

# Chapitre 1

## Rappels sur les relations d'équivalence

### Définition 0.1

Une relation binaire  $\mathcal{R}$  sur un ensemble  $E$  est la donnée d'une partie  $\mathcal{G}$  de  $E \times E$ .

Pour tout  $(x, y) \in E \times E$  on dit que  $x$  est en relation avec  $y$  si  $(x, y) \in \mathcal{G}$ , on écrit alors  $x\mathcal{R}y$ .

### Définition 0.2

Une relation binaire  $\mathcal{R}$  sur un ensemble  $E$  est une relation d'équivalence si elle est

- *réflexive* :

$$\forall x \in E, \quad x\mathcal{R}x \quad (1.1)$$

- *symétrique* :

$$\forall x, y \in E, \quad (x\mathcal{R}y) \Rightarrow (y\mathcal{R}x) \quad (1.2)$$

- *transitive*

$$\forall x, y, z \in E, \quad (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z \quad (1.3)$$

### Définition 0.3

La classe d'équivalence d'un élément  $x$  de  $E$ , notée  $\text{Cl}_{\mathcal{R}}(x)$ , est l'ensemble des éléments de  $E$  qui sont en relation avec  $x$ .

$$\text{Cl}_{\mathcal{R}}(x) = \{y \in E \mid x\mathcal{R}y\}. \quad (1.4)$$

L'ensemble quotient de  $E$  par la relation d'équivalence  $\mathcal{R}$ , noté  $E/\mathcal{R}$ , est l'ensemble des classes d'équivalence de  $E$  relativement à  $\mathcal{R}$  :

$$E/\mathcal{R} = \{\text{Cl}_{\mathcal{R}}(x) \mid x \in E\} \quad (1.5)$$

L'application  $\pi : E \rightarrow E/\mathcal{R}$  qui à  $x$  associe  $\text{Cl}_{\mathcal{R}}(x)$  est appelée la surjection canonique.

### Exemples:

- 1) Soit  $X$  l'ensemble des participants à un tournoi d'ultimate frisbee. La relation binaire définie par  $x\mathcal{R}y$  si  $x$  est dans la même équipe que  $y$  est (en général) une relation d'équivalence. L'ensemble quotient  $X/\mathcal{R}$  est l'ensemble des équipes.
- 2) Soient  $A$  et  $B$  deux ensembles non vides et  $f : A \rightarrow B$  une application. La relation binaire  $\mathcal{R}_f$  sur  $A$  définie par  $x\mathcal{R}_f y$  si  $f(x) = f(y)$  est une relation d'équivalence. Ici  $A/\mathcal{R}_f = \{f^{-1}(\{b\}), b \in f(A)\}$ .
- 3) Soit  $\mathcal{P}$  l'ensemble des couples de points du plan euclidien (celui vu au Lycée). La relation binaire sur  $\mathcal{P}$  définie par  $(A, B)\mathcal{R}(C, D)$  si  $ABDC$  est un parallélogramme (éventuellement dégénéré) c.-à-d. si  $[AD]$  et  $[BC]$  ont même milieu. On reconnaît en  $\mathcal{P}/\mathcal{R}$  l'ensemble des vecteurs du plan tel qu'il est défini au lycée. La classe d'équivalence de  $(A, B)$  est notée  $\overrightarrow{AB}$ .
- 4) La relation binaire sur  $M(n, \mathbb{R})$  (l'ensemble des matrices carrées d'ordre  $n$  à coefficients réels) définie par  $M\mathcal{R}N$  s'il existe  $P \in GL(n, \mathbb{R})$  (ie  $P$  est d'ordre  $n$  et inversible) tel que  $N = PMP^{-1}$  est une relation d'équivalence (appelée relation de similitude).
- 5) La relation binaire sur  $\mathbb{Z} \times \mathbb{Z}^*$  définie par  $(a, b)\mathcal{R}_q(c, d)$  si  $ad = bc$  est une relation d'équivalence. L'ensemble quotient  $(\mathbb{Z} \times \mathbb{Z}^*)/\mathcal{R}_q$  s'identifie à  $\mathbb{Q}$  l'ensemble des nombres rationnels (c'est une façon de définir  $\mathbb{Q}$ ). La classe d'équivalence de  $(a, b)$  est notée  $\frac{a}{b}$ .
- 6) Soit  $n > 0$  un entier. La relation binaire sur  $\mathbb{Z}$  définie par  $x\mathcal{R}y$  si  $n$  divise  $x - y$  est une relation d'équivalence. On note plutôt  $x \equiv y \pmod{n}$  ou  $x \equiv y [n]$ . L'ensemble quotient est noté  $\mathbb{Z}/n\mathbb{Z}$  et la classe d'un élément  $x$  est noté  $\bar{x}$  ou  $x + n\mathbb{Z}$  elle est égale à  $\{x + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$ . On peut voir que  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{(n-1)}\}$ , ces classes sont 2 à 2 distinctes et donc  $\mathbb{Z}/n\mathbb{Z}$  a  $n$  éléments.

#### **Proposition 0.4**

L'ensemble des classes d'équivalence de  $E$  relativement à une relation d'équivalence  $\mathcal{R}$  forme une partition de  $E$ , c'est-à-dire que les classes sont deux à deux disjointes et que leur réunion est égale à  $E$ .

Lorsqu'on connaît a priori le cardinal de chaque classe d'équivalence, on peut utiliser cette proposition pour compter les éléments de  $E$  (si  $E$  est fini). Ainsi dans l'exemple 1) ci-dessus, sachant que chaque équipe d'ultimate est composée de 7 joueurs, on en déduit que le cardinal de  $X$  (ie le nombre de joueurs) est égal à 7 fois celui de  $X/\mathcal{R}$  (le nombre d'équipes). C'est le théorème de Lagrange de l'ultimate.

### Théorème 0.5

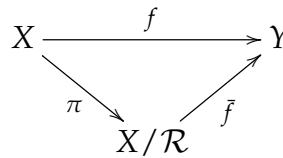
Soient  $X$  un ensemble,  $\mathcal{R}$  une relation d'équivalence sur  $X$ . Soit  $f : X \rightarrow Y$  une application. L'application  $\bar{f} : E/\mathcal{R} \rightarrow Y$  qui à  $\text{Cl}(x)$  associe  $f(x)$  est « bien définie » si et seulement si pour tout  $(x, y) \in X^2$ ,  $x\mathcal{R}y$  implique  $f(x) = f(y)$  (ie si  $f$  est constante sur chaque classe d'équivalence).

Si on trouve l'expression « être bien définie » ambiguë et que cet énoncé n'est donc pas assez rigoureux. On lui préférera la version suivante :

### Théorème 0.5

Soient  $X$  un ensemble,  $\mathcal{R}$  une relation d'équivalence sur  $X$  et  $\pi : X \rightarrow X/\mathcal{R}$  la projection canonique.

Soit  $f : X \rightarrow Y$  une application. Si pour tout  $(x, y) \in X^2$ ,  $x\mathcal{R}y$  implique  $f(x) = f(y)$  alors il existe unique application  $\bar{f} : E/\mathcal{R} \rightarrow Y$  telle que  $\bar{f} \circ \pi = f$ .



On dit alors que  $f$  passe au quotient par  $\mathcal{R}$ .

### Exemples:

- 1) L'application qui à un joueur d'ultimate associe la couleur de son maillot passe au quotient par la relation « appartenir à la même équipe ». Autrement dit l'application qui à une équipe associe son maillot est bien définie.
- 2) Soit  $f : A \rightarrow B$  et  $\mathcal{R}_f$  la relation d'équivalence sur  $A$  définie par  $x\mathcal{R}_f y$  si  $f(x) = f(y)$ . L'application  $\bar{f} : A/\mathcal{R}_f \rightarrow B, \text{Cl}(x) \mapsto f(x)$  est bien définie et même injective.
- 3) Soit  $f : \mathcal{P} \times \mathcal{P} \rightarrow \mathcal{P}$  qui à  $((A, B), (C, D))$  associe  $(A, E)$  où  $E$  est le point du plan tel que  $(B, E)\mathcal{R}(C, D)$ . Cette application passe au quotient et donne l'addition des vecteurs du plan (qui vérifie donc la relation de Chasles).
- 4) L'application déterminant passe au quotient par la relation de similitude.
- 5) Ici  $\mathbb{Q}$  désigne l'ensemble quotient  $\mathbb{Z} \times \mathbb{Z}^* / \mathcal{R}_q$ . Les applications de  $\mathbb{Q} \times \mathbb{Q}$  dans  $\mathbb{Q}$  qui à  $(\frac{a}{b}, \frac{c}{d})$  associe  $\frac{ac}{bd}$  et  $\frac{ad+cb}{bd}$  sont bien définies. On reconnaît la multiplication et l'addition des nombres rationnels.  
 En effet, si  $\frac{a}{b} = \frac{a'}{b'}$  et si  $\frac{c}{d} = \frac{c'}{d'}$  c'est que  $ab' = a'b$  et  $cd' = c'd$  et donc  $acb'd' = a'bc'd$  et donc  $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ .  
 De même  $(ad + bc)(b'd')$   $= ab'dd' + bcb'd' = a'bdd' + c'dbb' = (a'd' + b'c')(bd)$   
 et donc  $\frac{ad+cb}{bd} = \frac{a'd'+c'b'}{b'd'}$ .

6) On définit de même une addition et une multiplication sur  $\mathbb{Z}/n\mathbb{Z}$ .

**Proposition 0.6**

Soit  $n$  un entier naturel non nul. On note  $a, b, a'$  et  $b'$  quatre entiers relatifs. On a les propriétés suivantes : si  $a \equiv b \pmod{n}$  et  $a' \equiv b' \pmod{n}$  alors

$$a + a' \equiv b + b' \pmod{n} \quad a - a' \equiv b - b' \pmod{n} \quad aa' \equiv bb' \pmod{n}$$

La proposition 0.6 et le théorème 0.5 permettent en particulier de munir l'ensemble quotient  $\mathbb{Z}/n\mathbb{Z}$  d'une addition et d'une multiplication définies comme suit.

**Définition 0.7**

Soient  $\bar{x}$  et  $\bar{y}$  deux éléments de  $\mathbb{Z}/n\mathbb{Z}$ . On pose :

1) (Addition)  $\bar{x} + \bar{y} := \overline{x + y}$ ,

2) (Multiplication)  $\bar{x} \bar{y} := \overline{xy}$ .

Pour illustrer la construction ci-dessus, on donne ci-dessous les tables d'addition et de multiplication de  $\mathbb{Z}/3\mathbb{Z}$  :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

**Théorème 0.8**

L'addition et la multiplication définies ci-dessus munissent  $\mathbb{Z}/n\mathbb{Z}$  d'une structure d'anneau commutatif, c'est-à-dire

- 1) ces lois sont associatives et commutatives
- 2)  $\bar{0}$  est l'élément neutre de l'addition,
- 3) tout élément admet un opposé :  $\forall x \in \mathbb{Z}/n\mathbb{Z}, \exists y \in \mathbb{Z}/n\mathbb{Z} : x + y = \bar{0}$ .
- 4)  $\bar{1}$  est l'élément neutre de la multiplication,
- 5) La multiplication est distributive par rapport à l'addition.

# Chapitre 2

## Théorie des groupes

### 1 Définition et premiers exemples

#### Définition 1.1

Un groupe est la donnée d'un ensemble  $G$  et d'une **loi de composition interne**  $*$

$$\begin{aligned} G \times G &\rightarrow G \\ (x, y) &\mapsto x * y \end{aligned}$$

qui vérifie les propriétés suivantes :

- 1) la loi  $*$  est associative :  $\forall (x, y, z) \in G^3, x * (y * z) = (x * y) * z$
- 2) il existe un élément  $e \in G$ , qu'on appelle **élément neutre**, qui est tel que :  $\forall x \in G, x * e = e * x = x$
- 3) tout élément de  $G$  admet un **inverse** :  $\forall x \in G, \exists y \in G : x * y = y * x = e$ .

Si en outre la loi  $*$  est commutative (i.e.  $x * y = y * x$  pour tout  $x, y \in G$ ), on dit que  $G$  est un groupe abélien ou commutatif.

#### Proposition 1.2

Dans un groupe  $(G, *)$  :

- 1) l'élément neutre est unique,
- 2) tout élément  $x$  admet un unique inverse, que l'on note  $x^{-1}$ ,
- 3)  $e^{-1} = e, (x^{-1})^{-1} = x$  pour tout élément  $x$  de  $G$ , et  $(x * y)^{-1} = y^{-1} * x^{-1}$  pour tout couple  $(x, y)$  d'éléments de  $G$ .

Notation : Dans la suite on adoptera en général la *notation multiplicative* pour un groupe abstrait  $G$  : on notera  $xy$  au lieu de  $x * y$ . De même on notera  $x^{-1}$  l'inverse de

$x \in G$  et  $1$  le neutre de  $G$  (on conservera parfois la notation  $e$  pour le neutre, pour insister sur le caractère “général” d’une notion abordée).

Si  $G$  est un groupe abélien, on préférera souvent la notation *additive* :  $x * y$  est noté  $x + y$ ; l’inverse de  $x$  est noté  $-x$  et le neutre est noté  $0$ .

### Définition 1.3

L’ordre d’un groupe  $G$  est son nombre d’éléments. On dit que  $G$  est fini si son ordre est fini.

### Définition 1.4

Dans un groupe  $G$ , pour tout  $x \in G$  et  $n \in \mathbb{N}_{\geq 1}$ , on définit par récurrence

- $x^0 = e$ ;
- $x^n = (x^{n-1})x$ ;
- $x^{-n} = (x^{-1})^n$ .

Si  $n, m \in \mathbb{Z}$ , en utilisant l’associativité de la multiplication, on montre facilement que  $x^{n+m} = x^n x^m$ .

### Exemples:

- $(\mathbb{Z}, +)$  est un groupe infini abélien.
- $(\mathbb{R}^\times, \times)$  est un groupe infini abélien.
- $(\mathbb{Z}/n\mathbb{Z}, +)$  est un groupe abélien fini d’ordre  $n$ . L’addition est définie comme à la fin du chapitre précédent.
- L’ensemble des permutations de  $n$  symboles muni de la composition des applications  $(S_n, \circ)$  est un groupe fini d’ordre  $n!$ . C’est un groupe non-abélien dès que  $n \geq 3$ .
- L’ensemble des symétries d’un polygone régulier à  $n$  côtés muni de la composition des applications  $(D_n, \circ)$  est un groupe fini d’ordre  $2n$ .
- $(GL_n(\mathbb{R}), \times)$  est un groupe infini non-abélien dès que  $n \geq 2$ .
- Les racines de l’unité dans  $\mathbb{C}$  forment un groupe abélien infini.
- Si  $(G, \star_G)$  et  $(H, \star_H)$  sont des groupes alors le produit direct  $G \times H$  est un groupe pour la loi  $\star$  définie par

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \star_G g_2, h_1 \star_H h_2).$$

## 2 Sous-groupes

### 2.1 Définitions

#### Définition 2.1

Soit  $G$  un groupe noté multiplicativement. Une partie  $H$  de  $G$  est un sous-groupe si

- 1)  $H \neq \emptyset$ ,
- 2)  $\forall (x, y) \in H^2, xy \in H$ ,
- 3)  $\forall x \in H, x^{-1} \in H$ .

Remarquons en particulier qu'un sous-groupe d'un groupe  $G$  contient nécessairement l'élément neutre de  $G$ . Aussi, pour tout groupe  $G$ , les parties  $\{e\}$  et  $G$  de  $G$  sont des sous-groupes (les sous-groupes *triviaux*).

Clairement, la loi de groupe de  $G$ , quand on la restreint à un sous-groupe  $H$ , induit une structure de groupe sur  $H$ . En pratique, on montrera souvent qu'un ensemble, muni d'une loi de composition interne est un groupe en l'identifiant à un sous-groupe d'un groupe connu.

La proposition suivante fournit une caractérisation plus compacte pour un sous-groupe :

#### Proposition 2.2

Soit  $H$  une partie d'un groupe  $G$  noté multiplicativement. Alors  $H$  est un sous-groupe si et seulement si

$$H \neq \emptyset \text{ et } \forall (x, y) \in H^2, xy^{-1} \in H.$$

On termine ce paragraphe en donnant la description des sous-groupes de  $\mathbb{Z}$ .

#### Proposition 2.3

Les sous-groupes de  $(\mathbb{Z}, +)$  sont les  $a\mathbb{Z}$  pour  $a \in \mathbb{N}$ .

**Preuve.** Soit  $H \subset \mathbb{Z}$  un sous-groupe. Si  $H = \{0\}$ ,  $H = 0\mathbb{Z}$ . Sinon,  $H$  contient un élément non nul  $x$ , ainsi que son opposé  $-x$ . Ainsi  $H$  contient un élément strictement positif. Par conséquent, l'ensemble  $F_+ = \{x \in H : x > 0\} \subset \mathbb{N}$  est non vide. Il admet donc, comme toute partie non vide de  $\mathbb{N}$ , un plus petit élément noté  $a$ . Clairement,  $a$  ainsi que tous ses multiples appartiennent à  $H$ , donc  $a\mathbb{Z} \subset H$ . Inversement, si  $x$  est un élément (quelconque) de  $H$ , on peut effectuer la division euclidienne de  $x$  par  $a$  :

$$x = aq + r, \text{ avec } q, r \in \mathbb{Z} \text{ et } 0 \leq r < a.$$

On en déduit que  $r = x - aq$  appartient à  $H$ , comme différence de deux éléments de  $H$ . S'il était  $> 0$ , cela contredirait la définition de  $a$ , donc  $r = 0$ , ce qui signifie que  $x \in a\mathbb{Z}$ .

□

**Corollaire 2.4 (Théorème de Bézout)**

Si  $a$  et  $b$  sont deux entiers alors  $a\mathbb{Z} + b\mathbb{Z} := \{ah + bk \mid (h, k) \in \mathbb{Z}^2\} = (a \wedge b)\mathbb{Z}$ . En particulier, il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $au + bv = a \wedge b$ .

On déduit de ce résultat (exercice) que si  $a$  divise  $bc$  et si  $a \wedge b = 1$  alors  $a$  divise  $c$  c'est le lemme de Gauss.

## 2.2 Sous-groupe engendré par une partie

**Proposition 2.5**

L'intersection de deux sous-groupes, ou plus généralement d'une famille de sous-groupes, d'un groupe  $G$  est un sous-groupe de  $G$ .

⚠ La réunion de deux sous-groupes n'est en revanche pas un sous-groupe en général. Ce n'est même essentiellement "jamais" le cas, comme le montre l'énoncé suivant (exercice)

*"Si  $H$  et  $K$  deux sous-groupes d'un groupe  $G$ . Alors  $H \cup K$  est un sous-groupe de  $G$  si et seulement si  $H \subset K$  ou  $K \subset H$ ."*

La proposition 2.5 permet de définir la notion de sous-groupe engendré par une partie :

**Définition 2.6**

Soit  $S$  une partie d'un groupe  $G$ . On appelle sous-groupe engendré par  $S$ , et on note  $\langle S \rangle$  le plus petit sous-groupe de  $G$  contenant  $S$ . C'est l'intersection de tous les sous-groupes de  $G$  qui contiennent  $S$ . On dit alors que  $S$  est une partie génératrice de  $\langle S \rangle$  ou que  $S$  engendre  $\langle S \rangle$ .

⚠ La définition ci-dessus permet de considérer le sous-groupe  $\langle \emptyset \rangle$  de  $G$  (le "sous-groupe engendré par le vide"). On définit  $\langle \emptyset \rangle = \{e\}$ , ce qui est compatible avec la définition ci-dessus.

La définition ci-dessus est peu exploitable en pratique. On dispose de la description plus explicite suivante :

**Proposition 2.7**

Soit  $G$  un groupe. Alors le sous-groupe engendré par une partie non vide  $S$  de  $G$  est l'ensemble des éléments de la forme  $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_r^{\varepsilon_r}$  où :

- $r$  est un entier naturel non nul,
- les  $x_i$  sont des éléments de  $S$ ,
- $\varepsilon_i = \pm 1$  pour tout  $i$ .

En faisant la convention qu'un produit vide d'éléments de  $G$  est égal au neutre de  $G$  et en autorisant  $r = 0$  dans la proposition ci-dessus, on peut se débarrasser de la restriction  $S \neq \emptyset$  dans l'énoncé.



### 3 Ordre d'un élément

#### Définition 3.1

Soit  $G$  un groupe dont la loi est notée multiplicativement. On dit qu'un élément  $x$  de  $G$  est **d'ordre fini** s'il existe un entier naturel non nul  $k$  tel que  $x^k = e$ . Si tel est le cas on appelle **ordre de  $x$**  le plus petit entier  $k \in \mathbb{N}^*$  tel que  $x^k = e$ . Sinon, on dit que  $x$  est **d'ordre infini**.

Donnons un premier énoncé reliant l'ordre d'un élément à l'ordre du sous-groupe qu'il engendre.

#### Proposition 3.2

Soit  $G$  un groupe noté multiplicativement et de neutre  $e$ . Soit  $x \in G$ . Alors l'ordre de l'élément  $x$  de  $G$  est égal à l'ordre du sous-groupe engendré par  $\{x\}$  dans  $G$ .

**Preuve.** Notons  $n$  l'ordre de  $x$  (on a soit  $n \in \mathbb{N}_{\geq 1}$ , soit  $n = \infty$ ). D'après la proposition 2.7, le sous-groupe de  $G$  engendré par  $S = \{x\}$  est :

$$\langle S \rangle = \{x^k : k \in \mathbb{Z}\}.$$

Deux cas se présentent : soit  $n = \infty$  et alors  $|\langle S \rangle| = \infty$  puisque si on a des entiers  $k < \ell$  tels que  $x^k = x^\ell$ , alors  $x^{\ell-k} = e$ , ce qui contredit  $n = \infty$  car  $\ell - k \in \mathbb{N}_{\geq 1}$ . Sinon  $n \in \mathbb{N}_{\geq 1}$ ; montrons alors que

$$\langle S \rangle = \{e, x, \dots, x^{n-1}\}.$$

L'inclusion  $\supset$  est évidente. Réciproquement si  $y = x^k \in \langle S \rangle$  pour un  $k \in \mathbb{Z}$  alors, en écrivant la division euclidienne  $k = qn + r$ ,  $0 \leq r < n$ , de  $k$  par  $n$ , on voit que  $y = x^{qn+r} = (x^n)^q \cdot x^r = x^r$ , ce qui achève de démontrer l'égalité souhaitée.

