I$ un idéal de $A$. On note $\sim$ la relation définie par

$$a \sim b \qquad \Longleftrightarrow \qquad b - a \in I$$

pour tout $a, b \in A$.

***Théorème 4.1***. — *La relation $\sim$ est une relation d'équivalence compatible avec les lois $+$ et $\times$.*

*On peut munir l'ensemble quotient $A/I$ d'une structure d'anneau en définissant les lois $\dot{+}$ et $\dot{\times}$ par*

$$\dot{a} \mathbin{\dot{+}} \dot{b} = \overline{a+b}\,, \qquad \textit{et} \qquad \dot{a} \mathbin{\dot{\times}} \dot{b} = \overline{a \times b}\,.$$

*On dit que $(A/I, \dot{+}, \dot{\times})$ est l'*anneau quotient *de $A$ par $I$.*

*Démonstration.* — On remarque d'abord que $(I,+)$ est un groupe commutatif (et donc distingué) d' où la compatibilité avec l'addition. En ce qui concerne la multiplication, $a \sim b$ signifie $a - b \in I$; mais, $I$ étant un idéal, on a

$$\forall c \in A, \qquad c(a-b) \in I \quad \text{et} \quad (a-b)c \in I.$$

On a donc bien les lois de composition internes $\dot{+}$ et $\dot{\times}$ sur que quotient, qui héritent des propriétés vérifiées dans un anneau (la seule que nous n'avons pas vérifiée est la distributivité de la multiplication par rapport à l'addition, mais

sa démonstration ne présente pas de difficulté). On remarque que l'élément neutre pour la multiplication est $\dot{1}$.

□

Quelques mots sur le vocabulaire utilisé. Si $a \sim b$, on dira que $a$ et $b$ sont congrus modulo $I$. Dans le cas où l'idéal $I = c\,A$, on dira que $a$ et $b$ sont congrus modulo $c$.

***Exemple 4.36***. — *Considérons $n\,\mathbb{Z}$ qui est un idéal de $(\mathbb{Z}, +, \cdot)$. Alors $x \sim y$ si et seulement si $x \equiv y \quad [n]$.*

On note $A/I$ l'ensemble des classes d'équivalence pour la relation $\sim$ définie ci-dessus. La classe d'équivalence de $a \in A$ sera notée $\overline{a} = a + I := \{a + b : b \in I\}$.

***Exemple 4.37***. — *On considère l'idéal $n\,\mathbb{Z}$ de $(\mathbb{Z}, +, \cdot)$. Alors $(\mathbb{Z}/n\,\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau commutatif.*

***Exemple 4.38***. — *On considère l'idéal $(X^2 + 1)\,\mathbb{R}[X]$ dans $(\mathbb{R}[X], +, \times)$. Alors $(\mathbb{R}[X]/(X^2 + 1)\,\mathbb{R}[X], \dot{+}, \dot{\times})$ est un anneau commutatif. On remarquera que*

$$\overline{a + \dot{b}\,X} \,\dot{\times}\, \overline{a' + \dot{b}'\,X} = \overline{aa' - bb' + \dot{(ab' + ba')}\,X}\,,$$

*d' où l'on déduit facilement que l'application $f : (\mathbb{R}[X]/(X^2+1)\,\mathbb{R}[X], \dot{+}, \dot{\times}) \to \mathbb{C}$ définie par*

$$\forall a, b \in \mathbb{R}, \qquad f(\overline{a + \dot{b}\,X}) = a + ib,$$

*est un isomorphisme de corps, et donc que $(\mathbb{R}[X]/(X^2 + 1)\,\mathbb{R}[X], \dot{+}, \dot{\times})$ est un corps.*

On note

$$\pi : A \longrightarrow A/I\,,$$

la surjection canonique définie par $\pi(a) = \dot{a} = a + I$.

***Théorème 4.2***. — [Théorème d'Emmy Noether] *Soit $f : A \longmapsto A'$ un morphisme entre deux anneaux commutatifs $(A, +, \times)$ et $(A', +', \times')$. Alors* $\operatorname{Im} f$ *est isomorphe à $A/\operatorname{Ker} f$ et le diagramme ci-dessus est commutatif*

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & A' \\ \pi \big\downarrow & & \big\uparrow i \\ A/\operatorname{Ker} f & \xrightarrow{\ \overline{f}\ } & \operatorname{Im} f\,, \end{array}$$

*où $i$ est l'injection canonique de* $\operatorname{Im} f$ *dans $A'$ définie tout simplement par $i(x) = x$. Plus précisément, $\overline{f}$ est l'unique isomorphisme d'anneaux tel que*

$$f = i \circ \overline{f} \circ \pi\,.$$

*Démonstration.* — On vérifie d'abord que $\overline{f}$ est bien définie. En effet, elle est définie par

$$\overline{f}\ (\dot{x}) = f(x),$$

et il faut vérifier que cette définition ne dépend pas du représentant choisi dans $\dot{x}$. Mais si $\dot{x} = \dot{y}$, $x - y = z \in I$ et $f(x) = f(y)$ puisque $z \in \mathrm{Ker}(f)$.

Vérifions maintenant que $\overline{f}$ est un morphisme. On a

$$\overline{f}(\dot{x} + \dot{y}) = \overline{f}(\dot{\overline{x+y}}) = f(x+y) = f(x) + f(y) = \overline{f}(\dot{x}) + \overline{f}(\dot{y}).$$

La démonstration est similaire pour le produit. On a clairement $\overline{f}(e) = e'$.

