

# Structures algébriques

Extrait du programme officiel :

CONTENUS	CAPACITÉS & COMMENTAIRES
<b>a) Compléments sur les groupes</b>	
Intersection de sous-groupes.	
Sous-groupe engendré par une partie. Partie génératrice d'un groupe.	
Sous-groupes du groupe $(\mathbb{Z}, +)$ .	
Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ . Générateurs de $\mathbb{Z}/n\mathbb{Z}$ .	
Groupe monogène, groupe cyclique.	Groupe des racines $n$ -ièmes de l'unité.
Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$ .	
Ordre d'un élément d'un groupe.	L'ordre de $x$ est le cardinal du sous-groupe de $G$ engendré par $x$ .
Si $x$ est d'ordre fini $d$ et si $e$ désigne le neutre de $G$ , alors, pour tout $n \in \mathbb{Z}$ , $x^n = e \iff d n$ .	
L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.	La démonstration n'est exigible que pour $G$ commutatif.
<b>b) Compléments sur les anneaux</b>	
Produit fini d'anneaux.	
Idéal d'un anneau commutatif.	Noyau d'un morphisme d'anneaux commutatifs.
Idéal engendré par un élément.	Notation $xA$ .
Divisibilité dans un anneau commutatif intègre.	Interprétation en termes d'idéaux.
<b>c) Idéaux de <math>\mathbb{Z}</math></b>	
Idéaux de $\mathbb{Z}$ .	
Définition du PGCD de $n \geq 2$ entiers relatifs en termes d'idéaux, relation de Bézout.	Lien avec le programme de première année.
<b>f) Algèbres</b>	
Algèbre.	Les algèbres sont unitaires. Exemples : $\mathbb{K}[X]$ , $\mathcal{L}(E)$ , $\mathcal{M}_n(\mathbb{K})$ , $\mathcal{F}(X, \mathbb{K})$ .
Sous-algèbre.	
Morphisme d'algèbres.	



# Table des matières

<b>4 Structures algébriques</b>	<b>1</b>
<b>I Groupes et sous-groupes</b>	<b>3</b>
1 Structure de groupe (MP2I)	3
2 Puissances ou itérées d'un élément (MP2I)	4
3 Régularité	5
4 Groupe produit (MP2I)	7
5 Sous-groupes	7
a Définition et caractérisation (MP2I)	7
b Intersection et réunion (MPI)	9
c Sous-groupes de $(\mathbb{Z}, +)$ (MPI)	9
6 Morphismes (MP2I)	10
a Définition	10
b Noyau et image	11
c Isomorphismes	13
7 Groupes monogènes (MPI)	14
a Sous-groupes engendré par une partie	14
b Groupes monogènes et cycliques	15
c Ordre d'un élément dans un groupe	15
<b>II Anneaux et Corps</b>	<b>18</b>
1 Anneaux (MP2I)	18
2 Groupe des inversibles (MP2I)	19
3 Calculs dans un anneau (MP2I)	19
4 Corps (MP2I)	21
5 Intégrité (MP2I)	21
6 Anneau produit (MPI)	22
7 Sous-anneau et sous-corps (MP2I)	23
8 Morphismes d'anneaux (MP2I)	25
<b>III Idéal d'un anneau commutatif (MPI)</b>	<b>26</b>
1 Généralités	26
2 Somme et intersection d'idéaux	28
3 Idéal principal	29
4 Divisibilité dans un anneau intègre	29
<b>IV Arithmétique sur <math>\mathbb{Z}</math> (MP2I)</b>	<b>30</b>
1 PGCD	30
2 PPCM	32
3 Nombres premiers	33
4 Congruences	35
<b>V Structure d'algèbre (MPI)</b>	<b>36</b>
1 Algèbre et sous-algèbre	36
2 Morphismes d'algèbres	37

VI Complément (HP) : sous-groupes de  $(\mathbb{R}, +)$

# GROUPES ET SOUS-GROUPES

## 1 Structure de groupe (MP2I)

Remarque : Quelques rappels

R1 – ■ **Loi de composition interne** sur un ensemble  $E$  : toute application  $\star : \begin{matrix} E \times E & \longrightarrow & E \\ (x, y) & \longrightarrow & x \star y \end{matrix}$ .