Enfin, si  $n \in \mathbb{N}_{\geq 1}$ , alors dès que  $0 \leq i < j \leq n-1$ , on a  $x^i \neq x^j$ , car sinon la relation  $x^{j-i} = e$  contredirait le fait que  $n$  est l'ordre de  $x$ . Ainsi l'ordre du sous-groupe engendré par  $S = \{x\}$  est  $|\langle S \rangle| = n$ .  $\square$

On souhaite maintenant établir la caractérisation de l'ordre d'un élément donnée par le corollaire 3.4 ci-dessous. On donne d'abord la forme un peu plus générale suivante de ce résultat.

#### Proposition 3.3

Avec les mêmes hypothèses que précédemment, on définit, pour tout  $x$  de  $G$ , l'ensemble

$$E(x) = \{k \in \mathbb{Z} : x^k = e\}.$$

Alors  $E(x)$  est un sous-groupe de  $\mathbb{Z}$ , qui est différent de  $\{0\}$  si et seulement si  $x$  est d'ordre fini, auquel cas l'ordre de  $x$  est le générateur positif de  $E(x)$ .

**Preuve.**

L'ensemble  $E(x)$  contient 0 et si  $k, \ell$  sont dans  $E(x)$  alors  $x^{k-\ell} = e$  de sorte que  $k - \ell \in E(x)$ . Donc  $E(x)$  est un sous-groupe de  $\mathbb{Z}$  et, d'après la proposition 2.3, il existe  $k_x \in \mathbb{N}$  tel que  $E(x) = k_x \mathbb{Z}$ . On a  $k_x \neq 0$  si et seulement si  $E(x) \neq \emptyset$  si et seulement si il existe  $k \in \mathbb{N}_{>0}$  tel que  $x^k = e$ . Cela équivaut par définition au fait que  $x$  est d'ordre fini. Si tel est le cas, on a vu dans la preuve de la proposition 2.3 que  $k_x = \min\{k > 0 : k \in E(x)\}$  qui est par définition l'ordre de  $x$ .  $\square$

On déduit immédiatement le résultat suivant.

**Corollaire 3.4**

Soit  $x$  un élément d'ordre  $n$  de  $G$ . Alors on a, pour tout  $m \in \mathbb{Z}$ , l'équivalence

$$x^m = e \Leftrightarrow n \text{ divise } m.$$

## 4 Groupes monogènes et groupes cycliques

Pour alléger les notations, on note généralement  $\langle x \rangle$  (au lieu de  $\langle \{x\} \rangle$ ) le sous-groupe engendré par une partie  $S = \{x\}$  réduite à un élément. Ce cas particulier important conduit à la notion de *groupe monogène*.

**Définition 4.1**

Un groupe  $G$  est dit *monogène* s'il coïncide avec le sous-groupe engendré par un de ses éléments, autrement dit s'il existe  $x \in G$  tel que  $G = \langle x \rangle = \{x^k : k \in \mathbb{Z}\}$ . Si de plus  $x$  est d'ordre fini  $n$ , on dit que  $G$  est *cyclique d'ordre  $n$* , et on a alors  $\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$  (cf la preuve de la proposition 3.2).

**Exercice :** Montrer que pour tout  $n \geq 1$  le groupe  $\mathbb{Z}/n\mathbb{Z}$  et le groupe des racines  $n$ -èmes de 1 dans  $\mathbb{C}$  sont cycliques.

**Remarque :**

- 1) Un groupe monogène (en particulier un groupe cyclique) est automatiquement abélien.
- 2) L'ordre d'un groupe cyclique engendré par un élément  $x$  est égal à l'ordre de  $x$ , comme on l'a vu dans la preuve de la proposition 3.2.

**Lemme 4.2**

Soit  $G = \langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$  un groupe cyclique d'ordre  $n$ . Alors, pour tout  $\ell \in \mathbb{Z}$ , l'élément  $x^\ell$  est d'ordre  $\frac{n}{n \wedge \ell}$  où l'on rappelle la notation  $n \wedge \ell = \text{pgcd}(n, \ell)$ .

**Preuve.** Si  $D$  désigne le PGCD de  $\ell$  et de  $n$ , on a

$$\begin{cases} n = Dn' \\ \ell = D\ell' \\ n' \wedge \ell' = 1 \end{cases} .$$

On a alors les équivalences :

$$(x^\ell)^m = e \Leftrightarrow x^{\ell m} = e \Leftrightarrow n \mid \ell m \Leftrightarrow Dn' \mid D\ell' m \Leftrightarrow n' \mid \ell' m \Leftrightarrow n' \mid m \text{ (Gauss)}$$

ce qui signifie précisément que  $x^\ell$  est d'ordre  $n' = \frac{n}{n \wedge \ell}$ . □

### Théorème 4.3

- 1) Les sous-groupes d'un groupe monogène sont monogènes.
- 2) Si  $G$  est un groupe cyclique d'ordre  $n$ , alors tous ses sous-groupes sont cycliques et leur ordre divise  $n$ . Inversement, pour tout diviseur  $d$  de  $n$  il existe un unique sous-groupe  $G_d$  de  $G$  d'ordre  $d$  et on a

$$G_d = \langle x^{\frac{n}{d}} \rangle = \{g \in G \mid g^d = e\} .$$

**Preuve.**

- 1) C'est la même démonstration que pour montrer que les sous-groupes de  $\mathbb{Z}$  sont les  $a\mathbb{Z}$ ,  $a \in \mathbb{N}$ .

Si  $G = \langle x \rangle$  est un groupe monogène engendré par un élément  $x$  et si  $H$  est un sous-groupe de  $G$  alors ses éléments sont des puissances de  $x$ . Si  $H$  est réduit à l'élément neutre  $e$ , alors il est monogène (engendré par  $e$ ). Sinon, il existe un exposant  $k$  non nul tel que  $x^k$  appartienne à  $H$ , auquel cas  $x^{-k} = (x^k)^{-1}$  appartient aussi à  $H$ . L'un des deux entiers  $k$  ou  $-k$  est strictement positif, et il existe donc un plus petit entier naturel non nul  $k_0$  tel que  $x^{k_0}$  appartienne à  $H$ . On vérifie alors que  $H = \langle x^{k_0} \rangle$  : l'inclusion  $\langle x^{k_0} \rangle \subset H$  est évidente et en sens inverse, si  $x^k$  appartient à  $H$ , on effectue la division euclidienne de  $k$  par  $k_0$  ( $k = k_0q + r$ ,  $0 \leq r < k_0$ ) et on constate que  $x^r = x^k (x^{k_0})^{-q}$  appartient à  $H$ , comme produit d'éléments de  $H$ , ce qui n'est possible que si  $r = 0$ , en vertu de la minimalité de  $k_0$  ( $r$  est strictement inférieur à  $k_0$ ), c'est-à-dire si  $k_0$  divise  $k$ .

- 2) Soit  $G = \langle x \rangle$  un groupe cyclique d'ordre  $n$ , ce qui signifie en particulier que  $x$  est d'ordre  $n$ . Comme  $G$  est monogène, ses sous-groupes sont monogènes d'après la première partie du théorème, donc cycliques puisqu'ils sont finis.

Si  $d$  est un diviseur de  $n$ , c'est-à-dire si  $n = qd$  pour un certain entier  $q$ , alors le sous-groupe engendré par  $x^q$  est cyclique d'ordre  $d$ .

Montrons l'unicité : pour cela considérons l'ensemble

$$G_d = \{g \in G \mid g^d = e\}.$$

Pour qu'un élément  $y = x^k$  de  $G$  appartienne à  $G_d$ , il faut et il suffit que  $x^{kd} = e$ , ce qui équivaut, par le corollaire 3.4, à la propriété que  $n = qd$  divise  $kd$ , ou encore  $q$  divise  $k$ . Par conséquent,  $G_d = \langle x^q \rangle$  est un sous-groupe de  $G$  et il est d'ordre  $d$ . En outre, il est unique car tout sous-groupe d'ordre  $d$  de  $G$  est nécessairement cyclique d'après la première partie du théorème, donc engendré par un élément de  $G_d$  qui contient par définition tous les éléments d'ordre  $d$  de  $G$ .

Il reste à montrer que l'ordre d'un sous-groupe de  $G$  est nécessairement un diviseur de  $n$ . Soit  $H$  un tel sous groupe. Il existe donc un entier  $\ell$  tel que

$$H = \langle x^\ell \rangle = \{x^{\ell k}, k \in \mathbb{Z}\}$$

et l'ordre de  $H$  est égal à l'ordre de l'élément  $y = x^\ell$ , qui vaut  $\frac{n}{n \wedge \ell}$  d'après le lemme précédent. En particulier, c'est un diviseur de  $n$ .  $\square$

## 5 Classes modulo un sous-groupe et théorème de Lagrange

### 5.1 Classes modulo un sous-groupe

Étant donné un groupe  $G$  et un sous-groupe  $H$  de  $G$ , l'énoncé suivant donne la définition et les premières propriétés de deux relations d'équivalence sur  $G$  définies grâce à  $H$ .

#### Définition et proposition 5.1

Soit  $H$  un sous-groupe d'un groupe  $G$ .

1) La relation  $\mathcal{R}_H$  définie par

$$x \mathcal{R}_H y \text{ si } x^{-1}y \in H$$

est une relation d'équivalence sur  $G$ . La classe d'équivalence d'un élément  $x$  est égale à  $xH := \{xy \in G : y \in H\}$  ("classe à gauche de  $x$  modulo  $H$ "). L'ensemble quotient est noté  $G/H$ .

2) De même, la relation  $\mathcal{R}'_H$  définie par

$$x \mathcal{R}'_H y \text{ si } yx^{-1} \in H$$

est une relation d'équivalence sur  $G$ , dont les classes d'équivalence sont les "classes à droite"  $Hx := \{yx \in G : y \in H\}$ , dont l'ensemble est noté  $H \backslash G$ .

3) La bijection  $G \rightarrow G, x \mapsto x^{-1}$  induit une bijection de  $G/H$  sur  $H \backslash G$ ; ces ensembles ont donc même cardinal. On le note  $(G : H)$  et on l'appelle indice de  $H$  dans  $G$ .

**Preuve.**

- 1) La relation  $\mathcal{R}_H$  est réflexive puisque pour tout  $x \in G, x^{-1}x = e \in H$  qui est un groupe. Elle est symétrique car  $x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H$  qui est un groupe. Enfin, elle est transitive puisque  $x^{-1}y \in H, y^{-1}z \in H \Rightarrow (x^{-1}y)(y^{-1}z) = x^{-1}z \in H$  qui est un groupe.
- 2) Preuve similaire à celle de 1).
- 3) Il est clair que  $x \mapsto x^{-1}$  est une bijection de  $G$  et que  $z \in xH \Leftrightarrow z^{-1} \in Hx^{-1}$ .

□

**Exemple:** Soit  $n \in \mathbb{N}_{\geq 1}$ . Dans le cas  $G = \mathbb{Z}, H = n\mathbb{Z}$ , on a pour  $x, y \in \mathbb{Z}$ :

$$x\mathcal{R}_Hy \Leftrightarrow x\mathcal{R}'_Hy \Leftrightarrow (x - y) \in n\mathbb{Z} \Leftrightarrow x \equiv y \pmod{n}.$$

Le quotient  $G/H = \mathbb{Z}/n\mathbb{Z}$  correspond donc comme attendu aux classes de congruence modulo  $n$ . On a  $(G : H) = (\mathbb{Z} : n\mathbb{Z}) = |\mathbb{Z}/n\mathbb{Z}| = n$ .

## 5.2 Théorème de Lagrange

Il s'agit du résultat très important suivant.

### **Théorème 5.2 (Lagrange)**

Soit  $G$  un groupe fini, et  $H$  un sous-groupe de  $G$ . Alors on a la relation :

$$(G : H) = \frac{|G|}{|H|}.$$

En particulier l'ordre de  $H$  et l'indice de  $H$  dans  $G$  divisent l'ordre de  $G$ .

**Preuve.** Soit  $a \in G$ . L'application  $H \rightarrow aH$  qui à  $h$  associe  $ah$  est une bijection. On déduit que deux classes à gauche quelconques de  $G$  sont toujours en bijection. Comme  $G$  est réunion disjointe de ses classes à gauche modulo  $H$ , on déduit le résultat. □

### **Corollaire 5.3**

Si  $G$  est un groupe fini, alors son ordre est un multiple de l'ordre de chacun de ses éléments.

### Corollaire 5.4

Tout groupe  $G$  d'ordre  $p$  premier est cyclique.

**Preuve.** En effet, l'ordre du sous-groupe de  $G$  engendré par tout élément  $x \in G$  différent de  $e$  divise  $p$  et a au moins deux éléments. Ce sous-groupe est donc d'ordre  $p$  et  $x$  engendre  $G$ .  $\square$

On a la généralisation suivante du théorème de Lagrange (qui correspond à  $K = \{e_G\}$ ).

### Théorème 5.5

Soient  $G$  un groupe,  $H$  un sous-groupe de  $G$  d'indice fini et  $K$  un sous-groupe de  $H$  d'indice fini. Alors on a la relation :

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

**Preuve.** On considère l'application  $\varphi : G/K \rightarrow G/H, gK \mapsto gH$ . Cette application est clairement bien définie car  $K$  est un sous-groupe de  $H$ . Elle est évidemment surjective. En outre, pour tout  $gH \in G/H$ , nous avons une bijection  $H/K \rightarrow \varphi^{-1}(gH)$  donnée par  $hK \mapsto ghK$  (et dont la réciproque est  $xK \mapsto g^{-1}xK$ ). On en déduit immédiatement le résultat.  $\square$

## 6 Morphismes

### 6.1 Définitions

#### Définition 6.1

Une application  $\varphi$  d'un groupe  $G$  dans un groupe  $H$  est un morphisme de groupes (ou homomorphisme) si

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

**Exercice :** Décrire les morphismes de groupe  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$ .  
Décrire les morphismes de groupe  $\varphi : \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ .

#### Exemples:

a) Si  $G$  est un groupe (quelconque) et  $x$  un élément fixé de  $G$ , l'application

$$\begin{aligned} \varphi_x : \mathbb{Z} &\longrightarrow G \\ k &\longmapsto x^k \end{aligned}$$

est un morphisme de groupes.

a) L'application

$$\begin{aligned}\varphi_x : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ k &\longmapsto \bar{k}.\end{aligned}$$

est un morphisme de groupes.

b) Notons  $\zeta_n = \exp(2i\pi/n)$  et  $U_n = \{z \in \mathbb{C} : z^n = 1\}$ , pour  $n \in \mathbb{N}_{>0}$ . L'application  $\mathbb{Z}/n\mathbb{Z} \rightarrow U_n, \bar{k} \mapsto \zeta_n^k$  est bien définie et c'est un morphisme de groupes.

c) Soit  $G$  un groupe et soit  $g \in G$ . L'application

$$\begin{aligned}\varphi_x : G &\longrightarrow G \\ x &\longmapsto gxg^{-1}\end{aligned}$$

est un morphisme de groupes (qui est l'identité si  $G$  est abélien).

d) La signature  $\varepsilon : S_n \rightarrow \{\pm 1\}$  est un morphisme de groupes.

### Proposition 6.2

Soit  $\varphi : G \rightarrow H$  un morphisme de groupes. Alors

- 1)  $\varphi(e_G) = e_H$ .
- 2)  $\forall x \in G, \varphi(x^{-1}) = \varphi(x)^{-1}$ .
- 3) Si  $x \in G$  est d'ordre fini  $n$  alors l'ordre de  $\varphi(x)$  divise  $n$ .

**Exercice :** Décrire les morphismes de groupe  $\varphi : \mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{Z}/467\mathbb{Z}$ .

### Proposition 6.3

- 1) La composée de deux morphismes est un morphisme.
- 2) Soit  $\varphi : G \rightarrow H$  un morphisme de groupes bijectif alors  $\varphi^{-1}$  est un morphisme. On dit alors que  $\varphi$  est un isomorphisme; si de plus  $G = H$ , on dit que  $\varphi$  est un automorphisme de  $G$ .

Donnons une application de la notion d'isomorphisme dans le cadre des groupes cycliques.

### Proposition 6.4

Soit  $G$  un groupe cyclique d'ordre  $n$ , alors  $G$  est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$ , i.e. il existe un isomorphisme  $\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow G$ .

**Preuve.** Soit  $x$  un générateur de  $G$ . On définit  $\varphi$  comme étant le morphisme de groupes  $\mathbb{Z}/n\mathbb{Z} \rightarrow G$  tel que  $\varphi(\bar{k}) = x^k$  (vérifier qu'il est bien défini et que c'est un morphisme de groupes). Par définition de l'ordre,  $\varphi$  est une surjection et comme les deux groupes ont même ordre; c'est un isomorphisme.  $\square$

**Corollaire 6.5**

Si  $G$  est groupe d'ordre  $p$  premier alors  $G$  est isomorphe à  $\mathbb{Z}/p\mathbb{Z}$ .

On connaît donc tous les groupes d'ordre 2, 3, 5 et 7, complétons cette liste en décrivant ceux d'ordre 4 et 6

**Proposition 6.6**

Soit  $G$  un groupe. Si  $G$  est d'ordre 4 alors il est isomorphe à  $\mathbb{Z}/2\mathbb{Z}$  ou à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

S'il est d'ordre 6 alors il est isomorphe à  $\mathbb{Z}/6\mathbb{Z}$  ou à  $S_3$ .

**Preuve.** Soit  $G = \{e, a, b, c\}$  un groupe d'ordre 4. Si  $G$  contient un élément d'ordre 4 alors il est cyclique et donc isomorphe à  $\mathbb{Z}/4\mathbb{Z}$ . S'il n'en contient pas, le théorème de Lagrange nous dit que tout élément différent du neutre  $e$  est d'ordre 2. Par conséquent  $ab \neq e$ , car  $b \neq a^{-1}$ ,  $ab \neq a$ , car  $b \neq e$  et  $ab \neq b$ , car  $a \neq e$ , et donc  $ab = c$ . On montre de même  $ba = c$ ,  $ac = ca = b$  et  $bc = cb = a$ . L'application  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow G$  qui envoie  $(0, 0)$  sur  $e$ ,  $(1, 0)$  sur  $a$ ,  $(0, 1)$  sur  $b$  et  $(1, 1)$  sur  $c$  est un isomorphisme de groupes.

La preuve du cas  $|G| = 6$  est plus longue et sera faite en TD. En voici les étapes. Tout d'abord montrer que  $G$  possède un élément d'ordre 2, noté  $a$ , et un d'ordre 3 noté  $b$ . Ensuite montrer que si  $ab = ba$  alors  $ab$  est d'ordre 6 et donc  $G$  est cyclique. Enfin, montrer que si  $ab \neq ba$  alors forcément  $ba = ab^2$  et la table de  $G$  est la suivante

$e$	$a$	$b$	$b^2$	$ab$	$ab^2$
$a$	$e$	$ab$	$ab^2$	$b$	$b^2$
$b$	$ab^2$	$b^2$	$e$	$a$	$ab$
$b^2$	$ab$	$e$	$b$	$ab^2$	$a$
$ab$	$b^2$	$ab^2$	$a$	$e$	$b$
$ab^2$	$b$	$a$	$ab$	$b^2$	$e$

et en déduire un isomorphisme avec  $S_3$ . □

Il existe 5 groupes d'ordre 8 dont 4 sont abéliens.

**Proposition 6.7**

Soit  $\varphi : G \rightarrow H$  un morphisme de groupes. Alors

- 1) l'image d'un sous-groupe de  $G$  est un sous-groupe de  $H$ .
- 2) l'image inverse d'un sous-groupe de  $H$  est un sous-groupe de  $G$ .

**6.2 Noyau, image**



**Définition 6.8**

Soit  $\varphi : G \rightarrow H$  un morphisme de groupes.

- On appelle noyau de  $\varphi$  et on note  $\ker \varphi$  l'ensemble des antécédents par  $\varphi$  de l'élément neutre  $e_H$  de  $H$

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}.$$

- On appelle image de  $\varphi$  et on note  $\text{Im } \varphi$  l'ensemble des éléments de  $H$  admettant un antécédent par  $\varphi$

$$\text{Im } \varphi = \{h \in H \mid \exists g \in G, \varphi(g) = h\}.$$

On obtient, comme corollaire immédiat de la proposition 6.7 :

**Corollaire 6.9**

Soit  $\varphi : G \rightarrow H$  un morphisme de groupes. Le noyau de  $\varphi$  est un sous-groupe de  $G$ , et son image est un sous-groupe de  $H$ .

**Remarque.** Soit  $\varphi : G \rightarrow H$  un morphisme de groupes et  $S$  une partie de génératrice de  $G$ , alors  $\text{Im } \varphi$  est engendré par  $\varphi(S)$ . En particulier, si  $G = \langle x \rangle$  est monogène alors  $\text{Im } \varphi = \langle \varphi(x) \rangle$ .

**Proposition 6.10**

Soit  $\varphi : G \rightarrow H$  un morphisme de groupes. Alors pour tout  $(x, y) \in G^2$ ,  $\varphi(x) = \varphi(y)$  si et seulement si  $x \mathcal{R}_{\ker \varphi} y$ . D'où  $\varphi$  est injectif si et seulement si  $\ker \varphi = \{e_G\}$ .

**Remarque.**

- 1) Si  $x$  est un élément fixé dans un groupe  $G$ , le noyau du morphisme

$$\begin{aligned} \varphi_x : \mathbb{Z} &\longrightarrow G \\ k &\longmapsto x^k \end{aligned}$$

est un sous-groupe de  $\mathbb{Z}$ , donc de la forme  $k_x \mathbb{Z}$  pour un entier naturel  $k_x$  convenable. C'est le groupe  $E(x)$  de la proposition 3.3. Comme on l'a vu :

- $k_x = 0 \Leftrightarrow \varphi_x$  injectif  $\Leftrightarrow x$  d'ordre infini.
- $k_x \neq 0 \Leftrightarrow x$  d'ordre fini égal à  $k_x$ .

