

STRUCTURES ALGÈBRIQUES  
FONDAMENTALES

Faire de l'Algèbre, c'est essentiellement *calculer*, c'est-à-dire effectuer, sur des éléments d'un ensemble, des « opérations algébriques », dont l'exemple le plus connu est fourni par les « quatre règles » de l'arithmétique élémentaire.

La notion d'opération algébrique, d'abord restreinte aux entiers naturels et aux grandeurs mesurables, a peu à peu élargi son domaine, à mesure que se généralisait parallèlement la notion de « nombre », jusqu'à ce que, dépassant cette dernière, elle en vînt à s'appliquer à des éléments qui n'avaient plus aucun caractère « numérique ». C'est sans doute la possibilité de ces extensions successives, dans lesquelles la *forme* des calculs restait la même, alors que la *nature* des êtres mathématiques soumis à ces calculs variait considérablement, qui a permis de dégager peu à peu le principe directeur des mathématiques modernes, à savoir que les êtres mathématiques, en eux-mêmes, importent peu : ce qui compte, ce sont leurs relations.

On peut considérer Evariste Galois comme le véritable initiateur de la théorie des groupes. Les premières traces de ses travaux remontent à 1832 et ne furent publiées qu'après sa mort, en 1846. Il cherchait alors à prouver que les équations polynomiales de degré  $\geq 5$  à coefficients complexes ne pouvaient être résolues par radicaux. Pour ce faire, il s'intéressa à un groupe relié aux racines de l'équation considérée. Son génie consista à comprendre que les difficultés pour résoudre l'équation ne provenaient pas de son degré mais des propriétés de ce groupe.

Les mathématiciens ont compris depuis que les groupes interviennent dans de nombreux domaines. L'ensemble des isométries de l'espace ou du plan est un groupe appelé groupe orthogonal. L'ensemble des isométries préservant un objet donné a une structure de groupe. L'ensemble des transformations qui, en relativité restreinte, permettent de changer de référentiel galiléen tout en préservant les lois de la physique et la vitesse de la lumière forment un groupe appelé groupe de Lorentz. En chimie, les symétries des molécules permettent de leur associer des groupes qui aident à comprendre mieux leurs propriétés. Plus concrètement encore, l'ensemble des manipulations qu'on peut effectuer sur un Rubik's cube a lui

aussi une structure de groupe. L'étude de ce groupe permet de mettre en place des stratégies gagnantes pour le reconstituer.

## 14.1 LOI DE COMPOSITION

### §1 Loi de composition ; associativité ; commutativité

#### Définition 1

Soit  $E$  un ensemble. On appelle **loi de composition interne** sur  $E$  une application

$$\top : E \times E \rightarrow E.$$

La valeur  $\top(x, y)$  de  $\top$  pour un couple  $(x, y) \in E \times E$  s'appelle le **composé** de  $x$  et de  $y$  pour cette loi.

Le composé de  $x$  et de  $y$  se note le plus souvent en écrivant  $x$  et  $y$  dans un ordre déterminé et en les séparant par un signe caractéristique de la loi envisagée (signe qu'on pourra convenir d'omettre). L'écriture  $x\top y$  au lieu de  $\top(x, y)$  est traditionnelle et appelée **notation infixé**. Parmi les signes dont l'emploi est le plus fréquent, citons  $+$  et  $.$ , étant convenu en général que ce dernier peut s'omettre à volonté ; avec ces signes, le composé de  $x$  et  $y$  s'écrit respectivement  $x + y$ , et  $x.y$  ou  $xy$ . Une loi notée par le signe  $+$  s'appelle le plus souvent **addition** (le composé  $x + y$  s'appelant alors la **somme** de  $x$  et de  $y$ ) et on dit qu'elle est **notée additivement** ; une loi notée par le signe  $.$  s'appelle le plus souvent **multiplication** (le composé  $x.y = xy$  s'appelant alors **produit** de  $x$  et de  $y$ ), et on dit qu'elle est **notée multiplicativement**. Dans les raisonnements généraux des paragraphes 14.1 et 14.2 du présent chapitre, on se servira ordinairement des signes «étoile»  $\star$  et «truc»  $\top$  pour noter des lois de composition quelconques.

#### Exemples 2

1. Les applications  $(X, Y) \mapsto X \cup Y$  et  $(X, Y) \mapsto X \cap Y$  sont des lois de composition sur l'ensemble des parties d'un ensemble  $E$ .
2. Dans l'ensemble  $\mathbb{N}$  des entiers naturels, l'addition, la multiplication, l'exponentiation sont des lois de composition interne (les composés de  $x \in \mathbb{N}$  et  $y \in \mathbb{N}$  pour ces lois se notant respectivement  $x + y$ ,  $xy$  ou  $x.y$ , et  $x^y$ ).
3. La soustraction n'est pas une loi de composition interne sur  $\mathbb{N}$  puisque  $3 - 7$  n'existe pas. Mais c'est une loi de composition interne dans  $\mathbb{Z}$ .

#### Définition 3

Soit une loi de composition interne  $(x, y) \mapsto x \star y$  sur un ensemble  $E$ .

- On dit que  $\star$  est **associative** si

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

- On dit que deux éléments  $x$  et  $y$  **commutent** (ou sont **permutables**) si

$$y \star x = x \star y.$$

- On dit que  $\star$  est **commutative** si deux éléments quelconques de  $E$  commutent pour cette loi, c'est-à-dire si

$$\forall x, y \in E, y \star x = x \star y.$$

**Exemples 4**

1. La soustraction n'est pas associative dans  $\mathbb{Z}$  car  $7 - (3 - 1) \neq (7 - 3) - 1$ .
2. La composition des applications est une loi associative, mais en général non commutative dans l'ensemble  $\mathcal{F}(E, E)$ .

**Exemple 5**

Donner un exemple qui prouve que la composition des applications n'est pas commutative.

**Exemple 6**

Quelles sont les propriétés de la loi  $x \star y = \frac{x+y}{2}$  dans  $\mathbb{R}$  ?



**Convention** Nous conviendrons qu'une loi notée additivement est associative et commutative.

## §2 Élément neutre ; éléments inversibles

**Définition 7**

Soit une loi de composition interne  $(x, y) \mapsto x \star y$  sur un ensemble  $E$ . Un élément  $e$  de  $E$  est dit **élément neutre** si

$$\forall x \in E, e \star x = x \star e = x.$$

Il existe au plus un élément neutre pour une loi donnée  $\star$ , car si  $e$  et  $e'$  sont éléments neutres, on a  $e = e \star e' = e'$ .

L'élément neutre, pour une loi notée additivement, se note souvent 0 (ou  $0_E$ ) et s'appelle **zéro** ou **élément nul** (ou parfois **origine**). Pour une loi notée multiplicativement, il se note souvent 1 (ou  $1_E$ ) et s'appelle **élément unité** (ou **unité**).