Vérifions maintenant que $\overline{f}$ est bijective. D'abord, on a

$$\overline{f}(\dot{x}) = 0 \Longleftrightarrow f(x) = 0 \Longleftrightarrow x \in \mathrm{Ker}(f) \Longleftrightarrow \dot{x} = 0,$$

donc $f$ est injective. La surjectivité est immédiate.

Le dernier point du théorème (unicité) est admis sans démonstration. □

***Exemple 4.39.*** — *Considérons le morphisme d'anneaux $f : \mathbb{R}[X] \to \mathbb{C}$ défini par $f(P) = P(i)$. Alors le théorème de Noether montre que l'application*

$$\overline{f} : \left\{ \begin{array}{ccc} (\mathbb{R}[X]/(X^2+1)\,\mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ \overline{P} & \longmapsto & P(i) \end{array} \right.$$

*est un isomorphisme.*

Soit $(A, +, \times)$ un anneau commutatif et $I$ un idéal de $A$. Nous donnons ici une description des idéaux de $(A/I, \dot{+}, \dot{\times})$.

***Proposition 4.9.*** — *Soit $J$ un idéal de $(A, +, \times)$. qui contient $I$, alors $\pi(J) := \{\pi(a) \in A/I \,:\, a \in J\}$ est un idéal de $(A/I, \dot{+}, \dot{\times})$.*

*Soit $\dot{J}$ un idéal de $(A/I, \dot{+}, \dot{\times})$, alors $\pi^{-1}(\dot{J}) := \{a \in A \,:\, \pi(a) \in \dot{J}\}$ est un idéal de $(A, +, \times)$.*

*Démonstration.* — Il suffit d'utiliser le fait que $\pi$ est un morphisme d'anneaux. □

## 4.5. Idéal premier et idéal maximal

Soit $(A, +, \times)$ un anneau commutatif.

***Définition 4.10.*** — *On dit qu'un idéal $I$ de $(A, +, \times)$ est un* idéal maximal *si les idéaux de $(A, +, \times)$ qui contiennent $I$ sont $I$ et $A$.*

*On dit qu'un idéal $I$ de $(A, +, \times)$ est un* idéal premier *si*

$$\forall a, b \in A, \quad a \times b \in I \quad \Longrightarrow \quad (a \in I \quad ou \quad b \in I)\,.$$

***Exemple 4.40***. — *On considère l'anneau* $(\mathbb{Z}, +, \times)$. *On rappelle que*

$$n\,\mathbb{Z} \subset m\,\mathbb{Z} \qquad \Longleftrightarrow \qquad m \text{ divise } n \iff \qquad n \text{ multiplede } m\,.$$

*Soit* $n \geq 2$, *vérifier que* $n\,\mathbb{Z}$ *est un idéal maximal, si et seulement si* $n$ *est un nombre premier.*

*Démonstration.* — On suppose que $n\,\mathbb{Z}$ est un idéal maximal. Soit $d$ un diviseur de $n$, alors $n\,\mathbb{Z} \subset d\,\mathbb{Z}$. Donc $d\,\mathbb{Z} = n\,\mathbb{Z}$ ou $d\,\mathbb{Z} = \mathbb{Z}$, ce qui s'exprime aussi sous la forme de $d = n$ ou $d = 1$. Donc $n$ est un nombre premier.

Inversement, si $n$ est un nombre premier et si $n\,\mathbb{Z} \subset m\,\mathbb{Z}$ alors $m$ divise $n$ et donc $m = n$ ou $m = 1$, ce qui s'exprime par $m\,\mathbb{Z} = n\,\mathbb{Z}$ ou $m\,\mathbb{Z} = \mathbb{Z}$. Donc $n\,\mathbb{Z}$ est un idéal maximal. □

***Exemple 4.41***. — *On considère l'anneau* $(\mathbb{Z}, +, \times)$ *et* $n \in \mathbb{N} - \{0\}$. *Vérifier que* $n\,\mathbb{Z}$ *est un idéal premier, si et seulement si* $n$ *est un nombre premier.*

*Démonstration.* — On suppose que $n\,\mathbb{Z}$ est un idéal premier. Soit $d$ un diviseur de $n$, on peut écrire $n = q\,d$. Alors $q\,d \in n\,\mathbb{Z}$ donc soit $d \in n\,\mathbb{Z}$ soit $q \in n\,\mathbb{Z}$. Autrement dit soit $d$ est un multiple de $n$ soit $q$ est un multiple de $n$. Donc soit $d = n$ soit $d = 1$. Ce qui prouve que $n$ est un nombre premier.

Inversement, si $n$ est un nombre premier et si $a\,b \in n\,\mathbb{Z}$. Alors $n$ divise $a\,b$ et donc $n$ divise $a$ ou $n$ divise $b$. Autrement dit $a \in n\,\mathbb{Z}$ ou $b \in n\,\mathbb{Z}$. □

Plus généralement, nous avons la
Plus généralement, nous avons la

***Proposition 4.10***. — *Soit* $(A, +, \times)$ *un anneau commutatif et* $I$ *un idéal de* $A$. *Alors*

(i) $I$ *est un idéal premier* $\Longleftrightarrow$ $(A/I, \dot{+}, \dot{\times})$ *est un anneau intègre.*
(ii) $I$ *est un idéal maximal* $\Longleftrightarrow$ $(A/I, \dot{+}, \dot{\times})$ *est un corps.*

*En particulier, un idéal maximal est un idéal premier.*

*Démonstration.* — Démontrons (i). On note $\pi : A \longrightarrow A/I$ la surjection canonique définie par $\pi(a) = a + I$. Par définition, $I$ est un idéal premier si et seulement si

$$\forall a, b \in A, \qquad a \times b \in I \quad \Longrightarrow \quad (a \in I \quad \text{ou} \quad b \in I)\,.$$

Remarquons que

$$\pi(c) = \dot{0} \qquad \Longleftrightarrow \qquad c \in I\,.$$

En utilisant la définition de $\pi$, on constate que cette assertion est équivalente à l'assertion

$$\forall \dot{a}, \dot{b} \in A/I, \qquad \dot{a} \dot{\times} \dot{b} = \dot{0} \quad \Longrightarrow \quad (\dot{a} = \dot{0} \quad \text{ou} \quad \dot{b} = \dot{0})$$

ce qui est justement la définition du fait que $(A/I, \dot{+}, \dot{\times})$ est un anneau intègre.