- 2) L'application

$$\begin{aligned} \bar{\varphi}_x : \mathbb{Z}/n\mathbb{Z} &\longrightarrow G \\ \bar{k} &\longmapsto x^k \end{aligned}$$

est bien définie si  $x^n = 1$  c'est-à-dire si l'ordre de  $x$  divise  $n$ . C'est alors un morphisme de groupe. Si  $G = \mathbb{Z}/n\mathbb{Z}$  cette condition est toujours vérifiée et donc il existe  $n$  endomorphismes de  $\mathbb{Z}/n\mathbb{Z}$ . De plus,  $\bar{\varphi}_x$  est injective si et seulement si  $x$  est d'ordre  $n$  et surjective si  $G = \langle x \rangle$ .

3) Les morphismes des exemples b) et c) de §6.1 sont des isomorphismes.

## 7 Quotients de groupes abéliens

Commençons par l'analogie de la proposition 0.6 du chapitre 1.

### Proposition 7.1

Si  $G$  est un groupe abélien et si  $H$  est un sous-groupe de  $G$  alors il existe sur  $G/H$  une unique structure de groupe telle que la surjection canonique  $\pi : G \rightarrow G/H$  est un morphisme de groupe.

Soit  $f : G \rightarrow K$  un morphisme de groupe et  $H$  un sous-groupe de  $G$ .

On sait que  $[f(x) = f(y)] \Leftrightarrow x \mathcal{R}_{\ker f} y$ . Par conséquent,  $x \mathcal{R}_H y \Rightarrow [f(x) = f(y)]$  si et seulement si  $H$  est contenu dans  $\ker f$ . Autrement dit l'application  $\bar{f} : G/H \rightarrow K$ ,  $xH \mapsto f(x)$  est bien définie si et seulement si  $H \subset \ker f$ . On voit que  $\bar{f}$  est injective si et seulement si  $H = \ker f$ .

Si  $G$  est abélien, on munit  $G/H$  de la structure de groupe donnée par la proposition 7.1. Si  $H \subset \ker f$ , l'application  $\bar{f}$  est bien définie et pour tout  $xH, yH$  dans  $G/H$ , on a  $\bar{f}(xHyH) = \bar{f}(xyH) = f(xy) = f(x)f(y) = \bar{f}(xH)\bar{f}(yH)$  c'est-à-dire  $\bar{f}$  est un morphisme de groupe. On a montré :

### Théorème 7.2

Soient  $G$  un groupe abélien,  $K$  un groupe,  $f : G \rightarrow K$  un morphisme de groupes et  $H$  un sous-groupe de  $G$ . Si  $H \subset \ker f$ , alors il existe un unique morphisme de groupes  $\bar{f} : G/H \rightarrow K$  tel que  $f = \bar{f} \circ \pi$ , où  $\pi$  désigne la projection canonique de  $G$  sur  $G/H$ .

$$\begin{array}{ccc} G & \xrightarrow{f} & K \\ & \searrow \pi & \nearrow \bar{f} \\ & G/H & \end{array}$$

En particulier,  $f$  induit un isomorphisme  $G/\ker f \rightarrow \text{Im } f$ .

Exemples :

- Le morphisme

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{C} \setminus \{0\} \\ x &\longmapsto e^{2i\pi x} \end{aligned}$$

a pour noyau

$$\ker f = \mathbb{Z},$$

pour image

$$\operatorname{Im} f = U = \{z \in \mathbb{C} \mid |z| = 1\}$$

et induit donc un isomorphisme  $\bar{f} : \mathbb{R}/\mathbb{Z} \rightarrow U$ .

- Si  $x$  est un élément d'ordre  $n$  dans un groupe  $G$ , le morphisme

$$\varphi_x : \mathbb{Z} \longrightarrow G \\ k \longmapsto x^k,$$

de noyau  $\ker \varphi_x = n\mathbb{Z}$ , induit un isomorphisme  $\mathbb{Z}/n\mathbb{Z} \simeq \langle x \rangle$ .

**Application :** Soient  $a$  et  $b$  dans  $\mathbb{N} \setminus \{0\}$ . On note  $m$  leur ppcm. L'application

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \\ x \longmapsto (x + a\mathbb{Z}, x + b\mathbb{Z})$$

est un morphisme de groupe. Son noyau est  $a\mathbb{Z} \cap b\mathbb{Z}$  c'est-à-dire  $m\mathbb{Z}$ . Le théorème 7.2 dit que  $\operatorname{Im} f$  est isomorphe à  $\mathbb{Z}/m\mathbb{Z}$ . L'application  $f$  est surjective si et seulement si  $|\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}| = |\operatorname{Im} f|$  c'est-à-dire si et seulement si  $ab = m$  c'est-à-dire si et seulement si  $a$  et  $b$  sont premiers entre eux.

Ainsi, si  $a$  et  $b$  sont premiers entre eux, l'application (bien définie d'après le théorème 7.2)

$$\bar{f} : \mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \\ x + ab\mathbb{Z} \longmapsto (x + a\mathbb{Z}, x + b\mathbb{Z})$$

est un isomorphisme de groupes.

C'est ce qu'on appelle le théorème des restes chinois, sa première version connue est dans un manuscrit du mathématicien Sun Zi datant du 3ème siècle.

### Exercice

Soit  $n > 0$  un entier et  $d$  un diviseur de  $n$ .

- 1) Montrer que  $n\mathbb{Z}$  est un sous-groupe de  $d\mathbb{Z}$ .
- 2) Montrer que  $d\mathbb{Z}/n\mathbb{Z}$  est isomorphe à  $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$ .
- 3) Montrer que  $d\mathbb{Z}/n\mathbb{Z}$  est isomorphe au sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$  engendré par  $\bar{d}$ .
- 4) Montrer que  $(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z})$  est isomorphe à  $\mathbb{Z}/d\mathbb{Z}$ .



# Chapitre 3

## Le groupe des permutations

### 1 Définitions et premières propriétés

#### Définition 1.1

Soit  $n$  un entier naturel non nul. L'ensemble des bijections de  $\{1, \dots, n\}$  dans lui-même muni de la composition s'appelle le groupe symétrique sur  $n$  éléments. On le note  $S_n$ . Ses éléments s'appellent des permutations.

Plus généralement, l'ensemble des bijections d'un ensemble fini  $E$  dans lui-même muni de la loi de composition s'appelle le groupe des permutations de  $E$  ou le groupe symétrique sur  $E$ , il est noté  $\text{Sym}(E)$ .

Il y a exactement  $n!$  façons de permuter les entiers de 1 à  $n$ . On a donc

$$|S_n| = n!$$

**Remarque :** on ne définit pas " $S_0$ ", moyennant quoi, dans la suite, l'écriture  $S_n$  sous-entendra toujours que  $n$  est un entier naturel non nul.

Une façon commode de noter les éléments de  $S_n$  est d'utiliser un tableau à 2 lignes, la première contenant les entiers de 1 à  $n$ , et la seconde leurs images.

**Exemple :**

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

désigne la permutation de  $\{1, \dots, 5\}$  dans lui-même définie par

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

Sa bijection réciproque s'écrit

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

La composition des applications munit  $S_n$  d'une structure de groupe car la composée de deux permutations est une permutation, la composition est associative,  $S_n$  possède un élément neutre (l'application "identité" qui applique chaque entier  $i \in \{1, \dots, n\}$  sur lui-même), tout élément a un "inverse" (bijection réciproque).

Pour alléger les notations, on omettra le symbole "o" de la composition, c'est-à-dire qu'on écrira  $\sigma\gamma$  pour désigner la composée  $\sigma \circ \gamma$ .

Si  $n \geq 3$  ce groupe n'est pas commutatif : par exemple, les deux éléments

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ et } \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

de  $S_3$  ne commutent pas (on a  $\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$  et  $\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ ).

### Définition 1.2 (support)

Le support d'une permutation  $\sigma \in S_n$  noté  $\text{Supp } \sigma$  est le complémentaire dans  $\{1, \dots, n\}$  de l'ensemble  $\text{Fix } \sigma$  de ses points fixes. Autrement dit

$$\text{Supp } \sigma = \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\}, \text{ Fix } \sigma = \{i \in \{1, \dots, n\} \mid \sigma(i) = i\}.$$

**Remarque :** le support d'une permutation  $\sigma$  et son complémentaire sont stables par  $\sigma$

$$\sigma(\text{Supp } \sigma) = \text{Supp } \sigma, \sigma(\text{Fix } \sigma) = \text{Fix } \sigma.$$

La notion de support apparait dans la proposition (fondamentale) suivante.

### Proposition 1.3

Soient  $\sigma$  et  $\gamma$  deux éléments de  $S_n$  de supports disjoints. Alors  $\sigma\gamma = \gamma\sigma$ . Autrement dit, "deux permutations de supports disjoints commutent".

⚠ La réciproque est fautive : il se peut que deux permutations de supports non disjoints commutent. Par exemple, toute permutation commute avec elle-même!

**Preuve.** Comparons les images par  $\sigma\gamma$  et  $\gamma\sigma$  d'un élément  $x$  de  $\{1, \dots, n\}$ .

- Si  $x$  appartient au support de  $\sigma$ , alors il n'appartient pas au support de  $\gamma$  puisque ces deux supports sont disjoints, par hypothèse. Par conséquent,  $\gamma(x) = x$  et

$$\sigma\gamma(x) = \sigma(x). \tag{3.1}$$

Par ailleurs  $\sigma(x)$  appartient lui aussi au support de  $\sigma$ , puisque celui-ci est stable par  $\sigma$  (cf. remarque précédente), et n'appartient donc pas au support de  $\gamma$ . Par conséquent,

$$\gamma(\sigma(x)) = \sigma(x). \tag{3.2}$$

En comparant (3.1) et (3.2) on conclut que  $\sigma\gamma(x) = \gamma(\sigma(x))$ .

- Le raisonnement serait le même, en échangeant les rôles de  $\sigma$  et  $\gamma$ , si on supposait que  $x$  appartient au support de  $\gamma$ .
- Enfin, si  $x$  n'appartient à aucun des deux supports, alors  $\sigma\gamma(x) = \gamma\sigma(x) = x$ .

□

#### Définition 1.4

Soient  $n$  un entier naturel non nul, et  $k$  un entier compris entre 2 et  $n$ . Un élément  $\sigma$  de  $S_n$  s'appelle un cycle de longueur  $k$  (ou  $k$ -cycle) s'il existe une partie  $\{a_1, a_2, \dots, a_k\}$  de  $\{1, \dots, n\}$  telle que

- $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$
- $\text{Supp } \sigma = \{a_1, a_2, \dots, a_k\}$ .

Un tel cycle se note :  $\sigma = (a_1, a_2, \dots, a_k)$ .

Autrement dit, un  $k$ -cycle est un élément de  $S_n$  qui permute circulairement les éléments d'une partie à  $k$  éléments de  $\{1, \dots, n\}$  et fixe les autres :

$$a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_{k-1} \rightarrow a_k \rightarrow a_1.$$

**Exemple:** Dans  $S_4$  le cycle  $(1, 2, 4)$  désigne la permutation

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

△ Un même  $k$ -cycle peut s'écrire de  $k$  façons distinctes. Plus précisément, les  $k$  écritures suivantes

$$(a_1, a_2, \dots, a_k), (a_2, a_3, \dots, a_k, a_1), \dots, (a_k, a_1, a_2, \dots, a_{k-1})$$

désignent toutes le même cycle.

À l'inverse, le support d'un cycle ne suffit pas à le définir : dans  $S_4$ , les cycles  $(1, 2, 4)$  et  $(1, 4, 2)$  ont même support mais sont distincts (exercice : combien y a-t-il de cycles distincts de support donné ? Combien y a-t-il de cycles de longueur  $k$  dans  $S_n$  ?).

#### Proposition 1.5

L'ordre d'un  $k$ -cycle est égal à  $k$ .

Un cas particulier important est celui des cycles de longueur 2, que l'on appelle *transpositions*.

**Proposition 1.6**

Toute permutation peut s'écrire comme produit de transpositions. Autrement dit l'ensemble des transpositions engendre  $S_n$ .

⚠ cette décomposition n'est pas unique!

**Preuve.** Récurrence sur le cardinal du support de  $\sigma$  : si  $x \in \text{Supp } \sigma$  et si  $\tau$  désigne la transposition  $(x, \sigma(x))$  alors le support de  $\sigma' := \tau\sigma$  est contenu strictement dans celui de  $\sigma$ . En effet, comme  $x$  et  $\sigma(x)$  appartiennent à  $\text{Supp } \sigma$ ,  $\text{Fix } \sigma \subset \text{Fix } \sigma'$ . Mais par ailleurs, par construction,  $x \in \text{Fix } \sigma' \setminus \text{Fix } \sigma$ .  $\square$

## 2 Décomposition en cycles disjoints

**Définition 2.1 (orbite)**

Soit  $x \in \{1, \dots, n\}$  et  $\sigma \in S_n$ . On appelle orbite de  $x$  sous l'action de  $\sigma$  l'ensemble

$$\text{Orb}_\sigma(x) := \left\{ \sigma^k(x) : k \in \mathbb{Z} \right\}.$$

**Proposition 2.2**

Soit  $\sigma \in S_n$ . Pour tout  $x \in \{1, \dots, n\}$ , il existe un plus petit entier naturel non nul  $k$  tel que  $\sigma^k(x) = x$ . On a alors  $\text{Orb}_\sigma(x) = \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$ , en particulier les éléments  $\sigma^\ell(x)$ ,  $0 \leq \ell \leq k-1$ , sont deux à deux distincts.

**Preuve.** Le groupe  $S_n$  est d'ordre fini donc  $\sigma$  est d'ordre fini. Si l'on note  $d$  cet ordre on a bien sûr  $\sigma^d(x) = x$ . L'ensemble  $\{j \geq 1 : \sigma^j(x) = x\}$  est donc non vide et minoré car inclus dans  $\mathbb{N}$ . Cet ensemble admet un plus petit élément  $k$ .

Soit  $m \in \mathbb{Z}$  un entier. La division euclidienne de  $m$  par  $k$  s'écrit  $m = kq + r$ , avec  $0 \leq r < k$ . On a  $\sigma^m(x) = \sigma^r(x)$  ce qui démontre que  $\text{Orb}_\sigma(x)$  ne contient pas d'autres éléments que  $x, \sigma(x), \dots, \sigma^{k-1}(x)$ . Enfin s'il existe des entiers  $k-1 \geq i > j \geq 0$  avec  $\sigma^i(x) = \sigma^j(x)$  on déduit  $\sigma^{i-j}(x) = x$  ce qui contredit la minimalité de  $k$ . Cela démontre la seconde partie de l'assertion.  $\square$

**Exercice :** Montrer que le cardinal de l'orbite d'un élément de  $\{1, \dots, n\}$  sous l'action d'une permutation  $\sigma \in S_n$  divise l'ordre de  $\sigma$  comme élément de  $S_n$ .

**Proposition 2.3**

Les orbites sous l'action d'une permutation  $\sigma$  de  $S_n$  fournissent une partition de l'ensemble  $\{1, \dots, n\}$ . Plus précisément, il existe des éléments  $x_1, x_2, \dots, x_r$  dans  $\{1, \dots, n\}$  tels que  $\{1, \dots, n\}$  soit la réunion disjointe des orbites  $\text{Orb}_\sigma(x_1), \dots, \text{Orb}_\sigma(x_r)$  :

$$\{1, \dots, n\} = \bigsqcup_{i=1}^r \text{Orb}_\sigma(x_i).$$



**Preuve.** On remarque que la relation "x appartient à la même orbite que y sous l'action de  $\sigma$ " est une relation d'équivalence sur  $\{1, \dots, n\}$ . La réflexivité et la symétrie sont évidentes :  $x = \sigma^0(x)$  et  $y = \sigma^j(x)$  ssi  $x = \sigma^{-j}(y)$ . Enfin, si  $y = \sigma^j(x)$  et  $z = \sigma^k(y)$  alors  $z = \sigma^{k+j}(x)$  d'où la transitivité.

Les orbites sont donc par définition les classes d'équivalence modulo cette relation et on en déduit la proposition.  $\square$

Le théorème suivant est fondamental. Il fournit une décomposition "canonique" pour toute permutation.

#### **Théorème 2.4**

*Toute permutation différente de l'identité se décompose de façon essentiellement unique comme produit commutatif de cycles disjoints. Autrement dit, pour tout  $\sigma \in S_n \setminus \{\text{Id}\}$  il existe des cycles  $c_1, \dots, c_s$  à supports disjoints tels que*

$$\sigma = c_1 c_2 \dots c_s$$

*et cette décomposition est unique à l'ordre près des facteurs.*

**Preuve.**

- **Existence :** soient  $\Omega_1 = \text{Orb}_\sigma(x_1), \Omega_2 = \text{Orb}_\sigma(x_2), \dots, \Omega_s = \text{Orb}_\sigma(x_s)$  les orbites de  $\sigma$  non réduites à un point. Elles forment une partition du support de  $\sigma$ , dont on note les cardinaux  $k_1, k_2, \dots, k_s$  respectivement. On considère alors les cycles

$$c_1 = (x_1, \sigma(x_1), \dots, \sigma^{k_1-1}(x_1)), c_2 = (x_2, \sigma(x_2), \dots, \sigma^{k_2-1}(x_2)), \dots \\ \dots, c_s = (x_s, \sigma(x_s), \dots, \sigma^{k_s-1}(x_s))$$

et on vérifie immédiatement que  $\sigma = c_1 c_2 \dots c_s$ .

- **Unicité :** elle est claire car les cycles sont déterminés par  $\sigma$ .  $\square$

#### **Corollaire 2.5**

*L'ordre d'une permutation est égale au ppcm des longueurs des cycles à supports disjoints qui la composent.*

## 3 Conjugaison

### **Définition 3.1 (Conjugaison)**

*Dans un groupe  $G$  noté multiplicativement le conjugué d'un élément  $x \in G$  par un élément  $g \in G$  est l'élément  $g x g^{-1}$  de  $G$ .*

*La classe de conjugaison de  $x \in G$  est l'ensemble des conjugués de  $x$  dans  $G$  : c'est la partie  $\{g x g^{-1} : g \in G\}$  de  $G$ .*

**Remarque.** La propriété, pour 2 éléments de  $G$ , d'être conjugués, est une relation d'équivalence sur  $G$ .

On dispose d'une formule commode pour la conjugaison d'un cycle par une permutation de  $S_n$ .

**Proposition 3.2**

Soit  $2 \leq k \leq n$  des entiers et soit  $(a_1, a_2, \dots, a_k)$  un  $k$ -cycle de  $S_n$ . Pour tout  $\gamma \in S_n$ , on a

$$\gamma(a_1, a_2, \dots, a_k)\gamma^{-1} = (\gamma(a_1), \gamma(a_2), \dots, \gamma(a_k)).$$

En particulier le conjugué d'un  $k$ -cycle est encore un  $k$ -cycle.

**Preuve.** On évalue les membres de gauche et de droite en  $\gamma(a_i)$ . Dans les deux cas cela donne  $\gamma(a_{i+1})$  (resp.  $\gamma(a_1)$ ) si  $i < k$  (resp. si  $i = k$ ). Pour un indice  $\ell \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$ , l'évaluation des membres de gauche et de droite en  $\gamma(\ell)$  donne  $\gamma(\ell)$ . On a donc l'égalité de permutations annoncée.  $\square$

**Exercice**

- 1) Montrer que  $S_n$  est engendré par les transpositions de la forme  $(1, i)$ , avec  $2 \leq i \leq n$  (utiliser la proposition 1.6).
- 2) Montrer que  $S_n$  est engendré par les transpositions de la forme  $(i, i + 1)$ , avec  $1 \leq i \leq n - 1$ .
- 3) Montrer que  $S_n$  est engendré par  $\{(1, 2), (1, 2, \dots, n)\}$  (pour réaliser n'importe lequel des  $52!$  mélanges de cartes possibles on peut se contenter de répéter les opérations consistant soit à permuter les 2 premières cartes du paquet soit à faire passer la dernière carte en premier).

**Corollaire 3.3**

Soient  $\sigma = c_1 \dots c_s$  et  $\sigma' = c'_1 \dots c'_t$  les décompositions en cycles à supports disjoints de deux éléments de  $S_n$ . Les permutations  $\sigma$  et  $\sigma'$  sont conjugués si et seulement si pour tout  $2 \leq i \leq n$ ,  $\#\{1 \leq j \leq s \mid \text{ord}(c_j) = i\} = \#\{1 \leq k \leq t \mid \text{ord}(c'_k) = i\}$ .

En particulier, deux cycles de  $S_n$  sont conjugués entre eux si et seulement si ils ont même ordre.

## 4 Signature et groupe alterné

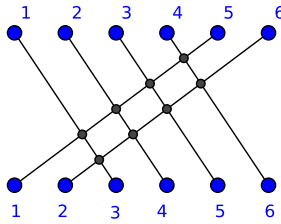
**Définition 4.1**

Soit  $\sigma \in S_n$ . On dit que  $\sigma$  réalise une inversion sur le couple  $(i, j)$  si  $i < j$  et  $\sigma(i) > \sigma(j)$ . On note  $I(\sigma)$  le nombre d'inversions réalisées par  $\sigma$ . La signature de  $\sigma$  est le nombre

$$\epsilon(\sigma) = (-1)^{I(\sigma)}.$$

Autrement dit,  $\epsilon(\sigma)$  vaut  $+1$  ou  $-1$  selon que  $\sigma$  réalise un nombre pair ou impair d'inversions.

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



$$\varepsilon(\sigma) = (-1)^8 = +1$$

### Proposition 4.2

1) La signature d'une permutation  $\sigma \in S_n$  est donnée par la formule

$$\varepsilon(\sigma) = \prod_{\{i,j\} \in \mathcal{P}} \frac{\sigma(i) - \sigma(j)}{i - j}$$

où le produit est pris sur l'ensemble  $\mathcal{P}$  des paires  $\{i, j\}$  d'éléments de  $\{1, \dots, n\}$ .