**Exemple 8**

L'application  $\text{Id}_E$  est l'élément neutre de la loi de composition  $\circ$  dans  $\mathcal{F}(E, E)$ .

**Exemple 9**

La loi  $x \star y = \frac{x+y}{2}$  dans  $\mathbb{R}$  possède-t-elle un élément neutre?

**Définition 10**

Soient une loi de composition interne  $(x, y) \mapsto x \star y$  sur un ensemble  $E$  possédant un élément neutre  $e$  et  $x$  et  $x'$  deux éléments de  $E$ .

- On dit que  $x'$  est **inverse** de  $x$  si l'on a  $x' \star x = x \star x' = e$ .
- On dit qu'un élément  $x$  de  $E$  est **inversible** s'il possède un inverse.

On dit parfois **symétrique** et **symétrisable** au lieu d'**inverse** et **inversible**. Lorsque la loi de  $E$  est notée additivement, on dit généralement **opposé** au lieu d'**inverse**.

Plus tard dans l'année, nous dirons que  $x'$  est **inverse à gauche** de  $x$  si l'on a  $x' \star x = e$ . De même, on dit que  $x'$  est **inverse à droite** de  $x$  si l'on a  $x \star x' = e$ .

**Proposition 11**

Soit  $E$  muni d'une loi de composition interne  $\star$ , associative et possédant un élément neutre  $e$ .

1. Lorsque qu'un élément  $x \in E$  est inversible, son inverse  $x'$  est unique.
2. Pour tous éléments  $x$  et  $y$  inversibles, d'inverse  $x'$  et  $y'$  respectivement. Alors  $x \star y$  est inversible et son inverse est  $y' \star x'$ .

**Définition 12**

Soit une loi de composition interne  $(x, y) \mapsto x \star y$  sur un ensemble  $E$ . On dit qu'un élément  $a \in E$  est **régulier** ou **simplifiable** pour la loi  $\star$  lorsque

$$\forall (x, y) \in E^2, (a \star x = a \star y \implies x = y) \text{ et } (x \star a = y \star a \implies x = y).$$

**Proposition 13**

Soit  $E$  muni d'une loi de composition interne  $\star$ , associative et possédant un élément neutre  $e$ . Tout élément inversible est simplifiable.

### §3 Loi associées à un même loi de composition interne

#### Loi interne sur $\mathcal{P}(E)$ déduite d'une loi interne définie sur $E$

Soit  $(x, y) \mapsto x \star y$  une loi de composition interne sur un ensemble  $E$ . Étant données deux parties quelconques  $X, Y$  de  $E$ , on désignera par  $X \star Y$  (pourvu que cette notation ne prête pas à confusion) l'ensemble des éléments  $x \star y$  de  $E$  tels que  $x \in X$  et  $y \in Y$  (autrement dit, l'image de  $X \times Y$  par l'application  $(x, y) \mapsto x \star y$ ).<sup>1</sup>

$$X \star Y = \{ x \star y \mid x \in X \text{ et } y \in Y \}$$

Si  $a \in E$ , on écrit généralement  $a \star Y$  au lieu de  $\{a\} \star Y$ , et  $X \star a$  au lieu de  $X \star \{a\}$ . L'application  $(X, Y) \mapsto X \star Y$  est une loi de composition interne sur  $\mathcal{P}(E)$ , l'ensemble des parties de  $E$ . Par exemple  $2\mathbb{N}$  désignera l'ensemble des entiers naturels pairs.

#### Partie stable ; loi induite


**Définition 14**

Une partie  $A$  d'un ensemble  $E$  est dite **stable** pour un loi de composition interne  $\star$  sur  $E$  si le composé de deux éléments de  $A$  appartient à  $A$  :

$$\forall x, y \in A, x \star y \in A.$$

L'application  $(x, y) \mapsto x \star y$  de  $A \times A$  dans  $A$  s'appelle alors la **loi induite** sur  $A$  par la loi  $\star$ .

Autrement dit, pour que  $A$  soit stable pour une loi  $\star$ , il faut et il suffit que  $A \star A \subset A$ .

<sup>1</sup>   $a \in X \star Y \iff \exists (x, y) \in X \times Y, a = x \star y$ .

### Loi interne définie sur $\mathcal{F}(X, E)$ déduite d'une loi interne sur $E$

$X$  étant un ensemble quelconque et  $E$  un ensemble muni d'une loi de composition interne  $\star$ , considérons deux applications  $f$  et  $g$  de  $X$  dans  $E$ , c'est-à-dire deux éléments de  $\mathcal{F}(X, E)$  ; on désignera par  $f \star g$  l'application définie par

$$\begin{aligned} f \star g : X &\rightarrow E \\ x &\mapsto f(x) \star g(x) \end{aligned} .$$

On dit que  $f \star g$  est définie ponctuellement. On voit que si  $\star$  est associative et commutative sur  $E$ , il en est de même sur  $\mathcal{F}(X, E)$ . Si  $\star$  possède un élément neutre  $e$ , la fonction constante prenant cette valeur  $e$  pour tout  $x$  de  $E$  est élément neutre pour la loi sur  $\mathcal{F}(X, E)$ .

#### Exemple 15

Soit  $X = E = \mathbb{R}$ , pour  $f, g, s, p \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ , on aura

$$\begin{aligned} s = f + g &\iff \forall x \in \mathbb{R}, s(x) = f(x) + g(x); \\ p = fg &\iff \forall x \in \mathbb{R}, p(x) = f(x)g(x). \end{aligned}$$

Les application  $s$  et  $p$  sont respectivement la somme et le produit des deux fonctions  $f$  et  $g$ .

## §4 Morphismes

Nous allons considérer simultanément deux ensembles munis de loi de composition interne, afin d'exprimer les liens possibles entre les « structures » ainsi définies. Nous noterons  $(E, \star)$  (lire  $E$  muni de la loi  $\star$ ) et  $(F, \top)$  ces deux structures.

#### Définition 16

Un **morphisme** de  $(E, \star)$  dans  $(F, \top)$  est une application  $f$  de  $E$  dans  $F$  telle que

$$\forall (x, y) \in E, f(x \star y) = f(x) \top f(y).$$

- Un morphisme bijectif est appelé **isomorphisme**.
- Un **endomorphisme** est un morphisme de  $(E, \star)$  dans lui-même (avec la même loi!).
- Un **automorphisme** est un isomorphisme de  $(E, \star)$  dans lui-même (avec la même loi!).

#### Remarque

Les vérifications (faciles) des faits suivants sont laissées en exercice.

1. Le composé de deux morphismes est un morphisme.
2. L'identité, le composé de deux isomorphismes, l'application réciproque d'un isomorphisme sont des isomorphismes.