Démontrons maintenant (ii). Dans un premier temps, on suppose que $(A/I, \dot{+}, \dot{\times})$ est un corps. Alors $A/I \neq \{\dot{0}\}$ (car nécessairement $\dot{1} \in A/I$). Autrement dit $I \neq A$. On note $\pi : A \longrightarrow A/I$ la surjection canonique définie par $\pi(a) = a + I = \dot{a}$. Soit $J$ un idéal de $A$ qui contient $I$ tel que $J \neq I$. Montrons que $J = A$, ce qui montrera que $I$ est un idéal maximal.

Soit $a \in J - I$. Alors $\pi(a) \in A/I - \{\dot{0}\}$. Or, $(A/I, \dot{+}, \dot{\times})$ est un corps, donc il existe $b \in A$ tel que $\pi(a) \mathbin{\overline{\times}} \pi(b) = \dot{1}$. En particulier, $a \times b \in 1_A + I$. Utilisons maintenant le fait que $J$ est un idéal pour conclure que $a \times b \in J$. Donc, $1_A \in J$, ce qui permet de conclure que $J = A$ (utiliser le résultat de l'Exemple 4.29).

Inversement, on suppose que $I$ est un idéal maximal, montrons que $(A/I, \dot{+}, \dot{\times})$ est un corps. Soit $\dot{a} \in A/I - \{\dot{0}\}$ et $a \in A$ tel que $\pi(a) = \dot{a}$. Le fait que $\dot{a} \neq \dot{0}$ se traduit par $a + I \neq I$. En particulier, $a \notin I$. On note

$$J = I + a\,A.$$

On vérifie que c'est un idéal de $(A, +, \times)$ qui contient strictement $I$. Étant donné que $I$ est un idéal maximal, on peut conclure que

$$I + a\,A = A.$$

En particulier, $1_A \in I + a\,A$. Il existe donc $b \in A$ tel que

$$1_A - a \times b \in I.$$

Donc

$$\dot{1}_A = \pi(a) \times \pi(b)\,,$$

ce qui montre que $\dot{a}$ est inversible. Le reste de la démonstration est aisé et laissé au lecteur. □

Donnons quelques applications de ce résultat.

***Exemple 4.42.*** — *On considère l'anneau $(\mathbb{Z}, +, \times)$ et $p$ un nombre premier. On a vu que l'idéal $p\,\mathbb{Z}$ est un idéal maximal donc $(\mathbb{Z}/p\,\mathbb{Z}, \dot{+}, \dot{\times})$ est un corps.*

***Exemple 4.43.*** — † *Soit $(A, +, \times)$ un anneau commutatif. Alors l'idéal $\{0_A\}$ est maximal, si et seulement si $(A, +, \times)$ est un corps.*

*Démonstration.* — Supposons que $\{0_A\}$ soit un idéal maximal. Soit $I$ un idéal de $(A, +, \times)$. On a $0_A \in I$, donc $I = \{0_A\}$ ou $I = A$. Conclusion, les seuls idéaux de $(A, +, \times)$ sont $\{0_A\}$ et $A$. En utilisant le résultat de la Proposition 4.8, on peut conclure que $(A, +, \times)$ est un corps.

Inversement, si $(A, +, \times)$ est un corps, alors la Proposition 4.8 nous permet d'affirmer que les seuls idéaux de $(A, +, \times)$ sont $\{0_A\}$ et $A$. Donc $\{0_A\}$ est un idéal maximal. □

## 4.6. Idéaux principaux

Soit $(A, +, \times)$ un anneau commutatif.

***Définition 4.11***. — *Soient $a, b \in A$. On dit que $a$* divise *$b$ (ou que $b$* est un multiple de *$a$ s'il existe $c \in A$ tel que $b = a \times c$.*

***Proposition 4.11***. — *$a$ divise $b$ si et seulement si $b\,A \subset a\,A$*

*Démonstration.* — Si $a$ divise $b$ alors il existe $c \in A$ tel que $b = a \times c$. En particulier $b \in a\,A$. Ce qui entraîne immédiatement que $b\,A \subset a\,A$.