2) Une transposition est de signature  $-1$ .

3) La signature est un morphisme de groupes  $S_n \rightarrow \{\pm 1\}$  :

$$\forall \sigma \in S_n, \forall \gamma \in S_n, \varepsilon(\sigma\gamma) = \varepsilon(\sigma)\varepsilon(\gamma).$$

Ce morphisme est surjectif dès que  $n \geq 2$ ; son noyau est alors un sous-groupe d'indice 2 de  $S_n$  appelé groupe alterné. On note ce sous-groupe  $A_n$ .

### Preuve.

1) On voit que le membre de droite est

- bien défini car  $\frac{\sigma(i) - \sigma(j)}{i - j} = \frac{\sigma(j) - \sigma(i)}{j - i}$ , donc indépendant de l'ordre de la paire  $\{i, j\}$ ;
- par définition du même signe que  $\varepsilon(\sigma)$ ;
- de valeur absolue 1 car, puisque  $\sigma$  est une bijection, l'ensemble des couples  $\{\sigma(i), \sigma(j)\}$  est égal à l'ensemble des couples  $\{i, j\}$ .

2) Notons  $i < j$  les termes échangés par la transposition, de sorte qu'elle est égale à

$$\begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}.$$

Les paires en inversion sont les paires de la forme  $\{i, k\}$  avec  $k$  compris entre  $i+1$  et  $j$  et celles de la forme  $\{k, j\}$  avec  $k$  compris entre  $i+1$  et  $j-1$ . Au total, il y a  $(j-i) + (j-i-1)$  soit un nombre impair d'inversions, et l'imparité de la permutation en découle.

3) Il suffit d'écrire

$$\begin{aligned} \varepsilon(\sigma\gamma) &= \prod_{\{i,j\} \in \mathcal{P}} \frac{\sigma\gamma(i) - \sigma\gamma(j)}{i-j} \\ &= \prod_{\{i,j\} \in \mathcal{P}} \frac{\sigma\gamma(i) - \sigma\gamma(j)}{\gamma(i) - \gamma(j)} \prod_{\{i,j\} \in \mathcal{P}} \frac{\gamma(i) - \gamma(j)}{i-j} \\ &= \prod_{\{i,j\} \in \mathcal{P}} \frac{\sigma(i) - \sigma(j)}{i-j} \prod_{\{i,j\} \in \mathcal{P}} \frac{\gamma(i) - \gamma(j)}{i-j} \end{aligned}$$

la dernière égalité étant justifiée par le fait que  $\gamma$  induit une bijection de  $\mathcal{P}$  sur lui-même.

Ainsi  $\varepsilon: S_n \rightarrow \{\pm 1\}$  est un morphisme de groupes. Comme la signature d'une transposition vaut  $-1$ , ce morphisme est surjectif pour  $n \geq 2$ . Enfin si  $\tau$  est une transposition de  $S_n$ , les classes à gauche  $A_n$  et  $\tau A_n$  de  $S_n$  modulo  $A_n$  sont distinctes et leur réunion vaut  $S_n$  (en effet, si  $\varepsilon(\sigma) = -1$ , alors  $\sigma = \tau(\tau\sigma)$  avec  $\tau\sigma \in A_n$ ). Donc  $A_n$  est d'indice 2 dans  $S_n$ .  $\square$

### Proposition 4.3

1) La signature d'un  $k$ -cycle est égale à  $(-1)^{k-1}$ .

2) Soit  $c_1 c_2 \dots c_s$  la décomposition en cycles à supports disjoints d'une permutation  $\sigma \in S_n$ . On note  $r$  le nombre de points fixes de  $\sigma$ . On a alors

$$\varepsilon(\sigma) = (-1)^{n-(s+r)}.$$

**Preuve.**

1) On remarque que tout  $k$ -cycle peut se décomposer (de manière non canonique) comme produit de  $k-1$  transpositions

$$(i_1, i_2, \dots, i_k) = (i_1, i_k) \circ (i_1, i_{k-1}) \circ \dots \circ (i_1, i_2).$$

La signature étant un morphisme de groupes dont la valeur en toute transposition est  $-1$ , on conclut.

- 2) C'est un corollaire immédiat du point précédent et de la multiplicativité de la signature (i.e. du fait que la signature est un morphisme) : en notant  $k_i$  la longueur du cycle  $c_i$ , on a

$$\varepsilon(\sigma) = (-1)^{(\sum_{i=1}^s k_i) - s} = (-1)^{n - r - s}.$$

□

**Remarques :** en combinant les propositions 1.6 et 4.2, on constate que la signature d'une permutation  $\sigma$  est égale à  $+1$  (resp.  $-1$ ) si  $\sigma$  se décompose en un produit d'un nombre *pair* (resp. *impair*) de transpositions. Ceci constitue un moyen de calcul parfois utile de la signature, si l'on dispose d'une décomposition en produit de transpositions.

En combinant le théorème 2.4 et la preuve du point 1) de la proposition précédente, on retrouve le fait qu'une permutation se décompose en produit de transpositions (proposition 1.6).

#### Exercice

Soit  $f : S_n \rightarrow \mathbb{Z}/2\mathbb{Z}$  un morphisme de groupe. Montrer que si  $f((1,2)) = \bar{0}$  alors  $f$  est constant.

## 5 Le théorème de Cayley

### Théorème 5.1 (Théorème de Cayley)

Tout groupe fini  $G$  d'ordre  $n$  est isomorphe à un sous-groupe du groupe symétrique  $S_n$ .

**Preuve.** Pour tout  $g \in G$ , on note  $\tau_g$  l'application de  $G$  dans  $G$  définie par  $\tau_g(x) = gx$ . On peut voir que  $\tau_g \circ \tau_{g'} = \tau_{gg'}$ . Ce qui montre que les  $\tau_g$  sont des bijections et que l'application  $\rho : G \rightarrow \text{Sym}(G)$  qui à  $g$  associe  $\tau_g$  est un morphisme de groupes. Ce morphisme est clairement injectif (il suffit de regarder  $\tau_g(e)$  pour s'en convaincre).

Par ailleurs, comme  $G$  est d'ordre  $n$  il existe une bijection  $f : G \rightarrow \{1, \dots, n\}$ . L'application  $\Phi : \text{Sym}(G) \rightarrow S_n, \varphi \mapsto f \circ \varphi \circ f^{-1}$  est un isomorphisme de groupes (vu que  $\forall (\varphi_1, \varphi_2) \in f \circ (\varphi_1 \varphi_2) \circ f^{-1} = (f \circ \varphi_1 \circ f^{-1})(f \circ \varphi_2 \circ f^{-1})$  et que  $\Phi^{-1}(\sigma) = f^{-1} \circ \sigma \circ f$ ).

Ainsi,  $\Phi \circ \rho$  est un morphisme de groupe injectif et son image est un sous-groupe de  $S_n$  isomorphe à  $G$ . □



# Chapitre 4

## Anneaux

On débute dans ce chapitre l'étude d'une structure relative à deux lois de composition interne. Le point de départ est un groupe abélien dont on note "+" la loi. Si l'ensemble en question est muni d'une seconde loi vérifiant certains axiomes et compatibilités vis à vis de la loi "+", on dit alors que c'est un *anneau*. On croise ce type de structure en permanence en mathématiques :  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $M_n(\mathbb{R})$ ,  $\mathbb{Z}/n\mathbb{Z}$ ,  $\text{End}(E)$ ,  $\mathbb{Q}[X]$ ,... sont des anneaux.

### 1 Définitions

#### Définition 1.1

Un anneau est la donnée d'un triplet  $(A, +, \cdot)$  où  $A$  est un ensemble et  $+$  et  $\cdot$  sont deux lois de composition internes telles que

- 1)  $(A, +)$  est un groupe abélien d'élément neutre noté 0.
- 2) La multiplication est associative :  $\forall (a, b, c) \in A^3$ ,  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- 3) La multiplication est distributive par rapport à l'addition, ce qui signifie que pour tout  $(a, b, c) \in A^3$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{et} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

- 4) La multiplication possède un élément neutre noté 1 (on dit que l'anneau  $A$  est unitaire) caractérisé par la propriété

$$\forall a \in A, a \cdot 1 = 1 \cdot a = a.$$

De plus, l'anneau  $A$  est dit **commutatif** si la multiplication est commutative.

**Remarque :** dans certains ouvrages, seuls les trois premiers axiomes ci-dessus sont demandés pour définir un anneau (*i.e.* on n'exige pas qu'il y ait un élément neutre

pour la multiplication). Dans ce cas, un anneau vérifiant l'axiome 4) ci-dessus est appelé anneau *unitaire*.

**Proposition 1.2**

$(A, +, \cdot)$  un anneau.

- 1)  $\forall x \in A, 0 \cdot x = x \cdot 0 = 0.$
- 2) L'élément neutre pour  $\cdot$  est unique.
- 3) Si  $A \neq \{0\}$  alors  $0 \neq 1.$
- 4)  $\forall x, y \in A, x \cdot (-y) = (-x) \cdot y = -x \cdot y.$

**Preuve.**

- 1)  $x = (1 + 0)x = 1x + 0x = x + 0x \Rightarrow 0x = 0.$  On montre de même  $x \cdot 0 = 0.$
- 2) Si 1 et 1' sont éléments neutres pour la multiplication alors  $1 \cdot 1' = 1$  et  $1 \cdot 1' = 1'.$
- 3) Si  $0 = 1$  alors  $\forall x \in A, x = 1x = 0x = 0.$
- 4)  $(-x)y + xy = (-x + x)y = 0.$  De même  $x \cdot (-y) + xy = x \cdot (-y + y) = 0.$

□

Dans la suite on omettra le plus souvent de préciser les lois relatives à la structure d'anneau : on écrira "soit  $A$  un anneau" et l'on sous-entendra alors que les lois correspondantes sont notées "+" et ".".

Dans un anneau commutatif, les identités remarquables du collège sont encore vraie :

**Proposition 1.3 (Binôme de Newton)**

Soit  $A$  un anneau et  $a, b$  des éléments de  $A$  dont on suppose qu'ils commutent i.e.  $ab = ba.$  Alors pour tout  $n \in \mathbb{Z}_{\geq 1},$  on a :

- 1)  $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k},$
- 2)  $a^n - b^n = (a - b) \sum_{j=1}^n a^{n-j} b^{j-1}.$

Une différence majeure entre  $+$  et  $\cdot$  : tous les éléments ne sont pas nécessairement inversibles pour la multiplication. Cette remarque induit la définition suivante.



**Définition 1.4**

Un élément  $a$  de  $A$  est dit inversible s'il existe  $b \in A$  tel que  $ab = ba = 1$ . L'ensemble des éléments inversibles (aussi appelés unités) de  $A$  est noté  $A^\times$  ou  $U(A)$ .

**Remarque-Exercice :** Certains auteurs parlent d'inverse à droite et à gauche (un élément peut avoir un inverse à droite mais pas à gauche...).

Montrer que si  $a \in A$  admet un inverse à droite et un inverse à gauche alors ils sont uniques et sont égaux (mieux : si  $a \in A$  admet un unique inverse à droite, alors il admet un inverse à gauche...).

**Proposition 1.5**

Si  $A$  est un anneau,  $A^\times$  est un groupe multiplicatif de neutre 1.

**Exercice.** Déterminer  $A^\times$  lorsque  $A = \mathbb{Z}, \mathbb{R}, \mathbb{Q}[X], \mathbb{Z}/n\mathbb{Z}, \{a + ib : a, b \in \mathbb{Z}\}$ .

**Définition 1.6 (Sous-anneau et produit cartésien d'anneaux)**

1) Un sous-anneau d'un anneau  $A$  est une partie  $B$  de  $A$  telle que

- (a)  $(B, +)$  est un sous-groupe de  $(A, +)$ ,
- (b)  $B$  est stable pour la multiplication,
- (c)  $1_A$  appartient à  $B$ .

2) Si  $A$  et  $B$  sont deux anneaux, leur produit cartésien  $A \times B$  est canoniquement muni d'une structure d'anneau en posant :

- $(x, y) + (x', y') = (x + x', y + y')$ ,
- $(x, y) \cdot (x', y') = (xx', yy')$

les éléments neutres pour l'addition et la multiplication étant définis respectivement par  $0_{A \times B} = (0_A, 0_B)$  et  $1_{A \times B} = (1_A, 1_B)$ .

**Proposition 1.7**

Si  $A$  est un anneau et  $B$  est un sous-anneau de  $A$  alors  $B$  est un anneau pour les lois induites par celles de  $A$ .

Pour montrer qu'un ensemble est un anneau, il est souvent commode (comme dans le cas des groupes) de montrer que c'est un sous-anneau d'un anneau déjà connu (exemple : pour montrer que  $\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\}$  est un anneau, on peut commencer par remarquer que  $\mathbb{Z}[i] \subseteq \mathbb{C}$ ).

**Définition 1.8 (Éléments nilpotents, diviseurs de zéros, anneaux intègres)**

Soit  $A$  un anneau.

1) Un élément  $a \in A$  est dit nilpotent s'il existe  $n \in \mathbb{N}$  tel que  $a^n = 0$ .

- 2) Un élément  $a \in A$  est diviseur de zéro s'il est non nul et s'il existe soit un élément  $b \in A \setminus \{0\}$  tel que  $ab = 0$  (on dit que  $a$  est diviseur de zéro à gauche), soit un élément  $c \in A \setminus \{0\}$  tel que  $ca = 0$  (on dit que  $a$  est diviseur de zéro à droite).
- 3) L'anneau  $A$  est intègre s'il est commutatif, si  $1 \neq 0$ , et s'il n'admet pas de diviseur de zéro.
- 4) Un anneau commutatif est un corps si  $1 \neq 0$  et si tout élément non nul est inversible pour la multiplication.

**Exemples.** • Les anneaux  $\mathbb{Z}$ ,  $\mathbb{R}$ ,  $\mathbb{Q}[X]$  sont intègres. Les anneaux  $\mathbb{Z}/6\mathbb{Z}$  (cf proposition ci-dessous),  $M_n(\mathbb{R})$  ( $n \geq 2$ ) ne sont pas intègres.

- Les anneaux  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  sont des corps,  $\mathbb{Z}$  n'est pas un corps.
- Un produit d'anneaux différents de  $\{0\}$  n'est jamais intègre :  $(0_A, 1_B)(1_A, 0_B) = 0_{A \times B}$ .

**Remarque.** Les éléments nilpotents et les diviseurs de zéro ne sont bien sûr jamais inversibles. **Un corps est intègre**, mais la réciproque n'est pas toujours vraie. En revanche cette réciproque est vraie pour un anneau fini : un anneau fini est intègre si et seulement si c'est un corps. (Exercice : démontrer toutes les affirmations contenues dans cette remarque.)

### Proposition 1.9

Soit  $n \in \mathbb{Z}_{\geq 1}$ , alors  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  où les lois sont définies par

$$\begin{aligned}\bar{a} + \bar{b} &= \overline{a + b}, \\ \bar{a} \times \bar{b} &= \overline{ab},\end{aligned}$$

est un anneau. De plus on a les équivalences :

$$\mathbb{Z}/n\mathbb{Z} \text{ est intègre} \Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ est un corps} \Leftrightarrow n \text{ est premier.}$$

### Définition 1.10

L'anneau  $A$  est dit euclidien s'il est intègre et s'il existe une fonction (appelée stathme euclidien)

$$\phi: A \setminus \{0\} \rightarrow \mathbb{N}$$

telle que pour tout couple  $(a, b)$  d'éléments de  $A$ , avec  $b \neq 0$ , il existe  $q, r \in A$  tels que

$$a = bq + r, \quad (r = 0 \text{ ou } \phi(r) < \phi(b)).$$

**Exemples.** • L'anneau des entiers  $\mathbb{Z}$  est euclidien pour le choix  $\phi = |\cdot|$ .

- Si  $K$  est un corps, l'anneau  $K[X]$  est euclidien pour le choix  $\phi = \deg$ ; la fonction

degré. Aussi  $K$  lui-même est euclidien pour la fonction  $\phi$  constante égale à 1. (Cela dit, faire des divisions euclidiennes dans un corps ne présente pas grand intérêt.)

• L'anneau des *entiers de Gauss*  $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$  est euclidien relativement à la restriction de la fonction "carré du module"  $z \in \mathbb{C} \mapsto |z|^2$  (cf TD).

Dans  $\mathbb{Z}$  et  $K[X]$ , on sait effectuer la division euclidienne pour trouver  $q$  et  $r$ . Dans  $\mathbb{Z}[i]$ , c'est un peu plus compliqué (cf TD).

## 2 Morphismes d'anneaux

De même que pour les groupes, les espaces vectoriels... on porte un intérêt particulier aux applications respectant la structure d'anneaux.

### Définition 2.1

Soient  $A$  et  $B$  deux anneaux. Une application  $f: A \rightarrow B$  est un morphisme d'anneaux si

- 1)  $c'$  est un morphisme de groupes additifs de  $(A, +)$  dans  $(B, +)$ ,
- 2)  $\forall (x, y) \in A^2, f(xy) = f(x)f(y)$ ,
- 3)  $f(1_A) = 1_B$ .

### Exemples.

- 1) Pour  $n \geq 1$ , la surjection canonique  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  est un morphisme d'anneaux.
- 2) La conjugaison complexe  $a + ib \mapsto a - ib$  est un morphisme d'anneaux  $\mathbb{C} \rightarrow \mathbb{C}$ .
- 3) Soit  $\alpha = 2^{1/3}$  l'unique solution réelle à l'équation  $x^3 = 2$ . On note  $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \dots + a_r\alpha^r : a_i \in \mathbb{Q}, r \in \mathbb{N}\} = \{a_0 + a_1\alpha + a_2\alpha^2 : a_i \in \mathbb{Q}\}$ ; c'est un sous-anneau de  $\mathbb{C}$  (et même de  $\mathbb{R}$ ). L'application d'évaluation

$$\text{eval}_\alpha: \mathbb{Q}[X] \rightarrow \mathbb{Q}[\alpha], \quad f(X) \mapsto f(\alpha),$$

est un morphisme d'anneaux.

- 4) Soit  $P \in GL_n(\mathbb{R})$ . L'application  $A \mapsto P^{-1}AP$  de  $M_n(\mathbb{R})$  dans lui-même est un morphisme d'anneaux.

### Définition 2.2

Soit  $f: A \rightarrow B$  un morphisme d'anneaux. Le noyau de  $f$  est

$$\ker f := \{x \in A : f(x) = 0\}$$

et l'image de  $f$  est  $\text{Im}(f) := f(A)$ .

Si  $f$  est injectif (i.e.  $\ker f = \{0\}$ ) et surjectif (i.e.  $\text{Im}(f) = B$ ), on dit que  $f$  est un isomorphisme d'anneaux.

### Proposition 2.3

Soit  $f: A \rightarrow B$  un morphisme d'anneaux. L'image directe par  $f$  d'un sous-anneau de  $A$  est un sous-anneau de  $B$  et l'image réciproque par  $f$  d'un sous-anneau de  $B$  est un sous-anneau de  $A$ .

△ Si  $f: A \rightarrow B$  est un morphisme d'anneaux,  $\text{Im}(f)$  est un sous-anneau de  $B$ , mais  $\ker f$  n'est pas un sous-anneau de  $A$  en général (ie dès que  $1_B \neq 0_B$ ), puisque  $f$  doit vérifier  $f(1_A) = 1_B$ .

## 3 L'anneau $\mathbb{Z}/n\mathbb{Z}$ et le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

Donnons pour commencer l'énoncé du théorème des restes chinois.

### Proposition 3.1 (Th. des restes chinois)

Soit  $a, b$  deux entiers premiers entre eux alors l'application

$$\mathbb{Z}/ab\mathbb{Z} \rightarrow (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}), \quad x \bmod ab \mapsto (x \bmod a, x \bmod b),$$

est un isomorphisme d'anneaux.

**Preuve.** Il est facile de vérifier que l'application est un morphisme d'anneaux. Elle est en outre injective car si  $x$  est divisible par  $a$  et par  $b$ , il est divisible par  $ab$  en vertu du lemme de Gauss puisque  $a$  et  $b$  sont premiers entre eux. Enfin  $\mathbb{Z}/ab\mathbb{Z}$  et  $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$  ont même cardinal  $ab$  donc l'application est bijective.  $\square$

**Remarque** On peut expliciter la réciproque de cette application. En effet, puisque  $\text{pgcd}(a, b) = 1$  il existe par le théorème de Bézout  $(u, v) \in \mathbb{Z}^2$  tel que  $au + bv = 1$ . On vérifie alors immédiatement que pour tout  $(y \bmod a, z \bmod b) \in (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ , l'image de  $x = ybv + zau \bmod ab \in \mathbb{Z}/ab\mathbb{Z}$  dans  $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$  est égale à  $(y \bmod a, z \bmod b)$ .

Soit  $n \in \mathbb{Z}_{\geq 1}$ . Dans l'anneau  $\mathbb{Z}/n\mathbb{Z}$ , on s'intéresse maintenant au groupe des unités  $(\mathbb{Z}/n\mathbb{Z})^\times$ . Rappelons les caractérisations de l'inversibilité d'une classe modulo  $n$ .

### Proposition 3.2

Soit  $n$  un entier naturel non nul. Alors, pour tout entier relatif  $k$ , les propriétés suivantes sont équivalentes :

- 1) la classe de  $k$  modulo  $n$  est inversible pour la multiplication.
- 2) la classe de  $k$  modulo  $n$  est un générateur du groupe additif  $(\mathbb{Z}/n\mathbb{Z}, +)$ .
- 3)  $k$  est premier à  $n$ .

**Preuve.** Les trois propriétés sont toutes des conséquences du fait que  $\text{pgcd}(k, n) = 1$  ssi il existe  $(u, v) \in \mathbb{Z}^2$  tel que  $ku + nv = 1$  (corollaire du théorème de Bézout).  $\square$

On rappelle la définition de l'indicatrice d'Euler d'un entier  $n \geq 1$  : il s'agit de la fonction  $\varphi$  définie par  $\varphi(1) = 1$ , et pour tout  $n \geq 2$  :

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

On commence par établir une formule qui d'une part permet en principe de calculer  $\varphi(n)$  récursivement, et jouera d'autre part un rôle important dans la démonstration de la cyclicité de  $(\mathbb{Z}/p\mathbb{Z})^\times$  pour  $p$  premier.