#### Exemple 17

L'application  $A \mapsto \complement_E A$  de  $\mathcal{P}(E)$  dans lui-même est un isomorphisme de  $(\mathcal{P}(E), \cap)$  dans  $(\mathcal{P}(E), \cup)$  et également un isomorphisme de  $(\mathcal{P}(E), \cup)$  dans  $(\mathcal{P}(E), \cap)$  (loi de Morgan). Ce n'est cependant pas un automorphisme car la loi n'est pas la même au départ et à l'arrivée.

#### Définition 18

S'il existe un isomorphisme de  $(E, \star)$  dans  $(F, \top)$ , on dit que  $(E, \star)$  et  $(F, \top)$  sont **isomorphes**.

**Remarque**

Si  $(E, \star)$  et  $(F, \top)$  sont isomorphes, alors l'une de ces deux lois est associative (resp. commutative) si et seulement si l'autre l'est.

De même, les isomorphismes transforment neutres (à gauche ou à droite) en neutres (à gauche ou à droite), inverses (à gauche ou à droite) en inverse (à gauche ou à droite), simplifiables (à gauche ou à droite) en simplifiable (à gauche ou à droite), absorbants (à gauche ou à droite) en absorbant (à gauche ou à droite), idempotents en idempotents.

## 14.2 LA STRUCTURE DE GROUPE

### §1 Groupes

**Définition 19**

On appelle **groupe** un couple formé d'un ensemble  $G$  et d'une loi de composition interne  $\star$  sur l'ensemble  $G$  associative, possédant un élément neutre et pour laquelle tout élément est inversible. Autrement dit,

- $\forall x, y, z \in G, x \star (y \star z) = (x \star y) \star z.$
- $\exists e_G \in G, \forall x \in G, e_G \star x = x \star e_G = x.$
- $\forall x \in G, \exists x' \in G, x \star x' = x' \star x = e_G.$

Si de plus la loi  $\star$  est commutative, on dit que le groupe est **commutatif** ou **abélien**.

**Notation**

- Pour définir un groupe, il ne suffit pas de se donner un ensemble  $G$  ; il faut aussi se donner une loi de composition interne sur l'ensemble  $G$  vérifiant les conditions ci-dessus ; néanmoins, on désigne toujours un groupe par la même lettre,  $G$  par exemple, que l'ensemble qui en constitue l'une des données.<sup>a</sup>
- Si  $(G, \star)$  est un groupe, il existe un unique élément neutre pour  $\star$ . Lorsqu'on travaille avec plusieurs groupes, on note  $e_G$  l'élément neutre de  $G$ .
- Fréquemment, on appelle produit la loi de composition interne du groupe  $G$ . On note le produit comme une multiplication et donc sans aucun symbole. On écrit simplement  $xy$  au lieu de  $x \star y$ . On utilise alors l'écriture  $x^{-1}$  pour l'inverse de  $x$ .<sup>b</sup>
- Lorsqu'une loi de groupe sur  $G$  est noté  $+$ , l'inverse d'un élément  $x$  s'appelle l'opposé et est noté  $-x$ , et l'élément neutre est noté  $0_G$ . Pour  $x, y \in G$ , l'élément  $x + (-y)$  est noté plus simplement  $x - y$ .
- On peut noter la loi de composition d'un groupe avec à peu près n'importe quel symbole  $(+, \cdot, \times, \cup, \cap, \vee, \wedge, \top, \perp, *, \star, \circ, \oplus, \otimes, \odot, \dots)$ . Mais par habitude, on réserve le symbole  $+$  pour des lois commutatives. En revanche, beaucoup de lois commutatives ne sont pas notées  $+$ .

<sup>a</sup>On prendra soin de *ne pas* dire qu'un groupe «est un ensemble  $G$  sur lequel il existe une loi de composition interne vérifiant...» car on peut facilement démontrer que, sur tout ensemble, il existe une telle loi de composition interne, et même qu'on peut en construire une infinité pour peu que l'ensemble donné soit lui-même infini ; en disant qu'un groupe est «un ensemble sur lequel il existe» une loi de composition interne, on ne dit donc rien d'autre que ceci : «un groupe est un ensemble» — définition dont la stupidité est particulièrement claire...

<sup>b</sup>En général, on ne note pas  $\frac{1}{x}$  l'inverse de  $x$ . En effet, si le groupe n'est pas commutatif,  $\frac{x}{y}$  ne permet pas de distinguer  $x \star y^{-1}$  et  $y^{-1} \star x$ .

**Exemples 20**

1. (Groupes additifs)  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  sont des groupes. L'élément neutre est 0 et l'opposé de  $x$  est  $-x$ . En revanche,  $(\mathbb{N}, +)$  n'est pas un groupe car si  $n \in \mathbb{N}$  est strictement positif, il n'a pas d'inverse pour  $+$ .
2. (Groupes multiplicatifs)  $(\mathbb{Q}^*, \cdot)$ ,  $(\mathbb{R}^*, \cdot)$ ,  $(\mathbb{R}_+^*, \cdot)$ ,  $(\mathbb{C}^*, \cdot)$  sont des groupes commutatifs. L'élément neutre est 1 et l'inverse de  $x$  est  $\frac{1}{x}$ .
3. (Similitudes directe du plan) L'ensemble des similitudes directes du plan est un groupe (non commutatif) pour la composition  $\circ$ . En prenant l'écriture analytique complexe  $z \mapsto az + b$  avec  $a \in \mathbb{C}^*$  et  $b \in \mathbb{C}$ , l'élément neutre est l'identité  $z \mapsto z$  et l'inverse de  $z \mapsto az + b$  est  $z \mapsto \frac{1}{a}z - \frac{b}{a}$ .

Pour  $x \in G$ , on note  $x^0 = e_G$ ,  $x^1 = x$ ,  $x^2 = x \star x$ ,  $x^3 = x \star x \star x$ , etc. L'associativité de la loi  $\star$  permet de définir sans ambiguïté le produit de  $n$  termes  $x^n = x \star x \star \dots \star x$  avec  $n \in \mathbb{N}$ .

**Définition 21**

Soit  $(G, \star)$  un groupe, d'élément neutre  $e_G$  et  $x \in G$ . On définit les puissances entières  $x^n$  ( $n \in \mathbb{Z}$ ) de la manière suivante:

- On pose  $x^0 = e_G$ .
- Pour tout  $n \in \mathbb{N}^*$ , on pose  $x^n = x \star x^{n-1}$ , c'est-à-dire  $x^n = x \star x \star \dots \star x$  ( $n$  termes).
- Pour tout  $n \in \mathbb{N}^*$ , on pose  $x^{-n} = (x^{-1})^n$ , ou ce qui revient au même  $x^{-n} = (x^n)^{-1}$ .

L'élément  $x^n$  est donc bien un élément du groupe  $(G, \star)$ .

**Notation**

Lorsqu'une loi de groupe sur  $G$  est noté  $+$  ayant pour élément neutre  $0_G$ , on note à la place

- $0 \cdot x = 0_G$ ,
- Si  $n \in \mathbb{N}^*$ ,  $n \cdot x = x + x + \dots + x$  ( $n$  termes),
- et  $(-n)x = n \cdot (-x)$  si  $n$  est un entier négatif.