Si $b\,A \subset a\,A$ alors $b \in a\,A$. En particulier, il existe $c \in A$ tel que $b = a \times c$. □

***Exemple 4.44***. — *Dans $(\mathbb{Z}, +, \times)$, $24\,\mathbb{Z} \subset 4\,\mathbb{Z}$ qui traduit le fait que 4 divise 24.*

***Définition 4.12***. — *On dit qu'un idéal $I$ de $(A, +, \times)$ est* principal*, s'il est engendré par un seul élément, autrement dit $I = a\,A$.*

***Exemple 4.45***. — *Pour tout $n \in \mathbb{N}$, $n\,\mathbb{Z}$ est un idéal principal de $(\mathbb{Z}, +, \cdot)$.*

***Définition 4.13***. — *On dit qu'un anneau commutatif $(A, +, \times)$ est* principal *si c'est un anneau intègre et si tout idéal de $A$ est* principal*.*

***Exemple 4.46***. — *$(\mathbb{Z}, +, \times)$ est un anneau principal.*

***Exemple 4.47***. — *Vérifier qu'un corps est un anneau principal.*

*Démonstration.* — On a vu que les idéaux d'un corps $(K, +, \times)$ sont $\{0_K\} = 0_K\,K$ et $K = 1_K\,K$, en particulier, ils sont tous principaux. □

***Exemple 4.48***. — *L'anneau $(\mathbb{Z}/6\,\mathbb{Z}, \dot{+}, \dot{\times})$ n'est pas un anneau principal car ce n'est pas un anneau intègre.*

Donnons un dernier exemple d'anneau qui n'est pas principal.

***Exemple 4.49***. — *On considère dans l'anneau $(\mathbb{R}[X, Y], +, \times)$, l'ensemble*

$$I := \{X\,P(X, Y) + Y\,Q(X, Y) \,:\, P, Q \in \mathbb{R}[X, Y]\}\,.$$

*Vérifier que $I$ est un idéal mais que $I$ n'est pas un idéal principal.*

*Démonstration.* — Supposons que $I$ est un anneau principal. Il existerait $P_0 \in \mathbb{R}[X, Y]$ tel que $I = P_0\,\mathbb{R}[X, Y]$. Dans ce cas, $X \in I$ s'écrirait sous la forme

$$X = P_0(X, Y)\,Q(X, Y)\,.$$

Il est facile de vérifier que cela entraîne nécessairement que $P_0$ est de la forme $P_0(X,Y) = a\,X + b$. Utilisons maintenant le fait que $Y \in I$ devrait s'écrire sous la forme

$$Y = P_0(X,Y)\,R(X,Y)\,,$$

et que nécessairement $P_0$ est de la forme $P_0(X,Y) = c\,Y + d$. Donc, finalement, $P_0$ est un polynôme constant (non nul). Donc, $I = \mathbb{R}[X,Y]$, ce qui constitue une contradiction. □

***Théorème 4.3***. — [Théorème d'Emmy Noether] *Soit $(A,+,\times)$ un anneau principal et $(I_n)_n$ une suite d'idéaux telle que*

$$I_n \subset I_{n+1}\,,$$

*alors la suite $(I_n)_n$ est stationnaire à partir d'un certain rang.*

*Démonstration*. — On note

$$I = \bigcup_{n\in\mathbb{N}} I_n$$

On vérifie aisément que c'est un idéal. L'anneau étant principal, il existe $a \in A$ tel que $I = a\,A$. En particulier, $a \in I$ donc il existe $n_0 \in \mathbb{N}$ tel que $a \in I_{n_0}$. On a donc les inclusions

$$I = a\,A \subset I_{n_0} \subset I_n \subset I$$

pour tout $n \geq n_0$. □

## 4.7. PGCD et PPCM

Soit $(A,+,\times)$ un anneau commutatif intègre.

***Définition 4.14***. — *Soient $a,b \in A$ et $d \in A$. On dit que $d$ est* un *PGCD de $a$ et $b$ si*

$$(\forall x \in A, \qquad x \mid a \quad et \quad x \mid b \quad \Longleftrightarrow \quad x \mid d)\,.$$

*Soient $a,b \in A$ et $m \in A$. On dit que $m$ est* un *PPCM de $a$ et $b$ si*

$$(\forall x \in A, \qquad a \mid x \quad et \quad b \mid x \quad \Longleftrightarrow \quad m \mid x)$$

Remarquons que le PGCD et le PPCM de deux éléments est défini à multiplication près par un élément inversible de $A$.

Soit $(A,+,\times)$ un anneau principal et $a,b \in A$. On vérifie que $a\,A + b\,A$ est un idéal. Donc, il existe $d \in A$ tel que

$$d\,A = a\,A + b\,A\,.$$

Le résultat suivant précise le lien entre $d$ et un PGCD de $a$ et $b$.

***Théorème 4.4***. — *Soit $(A,+,\times)$ un anneau principal, $a,b,d \in A$. Alors, les propositions suivantes sont équivalentes :*

(i) *$d$ est un PGCD de $a$ et $b$.*
(ii) *$d\,A = a\,A + b\,A$.*
(iii) *$d \mid a\,, \quad d \mid b \quad$ et $\quad \exists\, u, v \in A \quad d = a\,u + b\,v\,.$*

*Démonstration.* — Pour tout $x \in A$, on a l'équivalence

$$x \mid a \quad \text{et} \quad x \mid b \quad \Longleftrightarrow \quad (a\,A \subset x\,A \quad \text{et} \quad b\,A \subset x\,A) \quad \Longleftrightarrow a\,A + b\,A \subset x\,A\,.$$

Démontrons que (i) est équivalent à (ii). Supposons que $d\,A = a\,A + b\,A$ et montrons que $d$ est un PGCD de $a$ et $b$. Soit $x \in A$ tel que $x \mid a$ et $x \mid b$. Alors, $d\,A = a\,A + b\,A \subset x\,A$ et donc $x \mid d$. Inversement, si $x \mid d$ alors $a\,A + b\,A = d\,A \subset x\,A$, et donc $x \mid a$ et $x \mid b$ ce qui termine la démonstration du fait que $d$ est un PGCD de $a$ et $b$.