**Proposition 3.3**

Soit  $n \in \mathbb{Z}_{\geq 1}$ . On a l'égalité :

$$\sum_{d|n} \varphi(d) = n.$$

**Preuve.** Comme  $\mathbb{Z}/n\mathbb{Z}$  est cyclique, il y a pour tout diviseur  $d$  de  $n$ , un unique sous-groupe (nécessairement cyclique) d'ordre  $d$  dans  $\mathbb{Z}/n\mathbb{Z}$ . Ce sous-groupe est donc isomorphe à  $\mathbb{Z}/d\mathbb{Z}$  et admet donc  $\varphi(d)$  générateurs d'après la proposition 3.2. On partitionne  $\mathbb{Z}/n\mathbb{Z}$  en :

$$\bigcup_{d|n} S_d, \quad S_d := \{\bar{a} : |\langle \bar{a} \rangle| = d\},$$

et l'on obtient donc l'égalité annoncée.  $\square$

On peut aussi donner une formule explicite de  $\varphi(n)$  lorsque l'on connaît la factorisation de  $n$  en produit de nombres premiers. Pour cela on a besoin du lemme suivant :

**Lemme 3.4**

- 1) Si  $f : A \longrightarrow B$  est un isomorphisme d'anneaux, alors  $B^\times \simeq A^\times$  ( $B^\times = f(A^\times)$ ).
- 2) Si  $A$  et  $B$  sont deux anneaux, alors  $(A \times B)^\times = A^\times \times B^\times$ .

Si  $a$  et  $b$  premiers entre eux, le théorème des restes chinois et ce lemme entraînent que

$$(\mathbb{Z}/ab\mathbb{Z})^\times \simeq (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times \text{ si } a \wedge b = 1$$

En comparant les cardinaux, on prouve que la fonction indicatrice d'Euler est multiplicative ie que

$$a \wedge b = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b).$$

On en déduit une formule annoncée :

**Proposition 3.5**

1) Si  $p$  est un nombre premier et  $k$  un entier naturel non nul, on a

$$\varphi(p^k) = p^{k-1}(p - 1).$$

2) Si  $n$  est un entier naturel non nul et si  $P_n$  désigne l'ensemble des nombres premiers qui le divisent, on a

$$\varphi(n) = n \prod_{p \in P_n} \left(1 - \frac{1}{p}\right).$$

**Preuve.**

1) Comme  $p$  est premier, les entiers compris entre 1 et  $p^k$  qui ne sont pas premiers avec  $p^k$  sont ceux qui s'écrivent  $p\ell$  avec  $1 \leq \ell \leq p^{k-1}$ . Ils sont donc au nombre de  $p^{k-1}$  et  $\varphi(p^k) = p^k - p^{k-1}$ .

2) Si  $n = p_1^{k_1} \dots p_r^{k_r}$  avec les  $p_i$  premiers et deux à deux distincts, et les  $k_i \geq 1$ , il suffit d'utiliser la multiplicativité de la fonction  $\varphi$  pour obtenir

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1}) \dots \varphi(p_r^{k_r}) = p_1^{k_1-1}(p_1 - 1) \dots p_r^{k_r-1}(p_r - 1) \\ &= p_1^{k_1} \dots p_r^{k_r} \frac{p_1 - 1}{p_1} \dots \frac{p_r - 1}{p_r} = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right). \end{aligned}$$

**Remarque** En revenant un peu en arrière, on peut voir l'égalité  $\varphi(n) = \varphi(p_1^{k_1}) \dots \varphi(p_r^{k_r})$  de la preuve ci-dessus comme provenant de l'isomorphisme □

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \dots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^\times.$$

Pour connaître  $(\mathbb{Z}/n\mathbb{Z})^\times$  il suffit de déterminer les  $(\mathbb{Z}/p^k\mathbb{Z})^\times$  pour  $p$  premier.

**Théorème 3.6**

Pour tout nombre premier  $p$ , le groupe  $(\mathbb{Z}/p\mathbb{Z})^\times$  est cyclique d'ordre  $p - 1$ .

**Preuve.** Soit  $d$  un diviseur de  $p - 1$  et soit  $\psi(d)$  le nombre d'éléments de  $(\mathbb{Z}/p\mathbb{Z})^\times$  d'ordre  $d$ . Supposons que  $(\mathbb{Z}/p\mathbb{Z})^\times$  admette un élément  $a$  d'ordre  $d$  et soit  $H = \langle a \rangle$ . Chaque élément de  $H$  satisfait l'équation polynomiale  $x^d = 1$ . Comme  $\mathbb{Z}/p\mathbb{Z}$  est un corps, cette équation a au plus  $d$  solutions (cf théorème 4.10 ci-dessous). Ainsi par cardinalité  $H = \{x \in G : x^d = 1\}$  et  $H$  contient tous les éléments d'ordre  $d$  de  $(\mathbb{Z}/p\mathbb{Z})^\times$ . Comme  $H$  est cyclique d'ordre  $d$ , il a  $\varphi(d)$  éléments d'ordre  $d$ . Ce qui montre que si  $\psi(d) \neq 0$  alors  $\psi(d) = \varphi(d)$ . Comme de plus

$$\sum_{d|p-1} \psi(d) = p - 1 = \sum_{d|p-1} \varphi(d),$$

on a  $\psi(d) = \varphi(d)$  pour tout diviseur  $d$  de  $p - 1$ . En particulier  $\psi(p - 1) \neq 0$ .  $\square$

On se contente d'énoncer le résultat suivant.

**Proposition 3.7**

- Si  $p \neq 2$  est un nombre premier et si  $k \geq 1$  est un entier alors  $(\mathbb{Z}/p^k\mathbb{Z})^\times$  est cyclique c'est-à-dire isomorphe à  $\mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$ .
- Si  $k \geq 2$  entier, alors  $(\mathbb{Z}/2^k\mathbb{Z})^\times$  n'est pas cyclique, il est isomorphe à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$ .

## 4 Les anneaux de polynômes

### 4.1 Définitions et premières propriétés

**Définition 4.1**

Un polynôme à coefficients dans un anneau  $A$  est une suite  $(a_n)_{n \in \mathbb{N}}$  nulle à partir d'un certain rang, c'est-à-dire telle qu'il existe  $N \in \mathbb{N}$  avec la propriété que  $a_n$  est nul pour tout  $n > N$ . On note  $A[X]$  l'ensemble des polynômes à coefficients dans  $A$ .

Informellement, un polynôme est donc une suite  $(a_0, a_1, a_2, a_3, \dots, a_N, 0, 0, 0 \dots)$ .

**Définition 4.2**

Soient  $P = (a_n)_{n \in \mathbb{N}}$  et  $Q = (b_n)_{n \in \mathbb{N}}$  deux polynômes à coefficients dans  $A$ . Leur somme est le polynôme  $P + Q = (a_n + b_n)_{n \in \mathbb{N}}$  et leur produit est le polynôme  $PQ = (c_n)_{n \in \mathbb{N}}$  où  $c_n$  est défini par la formule

$$c_n = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_{n-1} b_1 + a_n b_0 = \sum_{k=0}^n a_k b_{n-k}.$$



Il faut vérifier que  $P + Q$  et  $PQ$  ainsi définis sont bien des polynômes, c'est-à-dire que leurs coefficients sont nuls à partir d'un certain rang :

On sait qu'il existe  $N_1 \in \mathbb{N}$  tel que  $a_n$  est nul pour tout  $n > N_1$  et  $N_2 \in \mathbb{N}$  tel que  $b_n$  est nul pour tout  $n > N_2$ , donc  $a_n + b_n$  est nul pour tout  $n > \max(N_1, N_2)$  et  $c_n = \sum_{k=0}^n a_k b_{n-k}$  est nul pour tout  $n > N_1 + N_2$ .

**Proposition 4.3**

Muni des deux lois précédentes, l'ensemble  $A[X]$  est un anneau, d'élément neutre additif le polynôme nul  $(0, 0, \dots)$  et d'élément neutre multiplicatif le polynôme  $(1, 0, 0, \dots)$ .

On peut aussi définir une loi externe sur  $A[X]$  : si  $\lambda \in A$  et si  $P = (a_n)_{n \in \mathbb{N}}$ , on définit le produit  $\lambda P = (b_n)_{n \in \mathbb{N}}$  par  $b_n = \lambda a_n$ . On peut remarquer que c'est aussi le produit du polynôme  $(\lambda, 0, 0, 0, \dots)$  par le polynôme  $P$ .

Après ce préambule un peu formel, on peut revenir à une notation plus familière en posant

$$1 := (1, 0, 0, \dots), \quad X := (0, 1, 0, 0, \dots).$$

Le symbole  $X$  ainsi défini est une *indéterminée*. On vérifie alors sans difficulté (récurrence) que  $X^2 = (0, 0, 1, 0, \dots)$ ,  $X^3 = (0, 0, 0, 1, 0, \dots)$ ,  $\dots$ ,  $X^n = (0, 0, \dots, 0, 1, 0, 0, \dots)$ . Avec ces notations, le polynôme  $P = (a_0, a_1, \dots, a_N, 0, 0, \dots)$  s'écrit

$$P = a_0 + a_1X + \dots + a_nX^n.$$

On appelle *monôme* un élément de  $A[X]$  dont exactement un coefficient est non-nul. D'après ce qui précède, un monôme peut toujours s'écrire  $a_iX^i$  pour un certain  $i \in \mathbb{N}$  et un certain  $a_i \in A \setminus \{0\}$ .

#### Définition 4.4

Le degré d'un polynôme  $P$  non nul, noté  $\deg P$ , est le plus grand entier  $n$  tel que le coefficient  $a_n$  de  $X^n$  dans  $P$  soit non nul. Le coefficient  $a_n$  est alors appelé coefficient dominant de  $P$ .

Par convention, le degré du polynôme nul, est égal à  $-\infty$ . On convient également que :

- $n + -\infty = -\infty$  pour tout  $n \in \mathbb{N}$ ,
- $n > -\infty$  pour tout  $n \in \mathbb{N}$ .

Un polynôme de degré 0 (ou le polynôme nul) est dit constant, égal à  $a_0$ .

#### Proposition 4.5

Soient  $P$  et  $Q$  deux polynômes à coefficients dans un anneau  $A$ .

- 1)  $\deg(P + Q) \leq \max(\deg P, \deg Q)$  et on a égalité si  $\deg P \neq \deg Q$ .
- 2) Si  $A$  est **intègre**,  $\deg(PQ) = \deg P + \deg Q$ . En particulier, si  $A$  est intègre,  $A[X]$  est également intègre.

Une conséquence immédiate de la formule  $\deg(PQ) = \deg P + \deg Q$  est le

#### Corollaire 4.6

Soient  $P$  et  $Q$  deux polynômes non nuls à coefficients dans un anneau  $A$  **intègre**. Si  $P$  divise  $Q$ , alors  $\deg P \leq \deg Q$ .

## 4.2 Division euclidienne

Donnons un théorème généralisant le fait, vu au semestre précédent précédent, que  $K[X]$  est un anneau euclidien.



### Théorème 4.7

Soient  $F$  et  $G$  deux polynômes à coefficients dans un anneau intègre  $A$ . Si le coefficient dominant de  $G$  est inversible dans  $A$ , alors il existe un unique couple  $(Q, R)$  de polynômes qui vérifie

$$\begin{cases} F = GQ + R \\ \deg R < \deg G \end{cases}$$

**Preuve.** • Existence. Posons  $G = g_0 + g_1X + \dots + g_dX^d$ , avec  $g_d \in A^\times$  (en particulier,  $\deg G = d$ ) et  $F = f_0 + f_1X + \dots + f_nX^n$ .

- Si  $n < d$ , alors le couple  $(Q, R) = (0, F)$  convient.
- Sinon, le polynôme  $F_1 := F - f_n g_d^{-1} X^{n-d} G$  est de degré strictement inférieur à  $n$ . On reprend alors le processus avec le couple  $(F_1, G)$ .
- Unicité. Si  $F = GQ_1 + R_1 = GQ_2 + R_2$  avec  $\deg R_1 < \deg G$  et  $\deg R_2 < \deg G$ , alors

$$G(Q_1 - Q_2) = R_2 - R_1$$

d'où

$$\deg(G(Q_1 - Q_2)) = \deg G + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg G$$

ce qui n'est possible que si  $Q_1 - Q_2 = 0$ , auquel cas on a également  $R_2 - R_1 = 0$ .  $\square$   
On notera que la preuve de l'existence, dans le résultat ci-dessus n'utilise pas l'hypothèse «  $A$  intègre ». De ce fait la proposition 4.9 ci-dessous vaut pour les polynômes à coefficients dans un anneau commutatif non nécessairement intègre.

### 4.3 Racines et multiplicités

À un polynôme  $P = a_0 + a_1X + \dots + a_nX^n \in A[X]$ , on associe une *fonction polynomiale*

$$\begin{aligned} \tilde{P} : A &\longrightarrow A \\ \alpha &\longmapsto \tilde{P}(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n. \end{aligned}$$



Il faut prendre garde de ne pas identifier un polynôme à la fonction polynomiale qui lui est associée, à cause du gag suivant : le polynôme  $P(X) = X^2 + X \in \mathbb{Z}/2\mathbb{Z}[X]$  est non nul, mais sa fonction polynomiale associée  $\tilde{P}$  l'est, puisque  $\tilde{P}(0) = \tilde{P}(1) = 0$ . Cependant, ce problème ne se pose pas si l'on considère des polynômes à coefficients dans un corps  $K$  infini, car alors l'application  $P \mapsto \tilde{P}$  est injective (exercice).

Ceci étant, on commet le plus souvent l'abus de notation consistant à noter " $P(\alpha)$ " l'image de  $\alpha$  par la fonction  $\tilde{P}$  (plutôt que " $\tilde{P}(\alpha)$ ").

**Définition 4.8**

Avec les notations ci-dessus, on dit que  $\alpha \in A$  est racine de  $P \in A[X]$  si  $\tilde{P}(\alpha) = 0$  dans  $A$ .

**Proposition 4.9**

Les propriétés suivantes sont équivalentes :

- 1)  $\alpha$  est racine de  $P$ .
- 2)  $(X - \alpha)$  divise  $P$ .

**Preuve.** On effectue la division euclidienne de  $P$  par  $X - \alpha$  :

$$P = (X - \alpha)Q + R \text{ avec } \deg R < 1. \quad (4.1)$$

Autrement dit,  $R$  est un polynôme constant. Supposons que  $\alpha$  soit racine de  $P$ . Alors, en évaluant le polynôme  $P$  en  $\alpha$  et en utilisant l'équation (4.1) on obtient

$$0 = P(\alpha) = R(\alpha),$$

ce qui signifie que  $R = 0$  puisque  $R$  est un polynôme constant. Donc  $X - \alpha$  divise  $P$ . Inversement, si  $X - \alpha$  divise  $P$ , alors il existe  $Q \in A[X]$  tel que  $P = (X - \alpha)Q$  auquel cas  $P(\alpha) = 0$ .  $\square$

**Théorème 4.10**

Soient  $\alpha_1, \alpha_2, \dots, \alpha_k$  des racines deux à deux distinctes d'un polynôme  $P \in A[X]$ , où  $A$  est un anneau intègre. Alors le produit  $(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$  divise  $P$ . En particulier, le nombre de racines deux à deux distinctes d'un polynôme  $P$  non nul à coefficients dans un anneau intègre est au plus égal à  $\deg P$ .

**Preuve.** La proposition précédente montre que  $X - \alpha_1$  divise  $P$ ; il existe donc  $Q_1 \in A[X]$  tel que

$$P = (X - \alpha_1)Q_1.$$

Comme  $\alpha_2$  est racine, on a

$$0 = P(\alpha_2) = (\alpha_2 - \alpha_1)Q_1(\alpha_2)$$

et donc  $Q_1(\alpha_2) = 0$  puisque  $\alpha_2 - \alpha_1 \neq 0$  et que  $A$  est intègre. En vertu de la proposition 4.9, on peut donc affirmer que  $X - \alpha_2$  divise  $Q_1$ , c'est-à-dire qu'il existe  $Q_2 \in A[X]$  tel que

$$Q_1 = (X - \alpha_2)Q_2$$

et par conséquent

$$P = (X - \alpha_1)(X - \alpha_2)Q_2.$$

En poursuivant ce raisonnement, on montre que  $(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$  divise  $P$ .  $\square$



Le résultat est faux si l'anneau  $A$  n'est pas intègre. Par exemple, si  $A = \mathbb{Z}/6\mathbb{Z}$  le polynôme  $X^2 - X \in A[X]$  a quatre racines dans  $A$ !

#### Définition 4.11

Soit  $P$  un polynôme à coefficients dans  $A$  et  $\alpha \in A$  une racine de  $P$ . On appelle *multiplicité de la racine  $\alpha$*  le plus grand entier naturel  $n$  tel que  $(X - \alpha)^n$  divise  $P$ .

On obtient alors le raffinement suivant du théorème 4.10 :

#### Théorème 4.12

Soient  $P$  un polynôme à coefficients dans un anneau intègre  $A$  et  $\alpha_1, \alpha_2, \dots, \alpha_k$  ses racines deux à deux distinctes dans  $A$ , de multiplicités respectives  $n_1, n_2, \dots, n_k$ . Alors il existe un polynôme  $Q \in A[X]$ , sans racine dans  $A$ , tel que

$$P = (X - \alpha_1)^{n_1}(X - \alpha_2)^{n_2} \cdots (X - \alpha_k)^{n_k}Q.$$

En particulier, le nombre de racines d'un polynôme non nul  $P \in A[X]$ , comptées avec multiplicité, est majoré par le degré de  $P$ .

**Preuve.** D'après le théorème 4.10,  $P$  se factorise par  $(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$ . Soit

$$P = (X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2} \cdots (X - \alpha_k)^{m_k}Q$$

une factorisation *maximale* de  $P$ , c'est-à-dire que chaque  $m_i \geq 1$  et  $P$  ne peut pas se factoriser davantage par une puissance d'aucun  $(X - \alpha_i)$ , ce qui est équivalent à  $Q(\alpha_i) \neq 0$  pour tout  $i$  d'après la proposition 4.9. On a  $n_i \geq m_i$  par définition de  $n_i$ , donc en simplifiant par  $(X - \alpha_i)^{m_i}$ , on obtient

$$(X - \alpha_i)^{n_i - m_i}P = \prod_{j \neq i} (X - \alpha_j)^{m_j}Q.$$

Or, le membre de droite ne s'annule pas en  $\alpha_i$ , donc le membre de gauche non plus ce qui implique que  $m_i = n_i$  pour tout  $i$ .  $\square$

## 5 Idéal d'un anneau

On définit maintenant la notion très importante d'idéal : les idéaux jouent, pour les anneaux, le rôle que les sous-groupes distingués jouent en théorie des groupes. Dans cette section  $A$  désigne un anneau **commutatif**.

**Définition 5.1**

Un idéal  $I$  de  $A$  est un sous-groupe additif de  $A$  vérifiant :

$$\forall a \in A, \forall x \in I, a \cdot x \in I.$$

**Exemples:**

• Les idéaux de  $\mathbb{Z}$  sont les  $d\mathbb{Z}$ , pour  $d \in \mathbb{N}$ . En effet les sous-groupes de  $(\mathbb{Z}, +)$  sont exactement les  $d\mathbb{Z}$  et l'on vérifie immédiatement que pour tout  $n \in \mathbb{Z}$  et tout  $x \in d\mathbb{Z}$ , on a encore  $nx \in d\mathbb{Z}$ .

• Soit  $P \in \mathbb{Q}[X]$  : l'ensemble des multiples de  $P$  (i.e. l'ensemble  $\{P \cdot Q : Q \in \mathbb{Q}[X]\}$ ) est un idéal de  $\mathbb{Q}[X]$ . On dit qu'il s'agit de l'idéal engendré par  $P$  (cf définition suivante).

**Remarque.** On peut définir la notion d'idéal dans le cadre plus général d'un anneau non nécessairement commutatif. Dans ce cas la définition 5.1 correspond à la notion d'idéal à gauche. On obtient la définition d'idéal à droite en remplaçant la seconde condition par : « pour tout  $a \in A$  et tout  $x \in I$ , on a  $x \cdot a \in I$  ».

**Proposition 5.2**

Soit  $B$  un anneau commutatif et  $f : A \rightarrow B$  un morphisme d'anneaux. Alors l'image réciproque de tout idéal de  $B$  est un idéal de  $A$ . En particulier  $\ker f$  est un idéal de  $A$ . D'autre part, l'image directe d'un idéal de  $A$  est un idéal de  $\text{Im } f$ . En particulier, si  $f$  est surjectif, l'image d'un idéal est un idéal.

**Exemple.** On reprend un exemple vu plus haut : soit  $\alpha = 2^{1/3}$  l'unique solution réelle à l'équation  $x^3 = 2$ . On note  $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \dots + a_r\alpha^r : a_i \in \mathbb{Q}, r \in \mathbb{N}\}$ . L'application d'évaluation

$$\text{eval}_\alpha : \mathbb{Q}[X] \rightarrow \mathbb{Q}[\alpha], \quad f(X) \mapsto f(\alpha),$$

est un morphisme d'anneaux. Son noyau est un idéal de  $\mathbb{Q}[X]$  ; c'est l'ensemble des polynômes à coefficients rationnels qui s'annulent en  $\alpha$  :

$$\ker(\text{eval}_\alpha) = \{P \in \mathbb{Q}[X] : P(\alpha) = 0\}.$$

**Définition et proposition 5.3 (Idéal engendré)**

Soit  $\Lambda$  un ensemble d'indices et  $(I_\lambda)_{\lambda \in \Lambda}$  une famille d'idéaux de  $A$ , alors l'intersection  $\bigcap_{\lambda \in \Lambda} I_\lambda$  est encore un idéal de  $A$ .