■ Elle est dite

★ **associative** lorsque

$$\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$$

(que l'on peut alors noter  $x \star y \star z$ .)

★ **commutative** lorsque

$$\forall (x, y) \in E^2, x \star y = y \star x.$$

■ On dit que  $e$  est **élément neutre** pour  $\star$  si pour tout  $x \in E, x \star e = e \star x = x$ .

### Exercice 1

S'il existe, l'élément neutre est unique.

★ **Notation additive** :  $0x = e$  avec  $e$  souvent noté  $0$  ou  $0_E$  appelé élément nul.

★ **Notation multiplicative** :  $x^0 = e$  avec  $e$  souvent noté  $1$  ou  $1_E$  appelé élément unité.

■ Un élément  $x$  de  $E$  est dit **symétrisable** pour  $\star$  si on a  $y \in E$  tel que  $x \star y = y \star x = e$ .

### Exercice 2

S'il existe,  $y$  est unique.

★ **Notation additive** : on parle d'opposé, noté  $-x$ . Pour  $x + (-y)$ , on note  $x - y$ .

★ **Notation multiplicative** : on parle d'inverse, noté  $x^{-1}$ .

⚠  $\frac{x}{y}$  n'a pas de sens en général : cela désigne  $x \star y^{-1}$  ou  $y^{-1} \star x$  ?

### Exemple

E1 – L'élément neutre  $e$  (lorsqu'il existe) est toujours symétrisable, de symétrique lui-même.

Être symétrisable à gauche ou à droite ne suffit pas.

### Exemple

E2 – Sur  $E^E$  pour  $\circ$ , l'élément neutre est  $\text{id}_E$ .

★  $(\exists g \in E^E, f \circ g = g \circ f = \text{id}_E) \iff f$  bijective (ie inversible pour  $\circ$ ).

★  $(\exists g \in E^E, f \circ g = \text{id}_E) \iff f$  surjective.

★  $(\exists g \in E^E, g \circ f = \text{id}_E) \iff f$  injective.

■ Soit  $\star$  une loi de composition interne associative sur  $E$  notée multiplicativement.

Si  $x$  et  $y$  sont symétrisables, alors

★  $x \star y$  l'est aussi. De plus,  $(x \star y)^{-1} = y^{-1} \star x^{-1}$ .

★  $x^{-1}$  l'est aussi et  $(x^{-1})^{-1} = x$ .

**Définition 1 : Groupe**

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- (i)  $\star$  est une loi de composition interne sur  $G$
- (ii)  $\star$  est associative
- (iii)  $G$  admet un élément neutre pour  $\star$
- (iv) Tout élément de  $G$  admet un symétrique dans  $G$  pour  $\star$ .

Si, de plus,  $\star$  est commutative, on dit que  $(G, \star)$  est un **groupe commutatif** ou **groupe abélien**.

**Remarque**

**R2** – En particulier, un groupe n'est jamais vide.

**Exemple**

**E3** –  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$  et  $(\mathbb{C}, +)$  sont des groupes commutatifs de neutre 0.

**E4** – Si  $D$  est un ensemble non vide,  $(\mathbb{R}^D, +)$  et  $(\mathbb{C}^D, +)$  et en particulier  $(\mathbb{R}^{\mathbb{N}}, +)$  et  $(\mathbb{C}^{\mathbb{N}}, +)$  sont des groupes commutatifs, de neutre la fonction / suite nulle.

**E5** –  $(\mathbb{Q}^*, \times)$ ,  $(\mathbb{Q}_+^*, \times)$ ,  $(\mathbb{R}^*, \times)$ ,  $(\mathbb{R}_+^*, \times)$  et  $(\mathbb{C}^*, \times)$  sont des groupes commutatifs de neutre 1.

**E6** – Si  $E$  est un ensemble non vide, on note  $\mathfrak{S}(E)$  l'ensemble des permutations de  $E$  (bijection de  $E$  sur  $E$ ). Alors  $(\mathfrak{S}(E), \circ)$  est un groupe d'élément neutre  $\text{id}_E$ .