Inversement, soit $\overline{d}$ un PGCD de $a$ et $b$ et $d$ tel que $a\,A + b\,A = d\,A$. Par hypothèse $\overline{d} \mid a$ et $\overline{d} \mid b$. Donc $d\,A = a\,A + b\,A \subset \overline{d}\,A$. Donc $\overline{d} \mid d$. De plus $a\,A \subset d\,A$ et $b\,A \subset d\,A$. Donc $d \mid a$ et $d \mid b$ donc $d \mid \overline{d}$ puis $d\,A \subset \overline{d}\,A$. Ce qui montre que $\overline{d}\,A = d\,A$.

Démontrons maintenant que (ii) est équivalent à (iii). Pour cela il suffit de remarquer que l'on a les équivalences

$$d \mid a \quad \text{et} \quad d \mid b \quad \Longleftrightarrow \quad (a\,A \subset d\,A \quad \text{et} \quad b\,A \subset d\,A) \quad \Longleftrightarrow a\,A + b\,A \subset d\,A$$

et

$$\exists\, u, v \in A \quad d = a\,u + b\,v \quad \Longleftrightarrow \quad d\,A \subset a\,A + b\,A\,.$$

Ce qui termine la démonstration. □

Soit $(A, +, \times)$ un anneau principal et $a, b \in A$. On vérifie que $a\,A \cap b\,A$ est un idéal. Donc, il existe $m \in A$ tel que

$$m\,A = a\,A \cap b\,A\,.$$

Le résultat suivant précise le lien entre $m$ et le PPCM de $a$ et $b$.

***Théorème 4.5***. — *Soit $(A, +, \times)$ un anneau principal, $a, b, m \in A$. Les propositions suivantes sont équivalentes :*

(i) *$m$ est un PPCM de $a$ et $b$.*
(ii) *$m\,A = a\,A \cap b\,A$.*

*Démonstration.* — Pour tout $x \in A$, on a l'équivalence

$$a \mid x \quad \text{et} \quad b \mid x \quad \Longleftrightarrow \quad (x\,A \subset a\,A \quad \text{et} \quad x\,A \subset b\,A) \quad \Longleftrightarrow x\,A \subset a\,A \cap b\,A\,.$$

Supposons que $m\,A = a\,A \cap b\,A$ et montrons que $m$ est un PPCM de $a$ et $b$. Soit $x \in A$ tel que $a \mid x$ et $b \mid x$. Alors, $x\,A \subset a\,A \cap b\,A = m\,A$ et donc $m \mid x$. Inversement, si $m \mid x$ alors $x\,A \subset m\,A = a\,A \cap b\,A$, et donc $a \mid x$ et $b \mid x$ ce qui termine la démonstration du fait que $m$ est un PPCM de $a$ et $b$.

□

***Définition 4.15***. — *Soit $(A,+,\times)$ un anneau principal et $a,b \in A$. On dit que $a,b$ sont premiers entre eux si $1_A$ est un PGCD de $a$ et $b$.*

***Théorème 4.6***. — [Théorème de Bézout] *Soit $(A,+,\times)$ un anneau principal et $a,b \in A$. Les propositions suivantes sont équivalentes :*

(i) *$a$ et $b$ sont premiers entre eux.*
(ii) $a\,A + b\,A = A$.
(iii) $\exists\, u,v \in A \quad a\,u + b\,v = 1_A$ .

***Exercice 4.1*** **(Théorème de Bézout généralisé)**. — *Dans un anneau principal $(A,+,\times)$, montrer que les éléments $a_1,\cdots,a_r$ sont premiers entre eux dans leur ensemble (i.e. tous les PGCD communs de $a_1,\cdots,a_r$ sont inversibles) si et seulement si il existe $(u_1,\cdots,u_r) \in A^r$ tel que $a_1\,u_1 + \cdots + a_r\,u_r = 1_A$.*

***Théorème 4.7***. — [Théorème de Gauss] *Soit $(A,+,\times)$ un anneau principal et $a,b \in A$. Si $a \mid b \times c$ et si $a$ et $b$ sont premiers entre eux, alors $a \mid c$.*

*Démonstration.* — On utilise le Théorème de Bézout qui nous assure de l'existence de $u,v \in A$ tels que

$$a\,u + b\,v = 1_A$$

On multiplie cette égalité par $c$ pour trouver que

$$a\,c\,u + b\,c\,v = c.$$

Clairement le membre de gauche est divisible par $a$, donc $a$ divise $c$. □

## 4.8. Anneaux euclidiens et entiers de Gauss

***Définition 4.16***. — *Un anneau commutatif intègre $(A,+,\times)$ est* euclidien *s'il existe une application*

$$N : A - \{0_A\} \longrightarrow \mathbb{N}\,,$$

*telle que pour tout couple $(a,b) \in A^2$ avec $b \neq 0_A$, il existe un couple $(q,r)$ de $A^2$ tel que*

$$a = b \times q + r \quad et \quad (r = 0 \quad \text{ou} \quad N(r) < N(b))\ .$$

Donnons deux exemples qui seront utiles pour éclaircir cette définition.

***Exemple 4.50***. — *Prenons sur l'anneau $(\mathbb{Z},+,\times)$ l'application $N(n) = |n|$. On vérifie que $(\mathbb{Z},+,\times)$ est un anneau euclidien.*

***Exemple 4.51***. — *Prenons sur l'anneau $(K[X],+,\times)$ avec $(K,+,\times)$ corps commutatif, l'application $N(P) = \deg P$. On vérifie que $(K[X],+,\times)$ est un anneau euclidien.*

En suivant pas à la pas la démonstration du corollaire 5.2, on obtient la:

***Proposition 4.12***. — *Tout anneau euclidien est principal.*

L'anneau des *entiers de Gauss*) est l'ensemble

$$\mathbb{Z}[i] := \{n + i\,m \,:\, n, m \in \mathbb{Z}\}$$

muni de l'addition et de la multiplication des nombres complexes.