Soit  $S$  une partie de  $A$  ; l'idéal engendré par  $S$  est l'intersection des idéaux de  $A$  contenant  $S$ . Au sens de l'inclusion, c'est le plus petit idéal de  $A$  contenant  $S$ . On note en général  $\langle S \rangle$  (ou bien  $(x_1, \dots, x_s)$  lorsque  $S = \{x_1, \dots, x_s\}$  est fini) l'idéal engendré par  $S$  et on peut décrire ses éléments :

$$\langle S \rangle = \left\{ \sum_{\text{finie}} a_i x_i : a_i \in A, x_i \in S \right\}.$$

Dans le cas où  $S = \{x\}$  pour un  $x \in A$ , l'idéal  $\langle S \rangle$  est alors noté  $(x)$  ou  $Ax$ . Il est appelé idéal principal engendré par  $x$ . On a

$$(x) = \{ax : a \in A\}.$$

On accorde une attention particulière aux idéaux principaux; il sont notamment au cœur du chapitre suivant. Notons déjà que si  $u \in A^\times$ , alors  $(u) = A$ . En particulier  $A$  est un idéal principal de  $A$  engendré par 1. Donnons tout de suite une première utilisation des idéaux principaux  $(0)$  et  $(1) = A$ .

#### Proposition 5.4

Un anneau commutatif  $A$  est un corps si et seulement si il contient exactement deux idéaux distincts :  $(0)$  et  $(1) = A$ .

**Preuve.** Supposons que  $A$  est un corps et soit  $I$  un idéal de  $A$  alors, si  $I \neq (0)$ , il existe dans  $I$  un  $x \neq 0$ . C'est un élément de  $A^\times$  et donc  $A = (x) \subseteq I$ .

Réciproquement si  $(0)$  et  $(1)$  sont les seuls idéaux de  $A$  (et s'ils sont distincts), alors fixons  $x \in A \setminus \{0\}$ . Bien sûr  $(x) \neq (0)$ , et donc  $(x) = (1)$ . Ainsi  $1 \in (x)$  i.e. il existe  $y \in A$  tel que  $xy = 1$ . On a montré que  $x$  est inversible.  $\square$

Outre l'intersection d'idéaux, utilisée dans la notion d'idéal engendré, on définit la somme et le produit d'idéaux.

#### Définition et proposition 5.5

Soit  $I, J$  des idéaux de  $A$ .

- 1) L'ensemble  $I + J := \{a + b : a \in I, b \in J\}$ , somme des idéaux  $I$  et  $J$  est encore un idéal de  $A$ . C'est l'idéal de  $A$  engendré par  $I \cup J$  (une telle réunion n'est pas un idéal en général).
- 2) L'idéal engendré par  $\{xy : x \in I, y \in J\}$  est noté  $IJ$ ; il est appelé idéal produit de  $I$  et  $J$ .

**Remarques.** On a toujours  $IJ \subseteq I \cap J$ . Dans le cas  $A = \mathbb{Z}$  la somme d'idéaux  $a\mathbb{Z} + b\mathbb{Z}$  (resp. l'intersection  $a\mathbb{Z} \cap b\mathbb{Z}$ ) est l'idéal  $d\mathbb{Z}$  où  $d = \text{pgcd}(a, b)$  (resp.  $m\mathbb{Z}$  où  $m = \text{ppcm}(a, b)$ ).

Notons enfin que si  $a, b \in A$  alors l'idéal produit  $(a)(b)$  est l'idéal engendré par  $ab$ .

#### Théorème 5.6

Soit  $A$  un anneau euclidien. Si  $I$  est un idéal de  $A$  alors il existe  $a \in A$  tel que  $I = (a)$  (l'ensemble des multiples de  $a$  aussi parfois noté  $aA$ ).

**Preuve.** Soit  $I$  un idéal de  $A$  différent de  $\{0\} = (0)$  qui est évidemment principal. On choisit  $b \in I \setminus \{0\}$  tel que  $\phi(b) = \min\{\phi(x) \mid x \in I \setminus \{0\}\}$ .

Soit maintenant  $a \in I$  arbitraire, on a alors  $a = bq + r$  avec  $q, r \in A$  et  $\phi(r) < \phi(b)$  ou  $r = 0$ . Cependant, comme  $I$  est un idéal,  $r = a - bq \in I$  et par conséquent, par minimalité de  $\phi(b)$ , on a  $r = 0$ , ce qui montre que  $I = (b)$ .  $\square$

**Exercice.** Montrer que l'anneau  $\mathbb{Z}[X]$  n'est pas euclidien.

**Application.** On reprend l'exemple vu précédemment :

Soient  $\alpha = 2^{1/3}$ ,  $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \dots + a_r\alpha^r : a_i \in \mathbb{Q}, r \in \mathbb{N}\}$  et

$$\text{eval}_\alpha : \mathbb{Q}[X] \rightarrow \mathbb{Q}[\alpha], \quad f(X) \mapsto f(\alpha).$$

On a vu que  $\ker \text{eval}_\alpha = \{P \in \mathbb{Q}[X] : P(\alpha) = 0\}$  et qu'il contient  $X^3 - 2$ . Comme  $\mathbb{Q}[X]$  est euclidien, il existe  $P_0 \in \mathbb{Q}[X]$  non constant tel que  $\ker(\text{eval}_\alpha) = (P_0)$ . Ainsi  $P_0 \mid X^3 - 2$  dans  $\mathbb{Q}[X]$ . Montrons que  $\deg(P_0) = 3$ .

Si  $\deg P_0 < 3$ , alors il existe  $R$  non constant dans  $\mathbb{Q}[X]$  tel que  $X^3 - 2 = P_0 R$  et donc  $X^3 - 2$  admet un facteur de degré 1 dans  $\mathbb{Q}[X]$  et donc une racine rationnelle. Or l'unique racine réelle  $\alpha$  de  $X^3 - 2$  est  $\alpha$  qui est irrationnelle (exercice : le démontrer en utilisant le lemme de Gauss). Donc  $\deg P_0 = 3 = \deg(X^3 - 2)$ .

Comme  $P_0 \mid (X^3 - 2)$ , c'est qu'il existe  $a \in \mathbb{Q}^\times$  tel que  $P_0 = a(X^3 - 2)$  et donc (exercice)  $P_0$  et  $X^3 - 2$  engendrent le même idéal et donc  $\ker \text{eval}_\alpha = (X^3 - 2)$ .

## 6 Anneaux quotients

Dans cette section  $A$  désigne un anneau **commutatif** (pour éviter cette restriction il faudrait travailler avec des idéaux « bilatères » ie des idéaux à gauche et à droite).

### 6.1 Structure quotient et théorème de factorisation

Soit  $I$  un idéal de  $A$ . La relation binaire  $\mathcal{R}_I$  sur  $A$  :

$$x \mathcal{R}_I y \text{ si } x - y \in I$$

est une relation d'équivalence. C'est en effet une conséquence du fait que  $I$  est un sous-groupe additif de  $A$ . On note  $A/I$  l'ensemble des classes d'équivalence pour la relation  $\mathcal{R}_I$ . Un élément de  $A/I$  (qu'on appelle *classe de  $A$  modulo  $I$* ) est une partie de  $A$  de la forme

$$x + I := \{x + b : b \in I\}.$$

Comme dans le cas des groupes, on a une application surjective évidente (que l'on appelle encore *surjection canonique*)

$$\pi : A \rightarrow A/I, \quad x \mapsto x + I.$$

On a alors le résultat fondamental suivant.

**Proposition 6.1**

Avec les notations comme ci-dessus, les lois “+” et “.” définies sur  $A/I$ , pour  $x, y \in A$ , par

$$(x + I) + (y + I) := (x + y) + I, \quad (x + I) \cdot (y + I) := (x \cdot y) + I$$

confèrent à  $A/I$  une structure d’anneau commutatif appelé anneau quotient de  $A$  par  $I$ . Le neutre pour l’addition est la classe triviale  $I = 0 + I$  et le neutre pour la multiplication est la classe  $1 + I$  de l’élément  $1 \in A$ .

Pour cette structure, la surjection canonique  $\pi: A \rightarrow A/I$  est un morphisme d’anneaux.

**Preuve.** Il faut vérifier l’indépendance de la définition des lois “+” et “.” relativement à un choix de représentants. Si  $x \mathcal{R}_I x'$  et  $y \mathcal{R}_I y'$ , alors il existe  $z_x, z_y \in I$  tels que  $x' = x + z_x$  et  $y' = y + z_y$ . Ainsi  $x' + y' = x + y + z_x + z_y$ , et comme  $I$  est un groupe additif, on a bien  $x' + y' \in (x + y) + I$ . Aussi  $x'y' = xy + xz_y + yz_x + z_xz_y$ . Or  $I$  est un idéal donc les éléments  $xz_y, yz_x, z_xz_y$  ainsi que leur somme sont dans  $I$ . On déduit  $x'y' \in xy + I$ .

On laisse en exercice la vérification du fait que ces deux lois confèrent bien une structure d’anneau à  $A/I$ .  $\square$

**Exercice.** Dans les notations de la proposition, vérifier que  $1 + I = 1_{A/I}$ .

**Exemple:** • Tout anneau  $\mathbb{Z}/n\mathbb{Z}$  est un anneau quotient de l’anneau  $\mathbb{Z}$  par l’idéal  $n\mathbb{Z}$ . On décrit l’ensemble des idéaux d’un anneau quotient  $A/I$ .

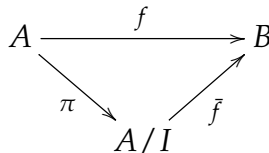
**Proposition 6.2**

Si  $I$  est un idéal de  $A$  et  $\pi$  est la surjection canonique associée, alors l’ensemble des idéaux de  $A/I$  est en bijection avec l’ensemble des idéaux de  $A$  qui contiennent  $I$  via l’application  $J \mapsto \pi^{-1}(J)$ .

L’analogie du théorème de factorisation 7.2 du chapitre 2 existe pour les anneaux. C’est le résultat suivant.

**Théorème 6.3**

Soit  $f: A \rightarrow B$  un morphisme d’anneaux commutatifs. Soit  $I$  un idéal de  $A$  tel que  $I \subset \ker f$ . Alors il existe un unique morphisme d’anneaux  $\bar{f}: A/I \rightarrow B$  tel que  $f = \bar{f} \circ \pi$ , où  $\pi$  désigne la projection canonique de  $A$  sur  $A/I$ .



En particulier si  $I = \ker f$ , le morphisme d’anneaux  $f$  induit un isomorphisme d’anneaux  $A/\ker f \rightarrow \text{Im } f$  :

$$\begin{array}{ccc}
 A & \xrightarrow{f} & B \\
 \pi \downarrow & & \uparrow i \\
 A / \ker f & \xrightarrow{\sim \bar{f}} & \operatorname{Im} f
 \end{array}$$

Les exemples suivants donnent des illustrations importantes du théorème de factorisation pour les anneaux.

**Exemples.**

1. (*Caractéristique d'un anneau*) Soit  $A$  un anneau commutatif dont on note  $1_A$  le neutre pour la multiplication. On considère le morphisme d'anneaux :

$$\varphi: \mathbb{Z} \rightarrow A, \quad n \geq 1 \mapsto 1_A + \cdots + 1_A,$$

où  $1_A$  apparaît  $n$  fois dans la somme (et donc  $\varphi(0) = 0_A, \varphi(-n) = -\varphi(n)$ ). Le noyau de  $\varphi$  est un idéal de  $\mathbb{Z}$ , il est donc de la forme  $d\mathbb{Z}$  pour un  $d \in \mathbb{N}$ . L'entier  $d$  s'appelle la *caractéristique* de l'anneau  $A$ . Le théorème de factorisation affirme que  $\varphi$  induit un isomorphisme d'anneaux :

$$\mathbb{Z}/d\mathbb{Z} \simeq \operatorname{Im}\varphi \subseteq A.$$

On déduit que la caractéristique d'un anneau intègre (et en particulier la caractéristique d'un corps) vaut soit 0, soit un nombre premier. [Exercice : quelle est la caractéristique de  $\mathbb{R}$ , de  $\mathbb{Z}/n\mathbb{Z}$ , de  $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$  ?]

2. On reprend l'exemple déjà considéré à trois reprises. Soient  $\alpha = 2^{1/3}, \mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_r\alpha^r : a_i \in \mathbb{Q}, r \in \mathbb{N}\}$  et

$$\operatorname{eval}_\alpha: \mathbb{Q}[X] \rightarrow \mathbb{Q}[\alpha], \quad f(X) \mapsto f(\alpha).$$

L'application  $\operatorname{eval}_\alpha$ , qui est évidemment surjective, induit donc un isomorphisme d'anneaux :

$$(\mathbb{Q}[X] / \ker(\operatorname{eval}_\alpha)) \simeq \mathbb{Q}[\alpha].$$

On a vu que  $\ker \operatorname{eval}_\alpha = (X^3 - 2)$  et donc  $(\mathbb{Q}[X] / (X^3 - 2)) \simeq \mathbb{Q}[\alpha]$ .

On se souvient que  $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 : a_i \in \mathbb{Q}\}$  (car  $\alpha^{3k+r} = 2^k\alpha^r$ ). Il semble que les éléments de  $\mathbb{Q}[\alpha]$ , et donc de  $\mathbb{Q}[X] / (X^3 - 2)$ , sont en bijection avec l'ensemble des polynômes rationnels de degré inférieur ou égal à 2. Si on les interprète comme étant les restes par la division dans  $\mathbb{Q}[X]$  par  $X^3 - 2$  cela rappelle beaucoup la situation dans  $\mathbb{Z}/n\mathbb{Z}$ .

**Proposition 6.4**

Si  $A$  est un anneau euclidien de stathme  $\phi$  et  $I = (a)$  un idéal non nul de  $A$ , alors  $A/I = \{x + I \mid x \in A \text{ et } (x = 0 \text{ ou } \phi(x) < \phi(a))\}$ .

Si  $A = K[X]$ , avec  $K$  un corps, alors  $A/I$  est en bijection avec  $\{P \in K[X] \mid \deg P < \deg a\}$ .



**Preuve.** Soit  $y \in A$ . Comme  $\phi$  est le stathme de  $A$  et que  $a \neq 0$  il existe  $q$  et  $x$  dans  $A$  tels  $y = aq + x$  avec  $x = 0$  ou  $\phi(x) < \phi(a)$ . Comme  $aq \in (a)$ , on a  $y \in x + (a)$ . Le deuxième point vient du fait que lorsque  $A = \mathbb{Z}$  ou  $K[X]$ , le couple  $(q, x)$  ci-dessus est unique.  $\square$

**Exemple:** Soit  $P$  un polynôme de degré 2 à coefficient dans  $\mathbb{F}_2$ . L'anneau  $\mathbb{F}_2[X]/(P)$  a donc 4 éléments. Cela fait potentiellement 4 nouveaux anneaux à 4 éléments (on connaît déjà  $\mathbb{Z}/4\mathbb{Z}$  et  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ). Prenons  $P = X^2 + X + 1$ , et notons  $\beta$  la classe de  $X$  modulo  $P$ . On peut facilement former les tables d'addition et de multiplication de l'anneau quotient. En effet  $\mathbb{F}_2[X]/(P) = \{0, 1, \beta, 1 + \beta\}$ ,  $1 + 1 = \beta + \beta = 0$  et  $\beta^2 = 1 + \beta$ , d'où

+	0	1	$\beta$	$1 + \beta$
0	0	1	$\beta$	$1 + \beta$
1	1	0	$1 + \beta$	$\beta$
$\beta$	$\beta$	$1 + \beta$	0	1
$1 + \beta$	$1 + \beta$	$\beta$	1	0

et

$\times$	0	1	$\beta$	$1 + \beta$
0	0	0	0	0
1	0	1	$\beta$	$1 + \beta$
$\beta$	0	$\beta$	$1 + \beta$	1
$1 + \beta$	0	$1 + \beta$	1	$\beta$

On peut voir qu'il s'agit d'un corps, cet anneau n'est donc ni isomorphe à  $\mathbb{Z}/4\mathbb{Z}$  ni à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

**Exercice** Former les tables des anneaux  $\mathbb{F}_2[X]/(X^2)$ ,  $\mathbb{F}_2[X]/(X^2 + 1)$  et  $\mathbb{F}_2[X]/(X^2 + X)$ . Lesquels de ces anneaux sont isomorphes entre eux? sont intègres? des corps?

## 6.2 Idéaux premiers, maximaux

Pour les anneaux commutatifs généraux, on a vu les notions d'intégrité et de corps. Puisque l'on sait maintenant construire des anneaux quotients  $A/I$  d'un anneau commutatif  $A$  par un idéal  $I$ , on se demande à quelle condition sur  $I$ , l'anneau  $A/I$  est intègre (resp. est un corps). La notion d'idéal premier (resp. d'idéal maximal) répond à cette question, comme on va le voir.

### Définition 6.5 (Idéal premier, idéal maximal)

Soit  $A$  un anneau commutatif et  $I$  un idéal de  $A$ , distinct de  $A$ .

1) On dit que  $I$  est un idéal premier de  $A$  si pour  $a, b \in A$  on a l'implication :

$$ab \in I \Rightarrow (a \in I \text{ ou } b \in I).$$

2) On dit que  $I$  est un idéal maximal de  $A$  si pour tout idéal  $J$  de  $A$  on a l'implication :

$$I \subseteq J \subseteq A \Rightarrow (J = I \text{ ou } J = A).$$

**Exemples.** L'idéal  $6\mathbb{Z}$  n'est pas premier dans  $\mathbb{Z}$ ; en revanche l'idéal  $5\mathbb{Z}$  est premier (et même maximal, ce qui est plus fort comme le montre la proposition suivante). Plus généralement les idéaux premiers non nuls de  $\mathbb{Z}$  coïncident avec les idéaux maximaux de  $\mathbb{Z}$  : ce sont les  $p\mathbb{Z}$ , pour  $p$  premier. On note que  $(0)$  est un idéal premier non maximal de  $\mathbb{Z}$  (car  $\mathbb{Z}/(0) \simeq \mathbb{Z}$  est intègre, mais ce n'est pas un corps). L'idéal  $I = (X)$  est premier dans  $A = \mathbb{Z}[X]$  mais il n'est pas maximal car on a par exemple la chaîne d'inclusions strictes  $I \subset (2, X) \subset A$ .

**Proposition 6.6**

Soit  $A$  un anneau commutatif et  $I$  un idéal de  $A$ . On a les équivalences :

- 1)  $A/I$  est intègre si et seulement si  $I$  est premier.
- 2)  $A/I$  est un corps si et seulement si  $I$  est maximal.

On déduit immédiatement le fait que tout idéal maximal est premier.

**Preuve.** (1) Soit  $\bar{a}, \bar{b}$  des éléments de  $A/I$ . On a

$$\bar{a} \cdot \bar{b} = \bar{0} \Leftrightarrow \overline{ab} = \bar{0} \Leftrightarrow ab \in I.$$

L'équivalence annoncée s'en déduit immédiatement.

(2) Si  $A/I$  est un corps alors d'après la proposition 5.4,  $A/I$  ne contient que deux idéaux,  $(\bar{0})$  et  $(\bar{1})$ . Soit  $I \subset J \subset A$  un idéal de  $A$ . Alors  $\pi(J) = J/I$  est un idéal de  $A/I$  et donc  $\pi(J) = (\bar{0})$  ce qui est équivalent à  $J = I$ , ou  $\pi(J) = (\bar{1}) = A/I$  ce qui est équivalent à  $J = A$ .

Réciproquement, si  $I$  est maximal, soit  $\bar{x} \in A/I$ ,  $\bar{x} \neq \bar{0}$ . On a alors  $(\bar{x}) = (\bar{1})$ . En effet,  $\pi^{-1}((\bar{x}))$  est un idéal de  $A$  qui contient  $I$  et qui est différent de  $I$ . On a donc  $\pi^{-1}((\bar{x})) = A$  par maximalité de  $I$  et  $(\bar{x}) = \pi(\pi^{-1}((\bar{x}))) = A/I$ . Enfin,  $(\bar{x}) = (\bar{1})$  est équivalent à  $\bar{x}$  inversible. □

**Exemples:**

- On a vu que  $\mathbb{F}_2[X]/(X^2 + X + 1)$  est un corps donc  $(X^2 + X + 1)$  est maximal (et premier).
- L'idéal  $(X^2)$  de  $\mathbb{F}_2[X]$  n'est ni maximal, il est contenu dans  $(X)$ , ni premier  $X \notin (X^2)$  mais  $X \cdot X \in (X^2)$ . Par conséquent  $\mathbb{F}_2[X]/(X^2)$  n'est pas un corps et n'est pas intègre.
- Le morphisme  $\text{eval}_i : \mathbb{R}[X] \rightarrow \mathbb{C}, P \mapsto P(i)$  est surjectif et a pour noyau l'idéal  $(X^2 + 1)$ . Par conséquent  $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$  qui est un corps et donc  $(X^2 + 1)$  est maximal.

# Chapitre 5

## Actions de groupes

Dans ce chapitre, on généralise la notion d'action d'un groupe sur un ensemble telle qu'entrevue au chapitre précédent avec l'action de  $S_n$  sur  $\{1, \dots, n\}$ , ainsi que divers concepts qui s'y rapportent, comme celui d'orbite.

### 1 Définition et exemples

#### Définition 1.1

Soit  $X$  un ensemble et  $G$  un groupe (noté multiplicativement et de neutre noté  $e$ ). Une action de  $G$  sur  $X$  est la donnée d'une application :

$$G \times X \rightarrow X, \quad (g, x) \mapsto g \cdot x$$

vérifiant

(a)  $\forall g, h \in G, \forall x \in X, g \cdot (h \cdot x) = (gh) \cdot x,$

(b)  $\forall x \in X, e \cdot x = x.$

**Exemples.** 1. La définition du groupe  $S_n$  des permutations de  $\{1, \dots, n\}$  induit une action évidente de  $S_n$  sur  $X = \{1, \dots, n\}$ .

2. Le groupe  $GL_n(\mathbb{R})$  agit (par multiplication à gauche) sur les vecteurs colonnes de taille  $n$  à coefficients réels.