Si  $|E| \geq 3$ , ce groupe n'est pas commutatif.

Si  $n \in \mathbb{N} \setminus \{0, 1\}$ , et  $E = \llbracket 1, n \rrbracket$ , on note  $\mathfrak{S}_n = \mathfrak{S}(\llbracket 1, n \rrbracket)$ .

$(\mathfrak{S}_n, \circ)$  est appelé **groupe symétrique d'ordre  $n$**  (et contient  $n!$  éléments).



Voir exercice du TD : 6, 13

**2 Puissances ou itérées d'un élément (MP2I)****Définition 2 : Itérées d'un élément**

Soit  $E$  un ensemble muni d'une loi de composition interne  $\star$  (notée multiplicativement) **associative** et possédant un élément neutre  $e$ .

Pour tout  $x \in E$  et tout  $n \in \mathbb{N}$ , on définit récursivement

$$x^n = \begin{cases} e & \text{si } n = 0 \\ x^{n-1} \star x & \text{sinon.} \end{cases}$$

**Remarque**

**R3** – Autrement dit,  $x^n = \prod_{k=1}^n x = \underbrace{x \star \cdots \star x}_{n \text{ fois}}$

**R4** – En notation additive,

$$n \cdot x = \begin{cases} 0 & \text{si } n = 0 \\ (n-1) \cdot x + x & \text{sinon.} \end{cases}$$

**Propriété 1 : des exposants**

Soient  $x, y \in E$  et  $n, m \in \mathbb{N}$ .

- (i)  $x^{n+m} = x^n \star x^m = x^m \star x^n$ .
- (ii)  $(x^n)^m = x^{nm} = (x^m)^n$ .
- (iii) Si  $x \star y = y \star x$ ,  $(x \star y)^n = x^n \star y^n$ .
- (iv) Si  $x$  est inversible,  $x^n$  est inversible et  $(x^n)^{-1} = (x^{-1})^n$ .

**Démonstration**

- (i) Par récurrence sur  $m$  (par exemple) à  $n$  fixé et par associativité.
- (ii) Par récurrence sur  $m$  à  $n$  fixé.
- (iii) Par récurrence sur  $n$ .
- (iv) On calcule avec la propriété précédente  $x^n \star (x^{-1})^n = (x \star x^{-1})^n = e$  et de même  $(x^{-1})^n \star x^n = e$ .

**Notation 1 : Exposant négatif**

Si  $x \in E$  inversible et  $n \in \mathbb{N}$ , on note  $x^{-n}$  l'élément  $(x^{-1})^n = (x^n)^{-1}$ .

**Remarque**

**R5** – Les propriétés (i) à (iii) restent vraies pour  $n, m \in \mathbb{Z}$  lorsque  $x$  et  $y$  sont inversibles.

**3 Régularité**

Soit <sup>1</sup>  $E$  un ensemble muni d'une loi de composition interne associative  $\star$  et possédant un élément neutre  $e$ .

**Définition 3 : Régularité**

Soit  $x \in E$ . On dit que  $x$  est **régulier** (ou **simplifiable**)

■ **à gauche** lorsque

$$\forall a, b \in E, \quad x \star a = x \star b \implies a = b$$

■ **à droite** lorsque

$$\forall a, b \in E, \quad a \star x = b \star x \implies a = b$$

On dit que  $x$  est **régulier** lorsqu'il l'est à gauche et à droite.



**Voir exercice du TD : 5**

**Propriété 2 : Régularité d'un inversible**

Tout élément inversible de  $(E, \star)$  est régulier.