On vérifie aisément (exercice) que $(\mathbb{Z}[i], +, \times)$ est un anneau intègre commutatif. On note alors

$$N(n + i\,m) := n^2 + m^2\,.$$

***Proposition 4.13***. — *L'anneau* $(\mathbb{Z}[i], +, \times)$ *est euclidien.*

*Démonstration.* — Soit $\xi \in \mathbb{C}$. On vérifie (faire un dessin) qu'il existe $z \in \mathbb{Z}[i]$ tel que

$$|\xi - z|^2 \leq \frac{1}{2}\,.$$

Soient $x, y \in \mathbb{Z}[i]$, $y \neq 0$. On note $\xi = \frac{x}{y}$. D'après ce que l'on vient de voir, il existe $q \in \mathbb{Z}[i]$ tel que

$$|\xi - q|^2 \leq \frac{1}{2}\,.$$

On note

$$r := x - y\,q\,.$$

On remarque que $r \in \mathbb{Z}[i]$ et que, par construction

$$N(r) = N(x - q\,y) = |\xi - q|^2\,|y|^2 \leq \frac{1}{2}|y|^2 < N(y)\,.$$

Ce qui termine la démonstration. □

# CHAPITRE 5

# POLYNÔMES

## 5.1. Généralités

Dans toute cette section, on fixe un anneau $(A, +, \times)$ commutatif. On note $A^{(\mathbb{N})}$ l'ensemble des *suites presque nulles* d'éléments de $A$, c'est-à-dire l'ensemble des suites de $A$ n'ayant qu'un nombre fini de termes distincts de $0_A$. On note $(0)$ la suite dont tous les termes sont nuls et $(e_n)$ la suite dont tous les termes sont nuls, sauf celui d'indice $n$, qui vaut 1.

Sur $A^{(\mathbb{N})}$ on définit deux lois de composition internes $+$ et $\times$ par

$$\begin{aligned}(a) + (b) &= (a_0 + b_0, a_1 + b_1, \cdots, a_n + b_n, \cdots)\\ (a) \times (b) &= \Big(a_0 \times b_0, a_1 \times b_0 + a_0 \times b_1, \cdots, \sum_{k=0}^{n} a_k \times b_{n-k}, \cdots\Big).\end{aligned}$$

Par des calculs faciles (mais un peu laborieux), on vérifie que $A^{(\mathbb{N})}$ muni de ces deux lois de composition interne est un anneau. Plus précisément :

- la suite nulle $(0)$ est l'élément neutre pour $+$;
- l'opposé de la suite $(a_0, \cdots, a_n, \cdots)$ est la suite $(-a_0, \cdots, -a_n, \cdots)$;
- la suite $(e_0) = (1, 0, \cdots, 0 \cdots)$ est l'élément neutre pour $\times$.

En pratique, on note 1 la suite $(e_0)$, $X$ la suite $(e_1)$ et $X^n$ la suite presque nulle $(e_n)$ avec $n \geq 2$. On convient que 0 désigne la suite nulle. Cette notation est cohérente avec le fait que pour tout $n \in \mathbb{N}$, on a bien

$$(X)^n = (e_1)^n = e_n = X^n.$$

De ce fait, l'élément $(a_0, \cdots, a_n, \cdots)$ de $A^{(\mathbb{N})}$ correspond à l'expression algébrique

$$\sum_{k=0}^{\infty} a_k X^k. \tag{2}$$

On note alors $A[X]$ l'ensemble de ces expressions algébriques, appelé *ensemble des polynômes à une indéterminée et à coefficients dans $A$*. Le terme général de (2) est appelé *monôme*.

Il est d'usage de ne pas écrire les monômes $a_k X^k$ de (2) tels que que $a_k = 0$. En conséquence, un polynôme ne comporte qu'un nombre fini de termes. On convient aussi de noter $a_0$ au lieu de $a_0 1$. En conséquence, suivant le contexte, $a_0$ désigne ou bien un élément de $A$ ou bien un élément de $A[X]$. Cet abus de notation ne crée pas de confusion en pratique et est justifié par le fait que les lois de composition interne $+$ et $\times$ agissent de la même façon sur les éléments de $A$ et sur les éléments de $A[X]$ du type $a\,1$.

Avec cette nouvelle notation, les lois de composition interne se transcrivent en:

$$P+Q = \sum_{k=0}^{\max(m,n)} (a_k+b_k)\, X^k$$

$$PQ = \sum_{k=0}^{m+n} \sum_{p+q=k} a_p \times b_q\, X^k,$$

si $P = a_0 + a_1 X + a_m X^m$ et $Q = b_0 + b_1 X + \cdots b_n X^n$.

***Exemple 5.1***. — *Les trois ensembles $\mathbb{Z}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$ désignent les polynômes à coefficients entiers, réels et complexes, respectivement. L'ensemble $(\mathcal{M}_n(\mathbb{R}))[X]$ contient les polynômes de matrices vus en cours de "réduction des endomorphismes".*

***Exemple 5.2***. — *Les ensembles $\mathbb{Z}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$ munis de $+$ et $\times$ sont des anneaux commutatifs. Tel n'est pas le cas de $(\mathcal{M}_n(\mathbb{R}))[X]$ (sauf si $n = 1$ bien sûr).*

***Définition 5.1***. — *Soit $P = a_n X^n + \cdots a_0$ un polynôme de $A[X]$. On associe à $P$ la* fonction polynôme *$\tilde{P} : A \times A$ définie par*

$$\forall x \in A,\ \tilde{P}(x) = \sum_{k=0}^{n} a_k x^k.$$

**Remarque:** En pratique, on utilise la même notation $P$ pour désigner le polynôme (objet algébrique) ou la fonction polynôme. Pour les polynômes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$ cette application est injective, et l'indentification entre le polynôme et la fonction polynôme est possible. Par contre, ce n'est plus la cas si $A$ est fini. Par exemple, si $A = \mathbb{Z}/2\mathbb{Z}$, il n'y a que 4 fonctions de $A$ dans $A$, mais une infinité de polynômes disctincts!