3. Tout groupe  $G$  agit sur l'ensemble de ses sous-groupes par conjugaison : étant donné  $g \in G$  et  $H$  un sous-groupe de  $G$ , le conjugué  $gHg^{-1}$  de  $H$  est encore un sous-groupe de  $G$ .

4. Étant donné un groupe  $G$  quelconque et un sous-groupe  $H$  de  $G$  fixé, le groupe  $G$  agit sur l'ensemble quotient  $G/H$  (classes à gauche de  $G$  modulo  $H$ ) via  $(g, aH) \mapsto (ga)H$ .

Donnons une caractérisation très utile de la notion d'action de groupes en termes

de morphismes. Si  $X$  est un ensemble quelconque, on note  $\text{Sym}(X)$  le groupe des bijections  $f: X \rightarrow X$  muni de la composition des applications.

**Proposition 1.2**

*Avec les mêmes notations que dans la définition, la donnée d'une action de  $G$  sur  $X$  est équivalente à la donnée d'un morphisme de groupes  $\rho: G \rightarrow \text{Sym}(X)$ .*

**Preuve.** Il s'agit d'une simple réécriture des axiomes (a) et (b) définissant ce qu'est une action. En effet à partir de la donnée d'une action de  $G$  sur  $X$ , on peut définir une application :

$$\rho: G \rightarrow \text{Sym}(X), \quad g \mapsto (x \mapsto g \cdot x).$$

Remarquons que  $G$  est bien à valeurs dans  $\text{Sym}(X)$  car les axiomes (a) et (b) impliquent que  $(x \mapsto g \cdot x)$  est bijective, de bijection réciproque  $(x \mapsto g^{-1} \cdot x)$ . L'axiome (a) de la définition implique que  $\rho$  est un morphisme de groupes. Réciproquement étant donné un morphisme  $\rho: G \rightarrow \text{Sym}(X)$ , on a une action de  $G$  sur  $X$  définie pour  $g \in G$  et  $x \in X$  par :

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

Le fait que  $\rho$  est un morphisme implique que (a) et (b) de la définition sont satisfaits.  $\square$

## 2 Orbite et stabilisateur

On fixe un groupe  $G$  (noté multiplicativement) et un ensemble  $X$  sur lequel  $G$  agit.

**Définition 2.1**

*Étant donné  $x \in X$ , on appelle orbite de  $x$  sous l'action de  $G$  l'ensemble :*

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

*Il s'agit d'un sous-ensemble de  $X$ .*

*On appelle stabilisateur de  $x$  le sous-groupe de  $G$  :*

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

**Exercice.** Soit  $G$  un groupe agissant sur un ensemble  $X$ . Montrer que si  $x, y \in X$  sont dans la même orbite alors leurs stabilisateurs sont conjugués. Que dire de l'assertion réciproque ?

**Remarque** Si  $G$  agit sur  $X$  alors  $\bigcap_{x \in X} \text{Stab}(x)$  est le noyau du morphisme  $\rho: G \rightarrow \text{Sym}(X)$  associé à l'action.

Ainsi le noyau du morphisme correspondant à l'action par multiplication à gauche de  $G$  sur ses classes gauche  $G/H$  modulo un sous-groupe  $H$  fixé est  $\bigcap_{a \in G} aHa^{-1}$ .

**Proposition 2.2**

Si un groupe  $G$  agit sur un ensemble  $X$  alors  $X$  est réunion disjointe des orbites pour cette action.

**Preuve.** On procède comme pour la preuve de la proposition 2.3 du chapitre 3. La relation sur  $X$  définie par  $x\mathcal{R}y$  ssi  $y \in \text{Orb}(x)$  est une relation d'équivalence. En effet, elle est réflexive car  $x = e \cdot x$  et elle est symétrique car  $y = g \cdot x$  ssi  $x = g^{-1} \cdot y$ . Enfin, elle est transitive car si  $y = g \cdot x$  et  $z = g' \cdot y$  alors  $z = (g'g) \cdot x$ . Les classes d'équivalence pour  $\mathcal{R}$  sont donc les orbites de l'action et le résultat se déduit immédiatement de la proposition 0.4 du chapitre 2.  $\square$

**Remarque.** Si  $G = S_n$  est le groupe symétrique et si l'on se donne  $\sigma \in S_n$  et  $i \in \{1, \dots, n\}$  alors la partie  $\text{Orb}_\sigma(i)$  de  $\{1, \dots, n\}$  définie dans le chapitre 3 est l'orbite de  $i$  sous l'action du sous-groupe  $\langle \sigma \rangle$  de  $S_n$ .

**Définition 2.3**

S'il n'y a qu'une seule orbite dans l'action d'un groupe  $G$  sur un ensemble  $X$ , on dit que l'action est transitive.

**Exemples:** • Si  $H$  est un sous-groupe de  $G$ , l'action de  $G$  sur  $G/H$  par translation à gauche est transitive.

• On note par exemple que  $S_n$  (et aussi  $A_n$  si  $n \geq 3$ ) agit transitivement sur  $\{1, \dots, n\}$ . On note également que, dans le cas général, si  $G$  agit sur  $X$ , alors l'action induite sur chaque orbite est transitive.

Le résultat suivant énonce une propriété fondamentale des actions de groupes.

**Théorème 2.4 (Relation orbite-stabilisateur et équation des classes)**

Soit  $G$  un groupe agissant sur un ensemble  $X$  alors pour tout  $x \in X$  l'application

$$\varphi_x: G/\text{Stab}(x) \rightarrow \text{Orb}(x), \quad g\text{Stab}(x) \mapsto g \cdot x$$

est une bijection. En particulier si  $G$  est fini, on a la relation orbite-stabilisateur :

$$|\text{Orb}(x)| \times |\text{Stab}(x)| = |G|,$$

c'est-à-dire l'indice de  $\text{Stab}(x)$  dans  $G$  est  $|\text{Orb}(x)|$ .

Enfin, si  $G$  et  $X$  sont finis, on déduit l'égalité suivante (équation des classes) :

$$|X| = \sum_{i=1}^r \frac{|G|}{|\text{Stab}(x_i)|},$$

où les orbites dans l'action de  $G$  sur  $X$  sont  $\text{Orb}(x_1), \dots, \text{Orb}(x_r)$ .

**Preuve.** Montrons déjà que  $\varphi_x$  est bien définie. Si  $g\text{Stab}(x) = h\text{Stab}(x)$  alors il existe  $s \in \text{Stab}(x)$  tel que  $g = hs$ . On a alors  $g \cdot x = (hs) \cdot x$ . Cette dernière quantité vaut  $h \cdot (s \cdot x) = h \cdot x$  car  $s$  stabilise  $x$ . Donc  $\varphi_x(g\text{Stab}(x)) = \varphi_x(h\text{Stab}(x))$ .

La surjectivité de  $\varphi_x$  est évidente. Quant à l'injectivité, l'égalité  $g \cdot x = h \cdot x$  implique  $(h^{-1}g) \cdot x = x$  i.e.  $h^{-1}g \in \text{Stab}(x)$ . Donc  $g\text{Stab}(x) = h\text{Stab}(x)$ .

L'assertion concernant l'indice de  $\text{Stab}(x)$  dans  $G$  se déduit alors du théorème de Lagrange puisque

$$\frac{|G|}{|\text{Stab}(x)|} = |G/\text{Stab}(x)| = |\text{Orb}(x)|.$$

Quant à l'équation des classes, elle provient de la relation orbite-stabilisateur combinée avec la proposition 2.2.  $\square$

**Remarque.** Dans le cas où  $G$  est infini, la relation orbite-stabilisateur prend la forme suivante : pour tout  $x \in X$ ,  $\text{Orb}(x)$  ou  $\text{Stab}(x)$  est infini.

**Exemple.** Soit  $G$  un groupe. On considère son action sur lui-même par conjugaison (cf la définition 3.1 du chapitre précédent) : étant donné  $g, x \in G$ , on définit

$$g \cdot x = gxg^{-1}.$$

Pour cette action, l'orbite de  $x \in G$  est sa classe de conjugaison. On remarque que  $\text{Orb}(x) = \{x\}$  si et seulement si  $x$  commute avec tous les éléments de  $G$ . Cette propriété donne lieu à la définition suivante.

**Définition 2.5 (Centre d'un groupe)**

Soit  $G$  un groupe (noté multiplicativement). Le centre de  $G$  est l'ensemble de tous les éléments  $x \in G$  tels que

$$\forall g \in G, gxg^{-1} = x,$$

de manière équivalente c'est l'ensemble des  $x \in G$  dont la classe de conjugaison est réduite à  $\{x\}$ . Le centre de  $G$ , noté  $Z(G)$  est un sous-groupe abélien de  $G$ .

Pour conclure avec l'exemple, on écrit l'équation des classes pour l'action par conjugaison d'un groupe fini  $G$  sur lui-même :

$$|G| = |Z(G)| + \sum_{i=1}^k |\text{Cl}_{\text{conj}}(x_i)| = |Z(G)| + \sum_{i=1}^k \frac{|G|}{|\text{Stab}(x_i)|},$$

où  $\{x_1, \dots, x_k\}$  est un ensemble de représentants de chaque classe de conjugaison (notées  $\text{Cl}_{\text{conj}}$ ) de  $G$  ayant plus d'un éléments (si  $G$  est abélien, cette somme, alors vide, vaut 0).

On conclut ce chapitre avec un théorème donnant une réciproque partielle au théorème de Lagrange.

**Théorème 2.6 (Cauchy)**

Soit  $G$  un groupe fini d'ordre divisible par un nombre premier  $p$ . Alors il existe dans  $G$  un élément d'ordre  $p$ .

**Preuve.** Notons  $n = |G|$ . On a par hypothèse  $p \mid n$ . On considère

$$X = \{(g_1, \dots, g_p) \in G^p : g_1 \cdots g_p = e\}.$$

On a  $|X| = n^{p-1}$  : en effet la donnée d'un élément de  $X$  est la donnée d'un  $(p-1)$ -uplet quelconque  $(g_1, \dots, g_{p-1})$  d'éléments de  $G$ . L'élément  $g_p$  correspondant est alors l'inverse du produit  $g_1 \cdots g_{p-1}$ .

Soit  $\sigma$  la permutation de  $X$  définie par

$$\sigma(g_1, \dots, g_p) = (g_2, \dots, g_p, g_1).$$

Il s'agit bien d'une permutation de  $X$ , comme on voit en conjugant les 2 membres de l'égalité  $g_1 \cdots g_p = e$  par  $g_1^{-1}$ . Il est par ailleurs facile d'explicitier la permutation réciproque de  $\sigma$ . On a bien sûr  $\sigma^p = \text{Id}$  de sorte que l'on a une action de  $\mathbb{Z}/p\mathbb{Z}$  sur  $X$  via le morphisme de groupes :

$$\mathbb{Z}/p\mathbb{Z} \rightarrow \text{Sym}(X), \quad \bar{r} \mapsto \sigma^r.$$

Le stabilisateur d'un élément quelconque de  $X$  est un sous-groupe de  $\mathbb{Z}/p\mathbb{Z}$ . Ce stabilisateur est donc soit  $\mathbb{Z}/p\mathbb{Z}$  tout entier, soit trivial. Si  $(g_1, \dots, g_p) \in X$  a pour stabilisateur  $\mathbb{Z}/p\mathbb{Z}$ , cela signifie que  $g_1 = g_2 = \dots = g_p$  et donc l'orbite de cet élément est réduite à lui-même. En particulier  $(e, \dots, e)$  est un tel élément. D'après la relation orbite-stabilisateur, les éléments de  $X$  dont le stabilisateur est trivial ont une orbite à  $p$  éléments. En notant  $s$  le nombre d'orbites ponctuelles et  $r$  le nombre d'orbites à  $p$  éléments on obtient

$$n^{p-1} = pr + s.$$

Comme  $p \mid n$ , on déduit  $p \mid s$ . Or on a vu que  $s \geq 1$  : ainsi  $s \geq p$  et il existe donc un élément de  $X$  distinct de  $(e, \dots, e)$  de stabilisateur trivial, i.e. il existe  $g \in G \setminus \{e\}$  tel que  $(g, \dots, g) \in X$ .  $\square$

L'idée de faire agir un groupe  $G$  sur un ensemble bien choisi pour mieux le comprendre a été poussée très loin (et continue à l'être actuellement). On l'illustre ici en démontrant en exercice le 1er théorème de Sylow, une généralisation du théorème de Cauchy.

Soit  $G$  un groupe fini d'ordre  $p^a m$  où  $p$  est premier et  $a, m \in \mathbb{N}$  sont tels que  $m \geq 1$  et  $p \nmid m$ . Un  $p$ -sous-groupe de Sylow de  $G$  est un sous-groupe de  $G$  d'ordre  $p^a$ .

Exercice. On souhaite montrer, en conservant les notations ci-dessus, que  $G$  admet toujours un  $p$ -sous-groupe de Sylow (on notera que l'on peut supposer  $a \geq 1$ , puisque le résultat est trivialement vrai dans le cas contraire).

- 1) Soit  $S$  l'ensemble des parties de  $G$  à  $p^a$  éléments. Montrer que  $G$  agit sur  $S$  par multiplication à gauche et que le cardinal de  $S$  est premier à  $p$ .
- 2) Montrer qu'il existe une orbite (notée  $S_1$ ) de  $G$  sur  $S$  de cardinal non divisible par  $p$ . Montrer que si  $X \in S_1$  alors l'ordre de son stabilisateur est divisible par  $p^a$ .

- 3) Fixons un  $X \in \mathcal{S}_1$ . Justifier que  $P := \text{Stab}(X)$  agit sur  $X$  par multiplication à gauche et que l'orbite d'un élément quelconque  $x \in X$  dans cette action est de cardinal  $|P|$ .
- 4) Dédire  $p^a \geq |P|$ , puis conclure.



# Chapitre 6

## Sous-groupes distingués, groupes quotients et théorème de factorisation

### 1 Sous-groupes distingués et groupes quotients

On a vu comment définir dans un groupe  $G$  l'ensemble des classes à gauche  $G/H$  (resp. à droite  $H\backslash G$ ) modulo un sous-groupe  $H$  et qu'il existait une application naturelle  $\pi: G \rightarrow G/H, g \mapsto gH$  appelée la *surjection canonique* (et son analogue  $\pi': G \rightarrow H\backslash G$ .)

Deux questions naturelles, et apparemment indépendantes, se posent :

- 1) À quelle condition a-t-on coïncidence entre "classes à gauche" et "classes à droite"?
- 2) À quelle condition peut-on munir l'ensemble quotient  $G/H$  (ou  $H\backslash G$ ) d'une structure de groupe « naturelle »?

Les deux questions admettent la même réponse, qui repose sur la notion de sous-groupe *distingué* (ou *normal*).

On a déjà vu que supposer  $G$  abélien permettait de répondre à ces questions. Dans ce cas, c'était grâce à la propriété fondamentale suivante :

$$\begin{cases} x' \equiv x \pmod{H} \\ y' \equiv y \pmod{H} \end{cases} \Rightarrow x' + y' \equiv x + y \pmod{H}$$

Pour imiter cette démarche dans le cas général, on a envie, pour définir une loi de groupe sur  $G/H$ , de poser  $xHyH := xyH$  de sorte que  $G \rightarrow G/H$  soit un morphisme. Mais cette définition est-elle bien indépendante d'un choix de représentants ? Non en général.

Précisément, à quelle(s) condition(s) a-t-on, pour tout  $x, x', y, y' \in G$  :

$$\begin{cases} x'H = xH \\ y'H = yH \end{cases} \Rightarrow x'y'H = xyH ?$$

### Définition et proposition 1.1

On dit que  $H$  est distingué ou normal dans  $G$  si l'une des 4 assertions équivalentes suivantes est satisfaite

$$1) \forall y \in G, \forall h \in H, y^{-1}hy \in H$$

$$2) \forall y \in G, y^{-1}Hy \subset H$$

$$3) \forall y \in G, y^{-1}Hy = H$$

$$4) \forall y \in G, Hy = yH$$

Notation :  $H \triangleleft G$ .

**Preuve.** Il est évident que 1)  $\Rightarrow$  2) et 3)  $\Rightarrow$  4)  $\Rightarrow$  1).

Quant à 2)  $\Rightarrow$  3), il suffit de remplacer  $y$  par  $y^{-1}$  dans 2) pour obtenir  $yHy^{-1} \subset H$  i.e.  $H \subset y^{-1}Hy$ .  $\square$

Clairement, cette propriété apporte une réponse à la première question posée en préambule de cette section : si  $H \triangleleft G$ , alors les classes à droite et à gauche de tout élément de  $G$  coïncident, c'est-à-dire que les relations d'équivalence  $\mathcal{R}$  et  $\mathcal{R}'$  du chapitre 2 sont égales. En particulier les ensembles de classes d'équivalence correspondants  $G/H$  et  $H \backslash G$  sont les mêmes.

Si l'on revient au problème de munir  $G/H$  d'une structure de groupe (telle que  $\pi: G \rightarrow G/H$  soit un morphisme de groupes), on voit que si  $H$  est distingué dans  $G$  alors en supposant

- $x'H = xH$ , c'est-à-dire s'il existe  $h \in H$  tel que  $x' = xh$ ,
- $y'H = yH$ , c'est-à-dire s'il existe  $k \in H$  tel que  $y' = yk$ ,

on déduit

$$x'y' = xhyk = xy(y^{-1}hy)k \in xyH \text{ et donc } x'y'H = xyH.$$

On obtient donc une loi de composition interne bien définie sur  $G/H$  en posant

$$\forall x \in G, \forall y \in G, xHyH := xyH$$

Il reste à voir que la loi ainsi définie est bien une loi de groupe :

- elle est associative car la loi de  $G$  est associative,
- elle possède un élément neutre, à savoir la classe de  $e$ ,  $eH = H$ , puisque  $eHxH = exH = xH = xeH = xHeH$  pour tout  $x \in G$ . En résumé,  $e_{G/H} = H$ ,
- tout élément de  $G/H$  admet un inverse : pour tout  $x \in G$  on a  $(xH)(x^{-1}H) = (x^{-1}H)(xH) = (xx^{-1})H = H = e_{G/H}$ , autrement dit,  $(xH)^{-1} = x^{-1}H$ .

En résumé, la propriété pour  $H$  d'être distingué dans  $G$  est donc une condition *suffisante* pour que  $G/H$  admette une structure de groupe compatible avec la loi de groupe de  $G$  (i.e telle que la surjection canonique  $\pi: G \rightarrow G/H$  soit un morphisme de groupes).

### Définition 1.2

Si  $H$  est un sous-groupe distingué de  $G$ , on appelle groupe quotient de  $G$  par  $H$  l'ensemble des classes à gauche  $G/H$  muni de la loi de groupe :

$$(xH) \cdot (yH) := (xyH), \quad (x, y \in G).$$

On montre facilement que cette condition est également nécessaire. En effet, pour pouvoir munir  $G/H$  d'une loi de groupe compatible avec celle de  $G$ , il faut en particulier que pour tout  $x \in G$ , et tout  $h \in H$ , on ait  $\pi(hx) = \pi(h)\pi(x) = \pi(e)\pi(x) = e_{G/H}\pi(x) = \pi(x)$  c'est-à-dire  $hx = xk$  avec  $k \in H$  ou encore  $x^{-1}hx \in H$ .

On résume tout cela dans l'énoncé suivant :

### Théorème 1.3

Soit  $G$  un groupe et  $H$  un sous-groupe de  $G$ .

- Si  $H \triangleleft G$ , il existe sur  $G/H$  une unique structure de groupe telle que la surjection canonique  $\pi: G \rightarrow G/H$  soit un morphisme. Elle est définie par  $xH \cdot yH = xyH$ .
- Réciproquement si  $G/H$  admet une structure de groupe telle que la surjection canonique  $\pi: G \rightarrow G/H$  est un morphisme de groupes, alors  $H \triangleleft G$ .

### Exemples :

- $\{e\}$  et  $G$  sont distingués dans  $G$ .
- Si  $G$  est abélien, tous ses sous-groupes sont distingués.
- Dans  $S_3$ , le sous-groupe engendré par  $(123)$  est distingué. En revanche, le sous-groupe engendré par  $(12)$  ne l'est pas.
- Si  $f: G \rightarrow K$  est un morphisme de groupes alors  $\ker f \triangleleft G$ . Si  $x \in \ker f$  et  $g \in G$  alors  $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)(f(g))^{-1} = e$  donc  $gxg^{-1} \in \ker f$ .

### Proposition 1.4 (Un sous-groupe d'indice 2 est toujours distingué)

Si  $G$  est un groupe et  $H$  est un sous-groupe de  $G$  tel que  $(G : H) = 2$  alors  $H \triangleleft G$ .

**Preuve.** Par hypothèse il y a deux classes à gauche de  $G$  modulo  $H$  : la classe triviale  $H$  et une classe s'écrivant  $aH$  pour un  $a \notin H$ . Comme  $a \notin H$  on a également exactement deux classes à droite :  $H$  et  $Ha$ . Par disjonction des classes (à droite ou à gauche) distinctes, on déduit  $aH = Ha$ . Prenons maintenant un  $x \in G$  quelconque.

Soit  $x \in H$  et alors  $xH = Hx = H$  car  $H$  est un sous-groupe. Sinon  $x \in aH = Ha$  et donc  $xH = Hx$ . Dans tous les cas on a montré  $xH = Hx$ .  $\square$

Application : le groupe alterné  $A_n$ , d'ordre  $n!/2$ , est distingué dans le groupe symétrique  $S_n$  d'ordre  $n!$ .

**Remarque.** Si  $G$  est fini on a plus généralement : si  $H$  est un sous-groupe de  $G$  d'indice  $p$ , le plus petit diviseur premier de  $|G|$ , alors  $H \triangleleft G$ . (Cf TD.)

### Proposition 1.5

Si  $H \triangleleft G$  et  $\pi$  est la surjection canonique associée, alors l'ensemble des sous-groupes de  $G$  qui contiennent  $H$  est en bijection avec l'ensemble des sous-groupes de  $G/H$  via l'application  $K \mapsto \pi(K)$ , l'application réciproque étant donnée par  $K' \mapsto \pi^{-1}(K')$ .