Signalons maintenant quelques-unes des principales propriétés d'un groupe.

**Proposition 22**

Soit  $(G, \cdot)$  un groupe. Alors

1.  $G$  est non-vide : il contient au moins son élément neutre.
2. L'élément neutre de  $G$  est unique.
3. Le symétrique de tout élément de  $G$  est unique.
4.  $\forall x \in G, (x^{-1})^{-1} = x$ .
5.  $\forall (x, y) \in G^2, (xy)^{-1} = y^{-1}x^{-1}$ .
6.  $\forall x \in G, \forall (n, m) \in \mathbb{Z}^2, x^{n+m} = x^n x^m$ .

⚠ En général  $(xy)^n \neq x^n y^n$ . Par exemple

$$(xy)^2 = xyxy \neq xxyy = x^2 y^2,$$

sauf si  $x$  et  $y$  commutent.

### Test 23

Écrire ces propriétés lorsque le groupe  $G$  est noté additivement.

### Proposition 24

Dans un groupe, tout élément est simplifiable. En effet, pour tout  $a \in G$ , on a

- $\forall (x, y) \in G^2, ax = ay \implies x = y.$
- $\forall (x, y) \in G^2, xa = ya \implies x = y.$

Quand on déduit l'égalité  $x = y$  de l'égalité  $ax = ay$ , on dit que l'on **simplifie à gauche** par  $a$  ; si on la déduit de  $xa = ya$ , on dit que l'on **simplifie à droite** par  $a$ . Si le groupe est commutatif, on se contente de dire que l'on **simplifie** par  $a$ .

## §2 Groupe produit

### Théorème 25

Soient deux groupes  $(E, \top)$  et  $(F, \perp)$ . On définit une loi  $\star$  sur  $E \times F$  par

$$(x, y) \star (x', y') = (x \top x', y \perp y').$$

1. La loi  $\star$  confère à  $E \times F$  une structure de groupe appelé **produit des groupes**  $(E, \top)$  et  $(F, \perp)$ .
2. Le produit de deux groupes commutatifs est un groupe commutatif.

## §3 Sous-groupes

### Définition 26

Soit  $(G, \star)$  un groupe. On appelle **sous-groupe** de  $G$  une partie  $H$  de  $G$  possédant les propriétés suivantes

1. L'élément neutre de  $G$  appartient à  $H$

$$e_G \in H;$$

2.  $H$  est stable pour  $\star$ , c'est-à-dire

$$\forall (x, y) \in H^2, x \star y \in H;$$

3.  $H$  est stable par passage à l'inverse, c'est-à-dire

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



**Proposition 27**

Soit  $(G, \star)$  un groupe et  $H$  une partie de  $G$ . Alors  $H$  est un sous-groupe de  $G$  si, et seulement si

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

**Remarque****Pour montrer que  $H$  est un sous-groupe**

Si  $(G, \star)$  est un groupe et  $H$  une partie de  $G$ , vérifier que  $H$  est un sous-groupe de  $G$  consiste à vérifier des propriétés d'appartenance. Il faut vérifier que l'élément neutre  $e$  appartient à  $H$ , pas que  $e \star x = x \star e = x$  pour tout  $x \in H$ . En effet cette dernière propriété est évidente, vu que  $G$  est un groupe et que tout élément de  $H$  appartient à  $G$ . De même, si  $x, y \in H$ , c'est  $x^{-1}$  appartient à  $H$  et  $x \star y$  appartient à  $H$  qu'il faut vérifier.

**Proposition 28**

Soient  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Alors  $(H, \star)$  est lui-même un groupe pour la loi de composition induite sur  $H$  par la loi de composition de  $G$ . Réciproquement, si  $H$  est une partie du groupe  $G$  telle que  $(H, \star)$  est un groupe, alors  $H$  est un sous-groupe de  $G$ .

Dans la pratique, pour montrer qu'un ensemble  $H$  est un groupe, il peut être plus facile de montrer que c'est un sous-groupe d'un groupe connu.

**Exemple 29**

L'ensemble des entiers pairs  $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$  est un sous-groupe de  $(\mathbb{Z}, +)$ . En effet, 0 est pair. Soient  $x, y \in 2\mathbb{Z}$ , il existe donc  $x', y' \in \mathbb{Z}$  tel que  $x = 2x'$  et  $y = 2y'$ . On a donc

$$x + y = 2(x' + y') \quad \text{et} \quad x' + y' \in \mathbb{Z},$$

c'est-à-dire,  $x + y \in 2\mathbb{Z}$ . De plus,

$$-x = 2(-x') \quad \text{et} \quad -x' \in \mathbb{Z},$$

c'est-à-dire,  $-x \in 2\mathbb{Z}$ .

**Exemples 30**

1. Si  $(G, \star)$  est un groupe d'élément neutre  $e$ , alors  $\{e\}$  est un sous-groupe de  $G$ . De même,  $G$  est un sous-groupe de  $G$ . Le sous-groupe  $\{e\}$  est appelé **sous-groupe trivial** de  $G$ .
2. Tout sous-groupe de  $G$ , distinct de  $\{e\}$  et  $G$  est appelé **sous-groupe propre** de  $G$ .
3. Chacun des groupe  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  est un sous-groupe de tous les suivants.
4. Chacun des groupe  $(\mathbb{Q}^*, \cdot)$ ,  $(\mathbb{R}^*, \cdot)$ ,  $(\mathbb{C}^*, \cdot)$  est un sous-groupe de tous les suivants.
5.  $\mathbb{R}_+^*$  est un sous-groupe de  $(\mathbb{R}^*, \cdot)$  mais n'est pas un sous-groupe de  $(\mathbb{R}, +)$ .
6. L'ensemble  $\mathbb{U}$  des nombres complexes de module un est un sous-groupe de  $\mathbb{C}^*$ . En effet, 1 est de module un ( $1 \in \mathbb{U}$ ), si  $z$  est de module un, alors  $1/z$  est de module un (car  $|1/z| = 1/|z|$ ), et si  $z, w$  sont de module un, alors  $zw$  aussi (car  $|zw| = |z| |w|$ ).
7. La géométrie élémentaire fournit de nombreux exemples de sous-groupes du groupe des permutations : le groupe des translations sur la droite, ou dans le plan, ou dans l'espace ; le groupe des rotations autour d'un point dans le plan ou dans l'espace ; le groupe des déplacements dans le plan, ou dans l'espace ; le groupe des homothéties de centre donné et de rapport *non nul* dans le plan ou dans l'espace, etc, etc,...

**Proposition 31**

Soient  $(G, \star)$  un groupe,  $H$  et  $K$  deux sous-groupe de  $G$ . Alors  $H \cap K$  est un sous-groupe de  $G$ .

Cette proposition se généralise à une intersection quelconque de sous-groupes d'un groupe  $G$ .