***Exercice 5.1***. — *Soit $x \in A$. Vérifier que l'application $\Phi_x : A[X] \to A$ est un homomorphisme d'anneaux vérifiant de plus:*

$$\forall \lambda \in A, \forall P \in A[X],\ \Phi(\lambda P) = \lambda \Phi(P).$$

## 5.2. Degré et valuation

***Définition 5.2***. — *Soit $(A, +, \times)$ un anneau (quelconque) et $P \in A[X]$ un polynôme à coefficients dans $A$. On suppose que les coefficients de $P$ sont donnés par la suite presque nulle $(a)$.*

*Si $P$ n'est pas nul, on appelle :*

- degré *du polynôme $P$, noté* $\deg P$, *le plus* grand *indice $k$ tel que $a_k \neq 0$;*
- valuation *du polynôme $P$, notée* $\mathrm{v}(P)$, *le plus* petit *indice $k$ tel que $a_k \neq 0$.*

*Par convention, on pose* $\deg 0 = -\infty$ *et* $\mathrm{v}(0) = +\infty$.

***Lemme 5.1***. — *Soient $P, Q \in A[X]$, alors*[1]

- $\deg PQ \leq \deg P + \deg Q$ *et* $\mathrm{v}(PQ) \geq \mathrm{v}(P) + \mathrm{v}(Q)$ *avec égalités si l'anneau $A$ est intègre;*
- $\deg(P+Q) \leq \max(\deg P, \deg Q)$ *et* $\mathrm{v}(P+Q) \geq \min(\mathrm{v}(P), \mathrm{v}(Q))$.

*Démonstration.* — On suppose que $P$ et $Q$ sont non nuls (donc de degré positif ou nul), sinon le résultat est évident. Notons $P = a_m X^m + \cdots + a_0$ et $Q = b_n X^n + \cdots + b_0$ avec $m = \deg P$ et $n = \deg Q$ (et donc $a_m \neq 0$ et $b_n \neq 0$). Alors

$$PQ = (a_m \times b_n)\, X^{m+n} + \cdots + a_0 b_0.$$

En conséquence, le degré de $PQ$ vaut au plus $m+n$. Si l'anneau $A$ est intègre, on peut de plus affirmer que $a_m \times b_n \neq 0$, et donc le degré de $PQ$ vaut exactement $m+n$.

Par ailleurs, si l'on suppose par exemple que $m \leq n$ alors

$$P + Q = (a_n + b_n)X^n + \cdots + (a_0 + b_0).$$

Donc $P+Q$ est de degré au plus $n$.

La démonstration pour les valuations est laissée au lecteur. □

***Corollaire 5.1***. — *Si l'anneau $(A, +, \times)$ est intègre alors il en est de même pour $(A[X], +, \times)$ et l'ensemble des éléments inversibles de $(A[X], +, \times)$ est l'ensemble des* polynômes constants *(c'est-à-dire de degré inférieur ou égal à 0) à coefficients inversibles.*

[1] Avec la convention que $-\infty + d = -\infty$ si $d \in \mathbb{N} \cup \{-\infty\}$ et $+\infty + d = +\infty$ si $d \in \mathbb{N} \cup \{+\infty\}$.

*Démonstration.* — Pour démontrer le premier point, supposons que $PQ = 0$. Alors, vu la proposition précédente, on doit avoir $\deg P + \deg Q = -\infty$ et donc $\deg P = -\infty$ ou $\deg Q = -\infty$. Autrement dit $P$ ou $Q$ est nul.

Soit maintenant $P$ un élément inversible de $A[X]$. Alors il existe un polynôme $Q$ tel que $PQ = 1$. En conséquence $\deg P + \deg Q = 0$, et donc les deux polynômes $P$ et $Q$ sont constants. Si $P = a_0$ et $Q = b_0$, on obtient donc $a_0 \times b_0 = 1_A$, ce qui signifie bien que $a_0$ est inversible. La réciproque est claire. □

## 5.3. Division euclidienne

***Proposition 5.1.*** — *Soient $P_1, P_2 \in A[X]$ tel que le terme de plus haut degré de $P_2$ soit inversible dans $A$. Alors, il existe un couple $(Q, R) \in (A[X])^2$ tel que*

$$P_1 = Q\,P_2 + R \quad \textit{et} \quad \deg R < \deg P_2.$$

*Si $A$ est intègre alors ce couple est unique.*

*Démonstration.* — La preuve de ce résultat repose sur une récurrence sur le degré $n$ de $P_1$. Si $\deg P_1 < \deg P_2$, alors on prend simplement $Q = 0$ et $R = P_1$.