**Preuve.** Comme  $\pi$  est un morphisme de groupes, on a : si  $K$  est un sous-groupe de  $G$  alors  $\pi(K)$  est un sous-groupe de  $G/H$  et si  $K'$  est un sous-groupe de  $G/H$  alors  $\pi^{-1}(K')$  est un sous-groupe de  $G$ .

Ensuite, on a toujours  $\pi(\pi^{-1}(K')) = K'$  et d'autre part,  $\pi^{-1}(\pi(K)) = KH = \{kh \mid k \in K, h \in H\}$  puisque  $\pi(x) = \pi(y)$  ssi il existe  $h \in H$  tel que  $y = xh$ . Mais si  $H \subset K$ ,  $KH = K$ .  $\square$

### Proposition 1.6

Soit  $g$  un groupe et  $H, K$  deux sous-groupes de  $G$ . Si  $H$  est distingué dans  $G$  alors  $HK := \{xy \mid x \in H \text{ et } y \in G\}$  est un sous-groupe de  $G$ .

## 2 Sous-groupes distingués et morphismes

### 2.1 Le théorème de factorisation

La preuve de la proposition suivante est immédiate.

#### Proposition 2.1

Soit  $\varphi : G \rightarrow H$  un morphisme de groupes. Si  $K \triangleleft H$  est un sous-groupe distingué de  $H$  alors  $\varphi^{-1}(K) \triangleleft G$  est un sous-groupe distingué de  $G$ . En particulier, le noyau de  $\varphi$  est un sous-groupe distingué de  $G$ .

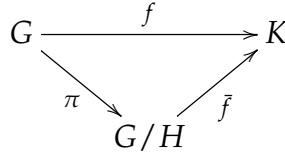
Si  $L \triangleleft G$  est un sous-groupe distingué de  $G$  alors  $\varphi(L) \triangleleft \text{Im } \varphi$  est un sous-groupe distingué de  $\text{Im } \varphi$ . En particulier, si  $\varphi$  est surjectif, on a  $\varphi(L) \triangleleft H$ .

En particulier on retrouve le fait que  $A_n \triangleleft S_n$ . Aussi, en considérant le morphisme "déterminant"  $GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$ , on déduit que  $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ .

On en déduit aussi que dans la proposition 1.5, l'ensemble des sous-groupes distingués de  $G$  qui contiennent  $H$  est en bijection avec l'ensemble des sous-groupes distingués de  $G/H$  par la même application.

**Théorème 2.2**

Soit  $f : G \rightarrow K$  un morphisme de groupes et  $H$  un sous-groupe normal de  $G$ . On suppose  $H \subset \ker f$ . Alors il existe un unique morphisme de groupes  $\bar{f} : G/H \rightarrow K$  tel que  $f = \bar{f} \circ \pi$ , où  $\pi$  désigne la projection canonique de  $G$  sur  $G/H$ .



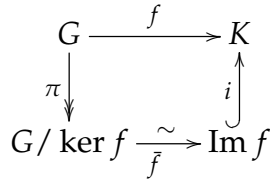
En particulier,  $f$  induit un isomorphisme  $G/\ker f \rightarrow \text{Im } f$ .

**Preuve.** Nécessairement, on doit définir  $\bar{f}$  par  $\bar{f}(xH) = f(x)$ . Comme  $H \subset \ker f$ ,  $\bar{f}$  est bien définie puisque pour tout  $h \in H$ ,  $f(xh) = f(x)f(h) = f(x)e_K = f(x)$ . On voit facilement que  $\bar{f}$  est un morphisme de groupes puisque

$$\bar{f}(xHyH) = \bar{f}(xyH) = f(xy) = f(x)f(y) = \bar{f}(xH)\bar{f}(yH).$$

On a évidemment  $\text{Im } \bar{f} = \text{Im } f$ .

En outre, si  $H = \ker f$ , on a  $\bar{f}(xH) = e_K \Leftrightarrow f(x) = e_K \Leftrightarrow x \in \ker f \Leftrightarrow xH = H$  i.e.  $\bar{f}$  est injective. Donc dans ce cas,  $\bar{f}$  est un isomorphisme de  $G/\ker f$  sur  $\text{Im } f$ .



□

**Exemple :**

- Via le morphisme de signature  $\varepsilon$ , on a  $S_n/A_n \simeq \{\pm 1\}$  pour  $n \geq 2$ , et via le morphisme "déterminant" on a  $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^\times$ .

**Corollaire 2.3**

Soient  $G$  un groupe,  $H$  un sous-groupe distingué de  $G$  et  $K$  un sous-groupe de  $G$ . Alors  $K \cap H$  est un sous-groupe distingué de  $K$  et  $K/K \cap H$  est isomorphe à  $HK/H$ .

**Preuve.** Si  $x \in K \cap H$  et  $k \in K$  alors  $kxk^{-1} \in H$  car  $k \in G$  et  $H \triangleleft G$  et  $kxk^{-1} \in K$  car  $x$  et  $k$  sont dans  $K$ . Ce qui montre  $K \cap H \triangleleft K$ .

D'après la proposition 1.6,  $HK$  est un groupe et il est clair que  $H \triangleleft HK$  et que  $K$  est un sous-groupe de  $HK$ . Soit  $\pi : HK \rightarrow HK/H$  la surjection canonique. Il est clair que  $\pi(K) = HK/K$  et que le noyau de la restriction de  $\pi$  à  $K$  est  $H \cap K$ . Le théorème de factorisation appliqué à  $\pi|_K$  nous dit que  $K/H \cap K \simeq HK/K$ . □

**Corollaire 2.4 (les quotients de mes quotients sont mes quotients)**

Soient  $G$  un groupe et  $K, H$  deux sous-groupes distingués de  $G$  avec  $K \subset H$ . Alors  $(G/K)/(H/K)$  est isomorphe à  $G/H$ .

**Preuve.** Remarquons que d'une part,  $K$  étant distingué dans  $G$ , il est a fortiori distingué dans  $H$  et d'autre part, d'après la proposition 2.1,  $H/K$  est un sous-groupe distingué de  $G/K$ . Le morphisme  $G/K \rightarrow G/H, gK \mapsto gH$  est évidemment surjectif, et son noyau est  $H/K$ , d'où le résultat par le théorème 2.2.  $\square$

# Chapitre 7

## Anneaux principaux

### 1 Divisibilité

Soit  $A$  un anneau, que l'on supposera, dans toute la suite de ce chapitre, *commutatif*. On peut généraliser dans  $A$  la notion de divisibilité de  $\mathbb{Z}$ .

#### Définition 1.1

Soit  $a, b \in A, b \neq 0$ . On dit que  $b$  divise  $a$  (ou que  $b$  est un diviseur de  $a$ , ou encore que  $a$  est multiple de  $b$ ) s'il existe  $c \in A$  tel que  $a = bc$ .

Si l'on suppose de plus que  $A$  est intègre, on dit que des éléments  $a$  et  $b$  de  $A \setminus \{0\}$  sont associés s'ils se divisent l'un l'autre i.e.  $b \mid a$  et  $a \mid b$ . Cette propriété équivaut à l'existence d'une unité  $u \in A^\times$  telle que  $a = ub$ .

Pour démontrer l'assertion contenue dans la définition écrivons  $a = bc$  et  $b = ad$ . On déduit  $a = adc$  puis  $a(1 - dc) = 0$ . Comme  $a \neq 0$  par hypothèse et que  $A$  est intègre, on déduit  $cd = 1$  et donc  $u = c$  est l'unité cherchée.

**Exemple.** Dans  $\mathbb{Q}[X]$  on a  $(2X + 2) \mid (X^2 + X)$ , en revanche cette divisibilité n'a pas lieu dans  $\mathbb{Z}[X]$ .

#### Définition et proposition 1.2 (Idéal principal, anneau principal)

Un idéal  $I$  de  $A$  est dit principal s'il existe  $a \in A$  tel que  $I = (a)$ . L'idéal  $(a)$  est l'ensemble des multiples de  $a$  dans  $A$ . On le note parfois  $Aa$ .

On dit que l'anneau  $A$  est principal s'il est intègre et si tous ses idéaux sont principaux.

**Remarque.** Si  $A$  est intègre, 2 éléments de  $A$  sont associés si et seulement si ils engendrent le même idéal principal. En particulier le générateur d'un idéal principal est toujours déterminé à multiplication par une unité près.

La proposition suivante est évidente.

**Proposition 1.3**

Soit  $a, b \in A$ . On a l'équivalence  $b \mid a \Leftrightarrow (a) \subseteq (b)$ .

Donnons deux exemples fondamentaux d'anneaux principaux.

**Théorème 1.4**

- L'anneau  $\mathbb{Z}$  est principal.
- Soit  $K$  un corps. L'anneau  $K[X]$  des polynômes en une indéterminée à coefficients dans  $K$  est principal.

Pour  $\mathbb{Z}$ , nous avons déjà vu au chapitre précédent que ses idéaux sont exactement les  $d\mathbb{Z}$ ,  $d \geq 0$  qui sont donc tous principaux. Ce théorème est en fait une conséquence du fait que  $\mathbb{Z}$  et  $K[X]$  sont des anneaux ayant une propriété plus remarquable encore que la principalité : ce sont des anneaux *euclidiens* (voir le théorème 5.6 de la section ??).

## 2 Arithmétique dans les anneaux principaux : PGCD, PPCM, éléments premiers entre eux

Dans toute cette section  $A$  désigne un anneau intègre (donc commutatif). La notion de divisibilité dans les anneaux (§1) permet d'étendre au cas des anneaux principaux les notions de pgcd et de ppcm.

**Définition 2.1**

Soient  $a$  et  $b$  deux éléments (non nuls) d'un anneau  $A$  principal (en particulier commutatif et intègre).

- 1) On appelle PGCD de  $a$  et  $b$  tout élément  $d$  de  $A$  tel que  $(d) = (a) + (b)$ .
- 2) On appelle PPCM de  $a$  et  $b$  tout élément  $m$  de  $A$  tel que  $(m) = (a) \cap (b)$ .

On dit que  $a$  et  $b$  sont premiers entre eux s'ils admettent 1 pour PGCD, en d'autres termes si  $(a) + (b) = A$ .

**Remarques.**

- 1) Ces définitions sont compatibles avec les définitions classiques de PGCD et PPCM dans  $\mathbb{Z}$  (voir le théorème ?? du chapitre ??).
- 2) Deux PGCDs (resp. PPCMs) d'un même couple d'éléments sont associés (c'est-à-dire se déduisent l'un de l'autre par multiplication par un inversible de  $A$ ; voir la remarque précédant la proposition 1.3).



- 3) On peut définir plus généralement un PGCD (resp. un PPCM) d'une famille d'éléments  $(a_1, \dots, a_n)$  comme étant un générateur de l'idéal  $(a_1) + \dots + (a_n)$  (resp.  $(a_1) \cap \dots \cap (a_n)$ )

**Proposition 2.2 (Bézout, Gauss)**

Soient  $a, b$  et  $c$  des éléments d'un anneau principal  $A$ .

- 1) (Bézout)  $a$  et  $b$  de  $A$  sont premiers entre eux si et seulement s'il existe  $u$  et  $v$  éléments de  $A$  tels que  $au + bv = 1$ .
- 2) (Gauss) Si  $a$  et  $b$  sont premiers entre eux et si  $a$  divise  $bc$ , alors  $a$  divise  $c$ .
- 3) (Gauss 2) Si  $a$  et  $b$  sont premiers entre eux et divisent tous les deux  $c$ , alors  $ab$  divise  $c$
- 4) Si  $a$  est premier avec  $b$  et avec  $c$ , alors  $a$  est premier avec  $bc$ .

**Preuve.**

- 1) Par définition,  $a$  et  $b$  sont premiers entre eux si et seulement si  $1 \in (a) + (b)$
- 2) Si  $au + bv = 1$ , alors  $acu + bcv = c$ . Or, si  $a$  divise  $bc$ , il divise le membre de gauche, et donc celui de droite.
- 3) Si  $a \mid c$  alors  $ab \mid bc$  et de même, si  $b \mid c$  alors  $ab \mid ac$ . Mais par ailleurs, si  $au + bv = 1$ ,  $acu + bcv = c$ . On vient de voir que  $ab$  divise le membre de gauche, donc aussi celui de droite.
- 4) Il existe  $(u, v)$  et  $(u', v')$  tels que  $au + bv = 1$  et  $au' + cv' = 1$  et en multipliant ces deux égalités,  $a(auu' + cuv' + bvu') + bc(vv') = 1$  d'où le résultat par le théorème de Bézout.

□

**Proposition 2.3**

Si  $a$  et  $b$  sont deux éléments d'un anneau principal  $A$ , et si  $d$  et  $m$  désignent respectivement un PGCD et un PPCM de  $a$  et  $b$ , alors :

- 1) Pour tout  $x \in A$ , on a :  $x$  divise  $a$  et  $b \Leftrightarrow x$  divise  $d$ .
- 2) Pour tout  $y \in A$ , on a :  $a$  et  $b$  divisent  $y \Leftrightarrow m$  divise  $y$ .
- 3)  $(ab) = (dm)$ .

**Preuve.** On utilise la proposition 1.3.

- 1) Si  $(a) \subset (x)$  et  $(b) \subset (x)$ , alors  $(a) + (b) \subset (x)$  i.e.  $(d) \subset (x)$ . Réciproquement, si  $(d) \subset (x)$ , comme  $(a) \subset (d)$  et  $(b) \subset (d)$ , on a  $(a) \subset (x)$  et  $(b) \subset (x)$ .
- 2) On raisonne de façon similaire.
- 3) On écrit  $a = da'$  et  $b = db'$  et on a  $(a') + (b') = A$  (en effet, il existe  $u, v \in A$  tels que  $au + bv = d$ , donc  $a'u + b'v = 1$ ). On a alors  $da'b' = ab' = a'b$ , donc  $da'b'$  est un multiple commun de  $a$  et de  $b$  donc de  $m$ , ou autrement dit

$$(m) \supset (da'b').$$

Inversement, en écrivant

$$\begin{aligned} m &= xa = xda' \\ &= yb = ydb' \end{aligned}$$

on obtient que  $xa' = yb'$ , d'où l'on conclut (Gauss) que  $a'$  divise  $y$  (et  $b'$  divise  $x$ ). Il suit que  $da'b'$  divise  $m$ , c'est-à-dire  $(m) \subset (da'b')$ .

□

### 3 Décomposition en produit d'irréductibles

#### Définition 3.1

Un élément  $x \neq 0$  d'un anneau  $A$  commutatif et intègre est dit irréductible s'il n'est ni inversible, ni produit de deux éléments non inversibles. Autrement dit,  $x$  est irréductible s'il n'est pas inversible et si

$$\forall (a, b) \in A \times A, x = ab \Rightarrow (a \in A^\times \text{ ou } b \in A^\times).$$

**Exemple :** Dans  $\mathbb{Z}$ , un élément irréductible est, au signe près, un nombre premier.

Le résultat suivant est bien connu dans  $\mathbb{Z}$  ou  $K[X]$  :

#### Lemme 3.2

Deux éléments irréductibles  $p_1$  et  $p_2$  d'un anneau intègre  $A$  sont soit premiers entre eux, soit associés.

**Preuve.** On a  $(p_1) + (p_2) = (d)$ . Comme  $d$  divise en particulier  $p_1$  qui est irréductible, soit  $d$  est inversible et dans ce cas  $(d) = A$ , soit  $d$  est associé à  $p_1$  mais alors, comme  $d$  divise aussi  $p_2$ , cela signifie que  $p_1$  divise  $p_2$  donc que  $p_1$  et  $p_2$  sont associés. □

**Lemme 3.3**

Dans un anneau principal, toute suite croissante d'idéaux est stationnaire. Autrement dit, il n'existe pas de suite infinie d'idéaux strictement croissante.

**Preuve.** Soit  $I_0 \subset I_1 \subset I_2 \subset \dots$  une suite croissante d'idéaux. Alors  $I := \bigcup_{n \in \mathbb{N}} I_n$  est un idéal de  $A$  (attention : ce serait en général faux si la suite n'était pas croissante). Il existe donc  $x \in I$  tel que  $I = (x)$ . Mais alors, il existe  $k \in \mathbb{N}$  tel que  $x \in I_k$ , auquel cas  $I_k \subset I = Ax \subset I_k$ , donc  $I_k = I$  et  $I_\ell = I_k$  pour tout  $\ell \geq k$ .  $\square$

**Proposition 3.4**

Soit  $a$  un élément non nul d'un anneau principal  $A$ . Alors

- 1) Si  $a$  est non inversible, alors il admet un diviseur irréductible.
- 2) Pour tout élément irréductible  $p$ , l'ensemble  $\{k \in \mathbb{N} \mid p^k \text{ divise } a\}$  est majoré.
- 3) L'ensemble des éléments irréductibles deux à deux non associés qui divisent  $a$  est fini.

**Preuve.**

- 1) Si  $a$  est irréductible, c'est clair. Sinon,  $a = a_1 b_1$  avec  $a_1$  et  $b_1$  non inversibles. Si  $a_1$  est irréductible, on obtient bien un diviseur irréductible de  $a$ . Sinon,  $a_1 = a_2 b_2$  avec  $a_2$  et  $b_2$  non inversibles, etc. Si le processus ne s'arrêtait jamais, on construirait ainsi une suite d'éléments  $a_0 = a, a_1, a_2, \dots$  tels que  $a_i$  divise strictement  $a_{i-1}$  pour tout  $i \geq 1$ . La suite des idéaux  $(a_i)$  serait donc strictement croissante, ce qui est impossible en vertu du lemme 3.3. Donc le processus s'arrête, et le dernier terme  $a_k$  construit est irréductible.
- 2) Supposons, par l'absurde, que  $a$  soit divisible par  $p^k$  pour tout  $k \in \mathbb{N}$ . Il existe alors, pour tout  $k \in \mathbb{N}$ , un élément  $a_k$  de  $A$  tel que  $a = p^k a_k$  et la suite  $(a_k)$  est strictement croissante, ce qui est impossible.
- 3) Si l'ensemble des diviseurs irréductibles de  $a$  deux à deux non associés est infini, on construit par récurrence une suite infinie  $(p_n)_{n \in \mathbb{N}}$  d'irréductibles deux à deux non associés et une suite strictement croissante d'idéaux de la façon suivante :

$$a = p_1 a_1 = p_1 p_2 a_2 = p_1 p_2 p_3 a_3 = \dots$$

(on utilise le lemme 3.2 et Gauss à chaque étape) et on a alors  $(a_1) \subsetneq (a_2) \subsetneq \dots$

$\square$

Pour conclure cette section on déduit de la proposition précédente l'énoncé d'une généralisation du théorème fondamental de l'arithmétique affirmant que tout entier  $n \geq 2$  est, de manière unique, produit de nombres premiers.

**Définition 3.5**

À tout élément irréductible  $p$  d'un anneau principal  $A$  est associée une application  $v_p : A \setminus \{0\} \rightarrow \mathbb{N}$  définie par

$$v_p(a) = \max \{k \in \mathbb{N} \mid p^k \text{ divise } a\}.$$

Le fait que  $v_p$  est bien définie est une conséquence de la proposition 3.4 2).

**Théorème 3.6**

Soit  $a$  un élément non nul et non inversible d'un anneau principal  $A$ . On note  $\mathbb{P}(a)$  un ensemble de représentants pour ses diviseurs irréductibles à association près. Alors il existe  $u \in A^\times$  et des entiers strictement positifs  $v_p(a)$  tels que

$$a = u \prod_{p \in \mathbb{P}(a)} p^{v_p(a)}.$$

Cette factorisation est unique à une unité près et au choix de représentants dans  $\mathbb{P}(a)$  près.

**Remarque.** Un anneau intègre dans lequel tout élément non nul admet une factorisation unique en produit d'irréductibles (comme dans le théorème) est dit factoriel.

**Preuve.** D'après la proposition 3.4 3),  $\mathbb{P}(a)$  est fini. Par définition,  $a$  est divisible par chacun des  $p^{v_p(a)}$  pour  $p \in \mathbb{P}(a)$  et comme ils sont deux à deux premiers entre eux, par le théorème de Gauss 2,  $a$  est divisible par  $\prod_{p \in \mathbb{P}(a)} p^{v_p(a)}$ . Le quotient de  $a$  par ce produit n'admet pas de diviseur irréductible car un tel diviseur  $p$  serait aussi un diviseur irréductible de  $a$  et on aurait une contradiction avec soit la définition de  $v_p(a)$ , soit celle de  $\mathbb{P}(a)$ . Par conséquent, d'après la proposition 3.4 1) ce quotient est inversible.

En ce qui concerne l'unicité, remarquons tout d'abord que si  $p$  est irréductible et divise un produit  $bc$ , alors  $p \mid b$  ou  $p \mid c$ . En effet, si  $p \nmid b$ ,  $\text{PGCD}(p, b) = 1$  car  $p$  est irréductible et on conclut par Gauss.

Supposons que  $a = u \prod_{i=1}^n p_i = v \prod_{j=1}^m q_j$  où  $u, v \in A^\times$  et les  $p_i, q_j$  sont irréductibles (remarquons que la décomposition du théorème s'écrit ainsi, avec des répétitions éventuelles des facteurs  $p_i$ ). Puisque  $p_1$  qui est irréductible divise le membre de droite,  $p_1$  divise un des facteurs que l'on peut supposer être  $q_1$  après renumérotation. Ce dernier étant lui aussi irréductible, on a  $q_1 = v_1 p_1$  avec  $v_1 \in A^\times$  et on peut donc simplifier par  $p_1$  les deux membres et obtenir  $u \prod_{i=2}^n p_i = v v_1 \prod_{j=2}^m q_j$ . En poursuivant de même pour  $p_i, i = 2, \dots, n$ , on obtient l'unicité (en particulier,  $m = n$  et quitte à réordonner,  $q_i = v_i p_i, v_i \in A^\times$ , pour tout  $i$ ).  $\square$

**Proposition 3.7**

Soient  $A$  un anneau principal et  $I = (a)$  un idéal de  $A$ . Les trois propriétés suivantes sont équivalentes :

- 1)  $I$  est premier,
- 2)  $I$  est maximal,
- 3)  $a$  est irréductible.