## §4 Morphismes de groupes

**Définition 32**

Soit  $(G, \star)$  et  $(H, \top)$  deux groupes. On appelle **morphisme de groupes** ou **homomorphisme de groupes** une application  $f : G \rightarrow H$  telle que

$$\forall (x, y) \in G^2, f(x \star y) = f(x) \top f(y).$$

- Lorsque l'application  $f$  est bijective, on dit que  $f$  est un **isomorphisme de groupes**. On dit que  $G$  et  $H$  sont **isomorphes** s'il existe un isomorphisme de  $G$  sur  $H$ .
- Lorsque  $G = H$ , on dit que  $f$  est un **endomorphisme** de  $G$ .
- Lorsque  $G = H$  et que  $f$  est bijectif, on dit que  $f$  est un **automorphisme** de  $G$ .

**Exemples 33**

1.  $(\mathbb{R}_+^*, \cdot) \rightarrow (\mathbb{R}, +)$  est un isomorphisme de groupes.  
 $x \mapsto \ln x$
2.  $(\mathbb{C}, +) \rightarrow (\mathbb{C}, +)$  est un automorphisme de groupes.  
 $z \mapsto \bar{z}$
3.  $(\mathbb{Z}, +) \rightarrow (\mathbb{R}_+^*, \cdot)$  est un morphisme de groupes non-surjectif.  
 $n \mapsto 5^n$
4.  $(\mathbb{Z}, +) \rightarrow (\{-1, 1\}, \cdot)$  est un morphisme de groupes non-injectif.  
 $n \mapsto (-1)^n$

**Proposition 34**

Soit  $f$  un morphisme du groupe  $G$  dans le groupe  $H$ . Alors

1.  $f(e_G) = e_H$ .
2.  $\forall x \in G, f(x^{-1}) = (f(x))^{-1}$ .
3.  $\forall x \in G, \forall n \in \mathbb{Z}, f(x^n) = (f(x))^n$ .

**Proposition 35**

1. La composée de deux morphismes de groupes est un morphisme de groupes.
2. Si un morphisme de groupes est bijectif, l'application réciproque est encore un morphisme de groupes.

**Théorème 36**

Soit  $f$  un morphisme du groupe  $G$  dans le groupe  $H$ .

1. Si  $G'$  est un sous-groupe de  $G$ , alors l'image

$$f(G') = \{ f(x) \mid x \in G' \} = \{ y \in H \mid \exists x \in G', y = f(x) \}$$

est un sous-groupe de  $H$ .

2. Si  $H'$  est un sous-groupe de  $H$ , alors l'image réciproque

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

est un sous-groupe de  $G$ .

## §5 Noyau et image d'un morphisme de groupes

**Définition 37**

Soit  $f$  un morphisme du groupe  $G$  dans le groupe  $H$ . L'image réciproque de l'élément neutre de  $H$  est appelé **noyau** de  $f$  et se note  $\ker(f)$ .

$$\ker(f) = \{ x \in G \mid f(x) = e_H \} = f^{-1}(\{ e_H \}).$$

L'image  $f(G)$  de  $f$  se note  $\text{Im}(f)$ .

$$\text{Im}(f) = \{ f(x) \mid x \in G \} = \{ y \in H \mid \exists x \in G, y = f(x) \}.$$



$$\begin{aligned} x \in \ker f &\iff x \in G \text{ et } f(x) = e_H. \\ y \in \text{Im}(f) &\iff \exists x \in G, y = f(x). \end{aligned}$$

**Proposition 38**

Soit  $f$  un morphisme du groupe  $G$  dans le groupe  $H$ .

1.  $\ker(f)$  est un sous-groupe de  $G$ .
2.  $\text{Im}(f)$  est un sous-groupe de  $H$ .

**Théorème 39**

Soient  $G$  et  $H$  deux groupes et  $f$  un morphisme de  $G$  dans  $H$ .

1.  $f$  est injectif si et seulement si  $\ker(f) = \{ e_G \}$ .
2.  $f$  est surjectif si et seulement si  $\text{Im}(f) = H$ .

**Exemple 40**

L'application  $f : (\mathbb{C}^*, \cdot) \rightarrow (\mathbb{R}^*, \cdot)$  est un morphisme de groupes.

$$z \mapsto |z|$$

En effet, si  $z, w \in \mathbb{C}^*$ , on a  $f(zw) = |zw| = |z||w| = f(z)f(w)$ .

Son noyau est  $\ker f = \{ z \in \mathbb{C}^* \mid |z| = 1 \} = \mathbb{U}$ .

Son image  $\text{Im}(f)$  est incluse dans  $\mathbb{R}_+^*$  car si  $z \in \mathbb{C}^*$ ,  $|z| > 0$ . De plus, si  $y \in \mathbb{R}_+^*$ , alors  $f(y) = |y| = y$  et donc  $y \in \text{Im}(f)$ . On a donc  $\text{Im}(f) = \mathbb{R}_+^*$ .

## §6 Quelques exemples usuels

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

#### Proposition 41

1. Pour  $a \in \mathbb{Z}$ , l'ensemble  $a\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .
2. Réciproquement, Soit  $H$  un sous-groupe de  $(\mathbb{Z}, +)$ . Il existe un entier  $a \geq 0$  et un seul tel que  $H = a\mathbb{Z}$ .

### Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit  $n \in \mathbb{N}$ . La relation de congruence modulo  $n$ , définie par

$$x \equiv y \pmod{n} \iff \exists k \in \mathbb{Z}, y = x + kn$$

est une relation d'équivalence. On note  $\mathbb{Z}/n\mathbb{Z}$  l'ensemble des classes d'équivalence modulo  $n$ , ainsi

$$\mathbb{Z}/n\mathbb{Z} = \{ \dot{x} \mid x \in \mathbb{Z} \} = \{ \dot{x} \mid x \in [0, n-1] \}$$

où  $\dot{x} = x + n\mathbb{Z}$  désigne la classe d'équivalence de l'entier  $x$  pour cette relation.

#### Proposition 42

Soit  $n \in \mathbb{N}$ ,  $n \geq 1$ .

1.  $\mathbb{Z}/n\mathbb{Z}$  est fini et de cardinal  $n$ .
2. L'application

$$\begin{aligned} \oplus : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ (\dot{x}, \dot{y}) &\mapsto \dot{x} \oplus \dot{y} = \overbrace{x+y}^{\cdot} \end{aligned}$$

définit une loi de composition interne sur  $\mathbb{Z}/n\mathbb{Z}$ .

3.  $(\mathbb{Z}/n\mathbb{Z}, \oplus)$  est un groupe commutatif.

Dans la suite, on notera simplement  $\dot{x} + \dot{y}$  plutôt que  $\dot{x} \oplus \dot{y}$ .

#### Exemple 43

Voici la table d'addition de  $\mathbb{Z}/6\mathbb{Z} = \{ \dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5} \}$ .