Supposons maintenant que le résultat est vrai pour $n-1$ (avec $n \geq \deg P_2$) et montrons-le pour $P_2$ de degré $n$. Écrivons

$$P_1(X) = a_n\,X^n + \ldots + a_0$$

et

$$P_2(X) = b_m\,X^m + \ldots + b_0.$$

Par hypothèse, $n \geq m$ et $b_m$ est un élément inversible de $A$. On vérifie alors que

$$\deg\left(P_1 - a_n \times b_m^{-1}\,X^{n-m}P_2\right) \leq n-1\,.$$

En conséquence, il existe $Q_1 \in A[X]$ et $R \in A[X]$ tels que $\deg R < \deg P_2$ et

$$P_1 - a_n \times b_m^{-1}\,X^{n-m}P_2 = Q_1P_2 + R.$$

On a alors le résultat voulu avec $Q = Q_1 + a_n \times b_m^{-1}\,X^{n-m}$.

L'unicité dans le cas $A$ intègre se démontre comme dans le cas "classique". On suppose que

$$P_1 = QP_2 + R = Q'P_2 + R' \quad \text{avec} \quad \deg R < \deg P_2 \;\text{ et }\; \deg R' < \deg P_2.$$

On a donc $R' - R = (Q - Q')P_2$. Donc $\deg(R' - R) = \deg(Q - Q') + \deg P_2$. Étant donné que $\deg(R' - R) < \deg P_2$, cela n'est possible que si $R' - R = Q - Q' = 0$. □

***Exercice 5.2***. — *Dans* $\mathbb{R}[X]$, *effectuer la division euclidienne de* $2X^5 - X^3 + X^2 + 1$ *par* $X^3 - X + 1$.

***Corollaire 5.2***. — *Soit* $(K, +, \times)$ *un corps commutatif. Alors pour tous polynômes* $P_1$ *et* $P_2$ *de* $A[X]$ *avec* $P_2 \neq 0$, *il existe un unique couple* $(Q, R) \in (A[X])^2$ *tel que*

$$P_1 = Q\,P_2 + R \quad et \quad \deg R < \deg P_2.$$

*On dit que* $(K[X], +, \times)$ *est un* anneau euclidien.

*Démonstration.* — On applique la proposition précédente en remarquant que dans un corps les éléments inversibles sont les éléments non nuls et que, par conséquent, on peut effectuer la division euclidienne par tout polynôme non nul. □

***Corollaire 5.3***. — *Soit* $(K, +, \times)$ *un corps commutatif. Alors* $(K[X], +, \times)$ *est un anneau principal.*

*Démonstration.* — Soit $I$ un idéal non réduit à $\{0\}$ de $(K[X], +, \times)$. Soit $P_0 \in I$ tel que

$$\deg P_0 = \min\{\deg P \,:\, P \in I - \{0\}\}\,.$$

Montrons que $I = P_0\,K[X]$. Clairement $P_0\,K[X] \subset I$ car $I$ est un idéal. Inversement, soit $P \in I$. Par définition il existe $Q, R \in K[X]$ tels que

$$P = QP_0 + R \quad \text{avec} \quad \deg R < \deg P_0.$$

Notons de plus que $R \in I$. donc, vu la définition de $P_0$, on doit avoir $\deg R = -\infty$ autrement dit $R = 0$. En conséquence $P = QP_0 \in P_0\,K[X]$. □

***Définition 5.3***. — *Soit* $(A, +, \times)$ *un anneau (quelconque). On dit que* $a \in A$ *est une* racine *du polynôme* $P$ *de* $A[X]$ *si* $P(a) = 0$.

***Corollaire 5.4***. — *Soit* $P \in A[X]$ *et* $a \in A$. *Alors* $X - a \mid P$ *si et seulement si* $P(a) = 0$.

*Démonstration.* — Si $X - a \mid P$ alors il existe $Q \in A[X]$ tel que $P = (X - a)\,Q$. En particulier $P(a) = (a - a)\,Q(a) = 0$.

Réciproquement, on utilise la proposition précédente pour écrire

$$P = (X - a)\,Q + R$$

avec $\deg R < \deg (X - a) = 1$. Donc $R$ est un polynôme constant. Calculons

$$0 = P(a) = (a - a)\,Q(a) + R(a)$$

pour conclure que $R(a) = 0$ et donc que $R = 0$. Ce qui montre que $X - a$ divise $P$. □

***Corollaire 5.5***. — *Soit* $(A, +, \times)$ *un anneau intègre et* $P \in A[X]$. *Soient* $a_1, \ldots, a_k$ *des racines distinctes de* $P$. *Alors* $(X - a_1) \ldots (X - a_k) \mid P$.

*Démonstration.* — On procède par récurrence sur $k$. Si $k = 1$, c'est le corollaire précédent. Supposons le résultat démontré pour $k$ racines distinctes quelconques, et considérons $a_1, \cdots, a_{k+1}$ des éléments deux à deux distincts de $A$. Alors l'hypothèse de récurrence assure l'existence de $Q \in A[X]$ tel que

$$P = (X - a_1) \dots (X - a_k)Q.$$

Si l'on évalue cette expression en $a_{k+1}$, on a donc

$$0 = P(a_{k+1}) = (a_{k+1} - a_1) \times \dots \times (a_{k+1} - a_k) \times Q(a_{k+1}).$$

Comme $A$ est intègre cela implique que $a_{k+1}$ est racine de $Q$, et donc $Q$ est divisible par $X - a_{k+1}$. Cela permet de conclure au résultat pour $k + 1$ racines. □

***Corollaire 5.6***. — *Si $(A, +, \times)$ est un anneau intègre alors tout polynôme de degré $n$ (avec $n \geq 0$) a au plus $n$ racines.*

**Remarque:** Il peut en avoir moins, cf. par exemple dans $\mathbb{R}[X]$ le polynôme $X^2 + 1$.