+	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{5}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$

### Groupes des permutations d'un ensemble

#### Exemple 44

##### Groupes des permutations d'un ensemble $X$

Soit  $X$  un ensemble et  $S(X)$  l'ensemble des permutations de  $X$ . Si  $f, g$  sont des permutations de  $X$ , il en est de même de  $f \circ g$  ;  $(f, g) \mapsto f \circ g$  définit donc une loi de composition interne sur l'ensemble  $S(X)$  ; cette loi de composition interne est associative ; elle admet un élément neutre, à savoir l'application identique  $\text{Id}_X$  ; enfin, si  $f$  est une permutation de  $X$ , il en est de même de l'application réciproque  $f^{-1}$  et celle-ci est évidemment inverse de  $f$  pour la loi de composition interne considérée.

Ainsi,  $(S(X), \circ)$  est un groupe ; on l'appelle le **groupe des permutations de l'ensemble  $X$** .

C'est l'étude de ces groupes par Galois (lorsque  $X$  est un ensemble fini) qui a conduit, historiquement, à la notion générale et « abstraite » de groupe.

#### Exemple 45

Soit  $X$  un ensemble et  $x$  un élément de  $X$  et  $G = S(X)$  le groupe des permutations de  $X$  (pour la loi  $\circ$  bien entendu). Alors  $G_x = \{ g \in G \mid g(x) = x \}$ , c'est-à-dire l'ensemble des éléments de  $G$  qui laisse  $x$  invariant, est un sous-groupe de  $G$ , appelé **stabilisateur de  $x$** . En effet, l'élément neutre de  $G$ , à savoir  $\text{Id}_X$ , vérifie  $\text{Id}_X(x) = x$ , donc  $\text{Id}_X \in G_x$ . De plus, si  $g \in G_x$ , alors  $g(x) = x$  ; en appliquant la fonction  $g^{-1}$  à cette égalité, on obtient  $x = g^{-1}(g(x)) = g^{-1}(x)$  et donc  $g^{-1} \in G_x$ . Enfin, si  $g, h \in G_x$ , alors  $(g \circ h)(x) = g(h(x)) = g(x) = x$  et donc  $g \circ h \in G_x$ .

### Sous-groupe engendré par un élément

#### Définition 46

Soit  $(G, \cdot)$  un groupe et  $a \in G$ . Le sous-groupe de  $G$  engendré par l'élément  $a$  est

$$\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}.$$

- On dit que  $G$  est un **groupe monogène** lorsqu'il existe  $a \in G$  tel que  $\langle a \rangle = G$ . Un tel  $a$  est un **générateur** de  $G$ .
- On qualifie de **cyclique** tout groupe monogène fini.

#### Exemple 47

1.  $(\mathbb{Z}, +)$  est un groupe monogène, engendré par 1.
2.  $(\mathbb{U}_n, \cdot)$  est un groupe cyclique, engendré par  $\omega = e^{2i\pi/n}$ .
3.  $(\mathbb{Z}/n\mathbb{Z}, +)$  est un groupe cyclique, engendré par  $\dot{1}$ .

## 14.3 LA STRUCTURE D'ANNEAU

### §1 Anneaux

#### Définition 48

Soit  $\top$  et  $\star$  deux lois de composition internes sur un ensemble  $E$ . On dit que la loi  $\star$  est **distributive** par rapport à la loi  $\top$  si l'on a

$$x \star (y \top z) = (x \star y) \top (x \star z) \quad (14.1)$$

$$(y \top z) \star x = (y \star x) \top (z \star x) \quad (14.2)$$

pour  $x, y, z$  dans  $E$ .

On remarquera que les deux égalités sont équivalentes si la loi  $\star$  est commutative.

#### Exemple 49

Dans l'ensemble  $\mathcal{P}(E)$  des parties d'un ensemble  $E$ , chacune des lois internes  $\cap$  et  $\cup$  est distributive par rapport à elle-même et à l'autre. Cela résulte des formules du type

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

#### Définition 50

On appelle **anneau** un ensemble  $A$  muni de deux lois de composition appelées respectivement **addition** et **multiplication**, satisfaisant aux axiomes suivants :

1. Pour l'addition,  $A$  est un groupe commutatif.
2. La multiplication est associative et possède un élément neutre.
3. La multiplication est distributive par rapport à l'addition.

On dit que l'anneau  $A$  est **commutatif** si sa multiplication est commutative.



**Dans la suite** On note  $(x, y) \mapsto x + y$  l'addition et  $(x, y) \mapsto xy$  la multiplication ; on note  $0$  (ou  $0_A$ ) l'élément neutre de l'addition et  $1$  (ou  $1_A$ ) celui de la multiplication. Enfin, on note  $-x$  l'opposé de  $x$  pour l'addition. Pour économiser les parenthèses, on convient que la multiplication est prioritaire sur l'addition.

Les axiomes d'un anneau s'expriment donc par les identités suivantes :

- |     |                             |                                      |
|-----|-----------------------------|--------------------------------------|
| (1) | $x + (y + z) = (x + y) + z$ | (associativité de l'addition)        |
| (2) | $x + y = y + x$             | (commutativité de l'addition)        |
| (3) | $0 + x = x + 0 = x$         | (zéro)                               |
| (4) | $x + (-x) = (-x) + x = 0$   | (opposé)                             |
| (5) | $x(yz) = (xy)z$             | (associativité de la multiplication) |
| (6) | $x \cdot 1 = 1 \cdot x = x$ | (élément unité)                      |
| (7) | $(x + y) \cdot z = xz + yz$ | (distributivité à gauche)            |
| (8) | $x \cdot (y + z) = xy + xz$ | (distributivité à droite)            |

Enfin, l'anneau  $A$  est commutatif si l'on a  $xy = yx$  pour  $x, y$  dans  $A$ .

**Exemple 51**

$$A = \{ 0, 1 \}.$$

Voici quelques anneaux que nous rencontrerons en MP2I

1.  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  sont des anneaux intègres.
2. L'anneau des suites à valeur réelles,  $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$ , est un anneau commutatif qui n'est pas intègre.
3. L'anneau des applications de  $\mathbb{R}$  dans  $\mathbb{R}$ ,  $(\mathfrak{F}(\mathbb{R}, \mathbb{R}), +, \cdot)$ , est un anneau commutatif qui n'est pas intègre.
4. L'anneau des matrices carrées  $n \times n$ ,  $(\mathfrak{M}_n(\mathbb{K}), +, \cdot)$  est un anneau qui n'est pas commutatif et possède des diviseurs de 0.
5. L'anneau des polynômes,  $(\mathbb{K}[X], +, \cdot)$ , est un anneau intègre (et donc commutatif).
6. ...

**Exemple 52**

On peut définir une addition et une multiplication sur  $\mathbb{Z}/n\mathbb{Z}$  par

$$\forall (x, y) \in \mathbb{Z}, \dot{x} \oplus \dot{y} = \overbrace{x + y}^{\cdot} \text{ et } \dot{x} \otimes \dot{y} = \overbrace{x \times y}^{\cdot}.$$

Muni de ces deux lois,  $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$  est un anneau commutatif. Dans la suite, on notera plus simplement  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ .

Voici les tables d'addition et multiplication de  $\mathbb{Z}/6\mathbb{Z} = \{ \dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5} \}$ .

+	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$		$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	et	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$		$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$		$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{0}$	$\dot{2}$	$\dot{4}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$		$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{0}$	$\dot{3}$
$\dot{4}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$		$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{4}$	$\dot{2}$
$\dot{5}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$		$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

## §2 Éléments inversibles d'un anneau; corps

**Définition 53**

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

- Si  $x \in A$  admet un inverse pour la multiplication, on dit que  $x$  est un **élément inversible**<sup>a</sup> de  $A$
- L'ensemble des éléments inversibles de  $A$  se note  $A^\times$  ou  $U(A)$ .
- $(A^\times, \cdot)$  est un groupe appelé **groupe multiplicatif de l'anneau  $A$**  dont 1 est l'élément neutre.

<sup>a</sup>On dit aussi que  $x$  est une **unité** de  $A$ , mais nous n'utiliserons pas cette terminologie dangereuse.

Plus généralement, lorsque l'on parle d'éléments permutables, d'élément inversible, d'élément simplifiable dans un anneau  $A$ , toutes ces notions sont relatives à la multiplication dans  $A$ .

**Remarque** Si  $x$  et  $y$  sont deux éléments inversibles d'un anneau  $A$ , alors  $xy$  l'est aussi et  $(xy)^{-1} = y^{-1}.x^{-1}$ .

**Exemple 54**  $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ ,  $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ ,  $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ .

**Proposition 55** *Le groupe multiplicatif de  $(\mathbb{Z}, +, \cdot)$  est  $\{-1, 1\} = \mathbb{U}_2$ .*

**Exemple 56** Le groupe multiplicatif de  $\mathbb{Z}/6\mathbb{Z}$  est  $\{1, 5\}$ . L'anneau  $\mathbb{Z}/6\mathbb{Z}$  n'est donc pas un corps.

**Définition 57** On dit qu'un anneau  $\mathbb{K}$  est un **corps** s'il est commutatif, non réduit à 0 et si tout élément non nul de  $\mathbb{K}$  est inversible.

**Exemple 58** Les corps usuels sont  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$ .

Néanmoins, il en existe bien d'autres, par exemple, le corps à deux éléments  $\{0, 1\}$  où l'on a  $0 + 0 = 1 + 1 = 0$ ,  $0 + 1 = 1 + 0 = 1$ , et la multiplication usuelle ; ou encore une structure de corps<sup>2</sup> sur  $\mathbb{N}$  telle que «deux et deux font zéro, mais deux fois deux font trois, trois fois deux font 1...».

**Proposition 59** *Soit  $n \in \mathbb{N}$ .*

1. *Pour  $x \in \mathbb{Z}$ ,  $x$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$  si, et seulement si  $\text{pgcd}(x, n) = 1$ .*
2. *Les générateurs du groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$  sont les éléments inversibles de l'anneau  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ .*
3. *L'anneau  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  est un corps si, et seulement si  $n$  est premier.*

### §3 Calculs dans un anneau

Si  $x$  est un élément de  $A$ , on a toujours les notations  $n.x$  ( $n \in \mathbb{Z}$ ) et  $x^n$  ( $n \in \mathbb{N}$ ) :

$$n.x = \begin{cases} \overbrace{x + \dots + x}^n & n > 0 \\ 0 & n = 0 \\ \underbrace{(-x) + \dots + (-x)}_{-n} & n < 0 \end{cases}, \quad x^n = \begin{cases} \overbrace{x \dots x}^n & n > 0 \\ 1 & n = 0 \\ \underbrace{x^{-1} \dots x^{-1}}_{-n} & n < 0 \text{ et } x \text{ inversible} \end{cases}$$

<sup>2</sup>Qui se généralise aux nombres «surréels», inventés par le mathématicien anglais John Conway. Ces nombres sont utiles en théorie des jeux ; voir *On numbers and games*, qui contient bien d'autres merveilles.



**Proposition 60**

Soient  $A$  un anneau et  $x, y$  des éléments de l'anneau  $A$ .

1.  $x \cdot 0 = 0 \cdot x = 0$ .

2.  $x \cdot (-y) = (-x) \cdot y = -(xy)$  et  $(-x)(-y) = xy$ . (Règle des signes)

3. Pour  $n \in \mathbb{N}$ , on a

$$(-x)^n = \begin{cases} x^n & \text{si } n \text{ est pair} \\ -x^n & \text{si } n \text{ est impair.} \end{cases}$$

Formule qui reste valable aussi si  $x$  est inversible et  $n \in \mathbb{Z}$ .

**Proposition 61****Conséquence de la distributivité**

Soit  $A$  un anneau,  $n$  un entier  $> 0$ . Alors pour  $a, x_1, x_2, \dots, x_n \in A$ , on a

$$a \left( \sum_{k=1}^n x_k \right) = \sum_{k=1}^n (ax_k) \quad \text{et} \quad \left( \sum_{k=1}^n x_k \right) a = \sum_{k=1}^n (x_k a).$$



Les règles de calcul classiques dans  $\mathbb{Z}$ ,  $\mathbb{Q}$  ou  $\mathbb{R}$  ne sont pas toujours valables dans un anneau quelconque ; par exemple si, dans un anneau non commutatif,  $x$  et  $y$  ne commutent pas, on a

$$(x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2 \neq x^2 + 2xy + y^2$$

$$(x + y)(x - y) = x^2 - xy + yx - y^2 \neq x^2 - y^2.$$

Si l'anneau est commutatif les formules classiques concernant  $(x+y)^2, (x+y)^3, \dots, (x+y)(x-y)$  sont vraies. Plus généralement, on a

**Théorème 62**

Soient  $A$  un anneau,  $(x, y) \in A^2$  deux éléments qui commutent ( $xy = yx$ ), alors pour tout entier  $n \in \mathbb{N}$ ,

$$(x + y)^n = \sum_{p=0}^n \binom{n}{p} x^{n-p} y^p;$$

$$x^{n+1} - y^{n+1} = (x - y)(x^n + x^{n-1}y + \dots + xy^{n-1} + y^n) = (x - y) \sum_{p=0}^n x^{n-p} y^p$$

**Corollaire 63****Calcul d'une progression géométrique**

Soient  $A$  un anneau,  $a$  un élément de  $A$  et  $n$  un entier  $> 0$ . Alors

$$1 - a^n = (1 - a)(1 + a + a^2 + \dots + a^{n-1}).$$

## §4 Sous-anneaux

### Définition 64

Soit  $(A, +, \cdot)$  un anneau et  $B$  une partie de  $A$ . On dit que  $B$  est un sous anneau de  $A$  lorsque

- $1_A \in B$ ,
- $B$  est un sous groupe de  $(A, +)$ ,
- $B$  est stable par produit :  $\forall (x, y) \in B^2, xy \in B$ .

### Proposition 65

*Si  $B$  est un sous anneau de  $A$ , alors  $B$  muni des deux lois induites a une structure d'anneau.*

## §5 Idéaux d'un anneau commutatif

### Remarque

Pour un entier  $a \geq 2$ , l'ensemble  $a\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$  et il est stable par produit ; mais  $1 \notin a\mathbb{Z}$ .  $a\mathbb{Z}$  n'est donc pas un sous-anneau de  $\mathbb{Z}$ .

### Définition 66

Soit  $(A, +, \cdot)$  un anneau *commutatif* et  $I$  une partie de  $A$ . On dit que  $I$  est un **idéal** de  $A$  lorsque

- $I$  est un sous groupe de  $(A, +)$ ,
- $\forall a \in A, \forall x \in I, ax \in I$ .

### Remarque

Les idéaux de  $\mathbb{Z}$  sont exactement les sous-groupes de  $(\mathbb{Z}, +)$ . Tout idéal d'un anneau  $A$  est un sous-groupe de  $(A, +)$ , l'inverse peut être faux :  $\mathbb{Z}$  est un sous-anneau, mais pas un idéal, de  $\mathbb{Q}$ .

### Définition 67

Soit  $(A, +, \cdot)$  un anneau commutatif et  $x \in A$ . L'ensemble

$$xA = \{ xa \mid a \in A \}$$

est un idéal de  $A$ . On l'appelle **idéal engendré par l'élément  $x$** .

## §6 Anneau intègre

### Définition 68

Soient  $A$  un anneau et  $x$  un élément de l'anneau  $A$ . On dit que  $x$  est **régulier** (ou **simplifiable**) si pour tout  $y \in A$ , on a les implication

$$x \cdot y = 0_A \implies y = 0_A \quad \text{et} \quad y \cdot x = 0_A \implies y = 0_A.$$

Dans le cas contraire, on dit que  $x$  est un **diviseur de 0**.

### Remarque

- On dit que  $x$  est un **diviseur à droite de 0** s'il existe  $y \neq 0$  tel que  $yx = 0$ .
- On dit que  $x$  est un **diviseur à gauche de 0** s'il existe  $y \neq 0$  tel que  $xy = 0$ .  
Lorsque  $A$  est commutatif, il est inutile de préciser « à gauche » ou « à droite ».

**Définition 69**

On dit qu'un anneau  $A$  est **intègre** s'il est commutatif, non réduit à 0, et si le produit de deux éléments non nuls de  $A$  est non nul, ou encore

$$\forall (x, y) \in A^2, xy = 0 \implies (x = 0 \text{ ou } y = 0).$$

**Proposition 70**

Soit  $A$  un anneau intègre, alors on a une règle de simplification pour la multiplication

$$\forall (x, y, a) \in A^3, (ax = ay \text{ et } a \neq 0) \implies x = y$$

$$\forall (x, y, a) \in A^3, (xa = ya \text{ et } a \neq 0) \implies x = y$$

On retiendra surtout que ceci est faux dans un anneau quelconque.

**Exemple 71**

L'ensemble  $\mathbb{Z}$  des entiers relatifs muni de l'addition et la multiplication usuelle, est un anneau intègre.

## §7 Morphisme d'anneaux

**Définition 72**

Soient  $A, A'$  deux anneaux. Une application  $f : A \rightarrow A'$  est appelée **morphisme d'anneaux** si elle vérifie les conditions suivantes:

- Pour tous  $x, y \in A$ ,  $f(x + y) = f(x) + f(y)$ .
- Pour tous  $x, y \in A$ ,  $f(xy) = f(x)f(y)$ .
- $f(1_A) = 1_{A'}$ .

Si de plus  $f$  est bijective, on dit que c'est un **isomorphisme d'anneaux** de  $A$  sur  $A'$ .

**Proposition 73**

Soit  $f : A \rightarrow A'$  un morphisme d'anneaux.

1. L'image  $f(B)$  d'un sous-anneau  $B$  de  $A$  est un sous-anneau de  $A'$ . En particulier,  $\text{Im}(f) = f(A)$  est un sous-anneau de  $A'$ .
2. Si  $B'$  est un sous-anneau de  $A'$ ,  $f^{-1}(B')$  est un sous-anneau de  $A$ .
3. Supposons  $A$  commutatif. Le noyau  $\ker(f)$  de  $f$  est un idéal de  $A$ .

**Théorème 74**

Soit  $f : A \rightarrow A'$  un morphisme d'anneaux.

1. Pour que  $f$  soit injectif, il faut, et il suffit que son noyau soit  $\{0_A\}$ .
2. Si  $f$  est surjectif,  $f^{-1}$  est aussi un morphisme d'anneaux.

## 14.4 LA STRUCTURE D'ESPACE VECTORIEL

### Définition 75

Étant donné un corps  $(\mathbb{K}, +, \cdot)$ , d'éléments neutres  $0_{\mathbb{K}}$  et  $1_{\mathbb{K}}$ , on appelle **espace vectoriel sur  $\mathbb{K}$**  un ensemble  $E$  muni d'une structure algébrique définie par la donnée

1. d'une loi de composition interne, appelée **addition**

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

telle que  $(E, +)$  soit un groupe commutatif.

2. D'une loi d'action appelée **multiplication externe**

$$\begin{aligned} \mathbb{K} \times E &\rightarrow E \\ (\lambda, x) &\mapsto \lambda \cdot x \end{aligned}$$

qui satisfait aux axiomes suivants <sup>a</sup>

- Pour tous  $\lambda \in \mathbb{K}, x \in E, y \in E$ ,  $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$ .
- Pour tous  $\lambda \in \mathbb{K}, \mu \in \mathbb{K}, x \in E$ ,  $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$ .
- Pour tous  $\lambda \in \mathbb{K}, \mu \in \mathbb{K}, x \in E$ ,  $(\lambda \cdot \mu) \cdot x = \lambda \cdot (\mu \cdot x)$ .
- Pour tout  $x \in E$ ,  $1_{\mathbb{K}} \cdot x = x$ .

<sup>a</sup>Règle bien connue : pour économiser les parenthèses, on convient que la multiplication est prioritaire sur l'addition.

## 14.5 LA STRUCTURE D'ALGÈBRE

### Définition 76

On appelle  $\mathbb{K}$ -algèbre un quadruplet  $(A, +, *, \cdot)$  tel que

- $(A, +, *)$  est un anneau.
- $(A, +, \cdot)$  est un  $\mathbb{K}$ -espace vectoriel.
- $\forall \lambda \in \mathbb{K}, \forall (x, y) \in A^2, (\lambda x) * y = x * (\lambda y) = \lambda(x * y)$ .