**Démonstration**

Si  $x$  est inversible et si  $x \star a = x \star b$ , alors

$$a = (x^{-1} \star x) \star a = x^{-1} \star (x \star a) = x^{-1} \star (x \star b) = (x^{-1} \star x) \star b = b$$

1. On dit que  $(E, \star)$  est un **monoïde**.



par associativité. ■

### Corollaire 1 : Régularité dans un groupe

*Si  $(G, \star)$  est un groupe, alors tout élément de  $G$  est régulier.*

### Corollaire 2 : Bijectivité des translations

*Si  $(G, \star)$  est une groupe et  $a \in G$  fixé.*

Les applications  $\varphi_a : \begin{cases} G \longrightarrow G \\ x \longmapsto a \star x \end{cases}$  et  $\psi_a : \begin{cases} G \longrightarrow G \\ x \longmapsto x \star a \end{cases}$  (appelées translations à gauche et à droite) sont bijectives.

#### Démonstration

On vérifie que  $\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a^{-1}} \circ \varphi_a = \text{id}_G$  et  $\psi_a \circ \psi_{a^{-1}} = \psi_{a^{-1}} \circ \psi_a = \text{id}_G$ . ■

### Corollaire 3

*Si  $(G, \star)$  est une groupe et  $a \in G$  fixé.*

$$G = \{a \star x, x \in G\} = \{x \star a, x \in G\}.$$

#### Démonstration

Il s'agit de la surjectivité des deux applications précédentes. ■

#### Remarque

**R6** – Cela signifie que dans la table de la loi  $\star$  du groupe  $G$ , chaque élément de  $G$  apparaît une et une seule fois sur chaque ligne et sur chaque colonne.

#### Exemple

**E7** – Si on considère le groupe des racines cubique de l'unité :  $\mathbb{U}_3 = \{1, j, j^2\}$  muni de la loi  $\times$ , on a la table

$\star$	1	j	$j^2$
1	1	j	$j^2$
j	j	$j^2$	1
$j^2$	$j^2$	1	j

## 4 Groupe produit (MP2I)

### Propriété 3 : Groupe produit

Soit  $(G, \star)$  et  $(H, \Delta)$  des groupes.  
 Pour tout  $(g, h)$  et  $(g', h')$  dans  $G \times H$ , on pose

$$(g, h) \top (g', h') = (g \star g', h \Delta h').$$

Alors  $(G \times H, \top)$  a une structure de groupe.  
 Si, de plus, les lois  $\star$  et  $\Delta$  sont commutatives, alors  $\top$  l'est.

### Démonstration

- Le fait que  $\top$  soit une loi de composition interne sur  $G \times H$  provient du fait que  $\star$  et  $\Delta$  le sont sur  $G$  et  $H$  respectivement.
- Un calcul facile mais pénible à écrire permet de vérifier que les associativités de  $\star$  et  $\Delta$  donnent celle de  $\top$ .
- Si  $e_G$  et  $e_H$  sont les éléments neutres de  $G$  et  $H$ , alors  $(e_G, e_H)$  est bien neutre sur  $G \times H$ .
- Si  $g \in G$  et  $h \in H$  d'inverses  $g^{-1}$  et  $h^{-1}$ , alors  $(g^{-1}, h^{-1})$  est l'inverse de  $(g, h)$ .

### Remarque

**R7** – Cela se généralise à un nombre de groupes quelconque  $(G_1, \star_1), \dots, (G_p, \star_p)$  avec pour tout  $(x_1, \dots, x_p)$  et  $(y_1, \dots, y_p)$  dans  $G_1 \times \dots \times G_p$ ,

$$(x_1, \dots, x_p) \top (y_1, \dots, y_p) = (x_1 \star_1 y_1, \dots, x_p \star_p y_p).$$

## 5 Sous-groupes

### a Définition et caractérisation (MP2I)

#### Définition 4 : Sous-groupe

Soit  $(G, \star)$  groupe. On note  $\star|_{H^2}$  la restriction à  $H^2$  de la loi  $\star$ .  
 On dit que  $H$  est un **sous-groupe** de  $(G, \star)$  si  $H \subset G$  et  $(H, \star|_{H^2})$  est un groupe.

#### Propriété 4 : Sous-groupes triviaux

Soit  $(G, \star)$  groupe.  $G$  et  $\{e_G\}$  sont des sous-groupes de  $(G, \star)$  appelés **sous-groupes triviaux**.

#### Propriété 5

- Soit  $H$  un sous-groupe de  $(G, \star)$ .
- (i)  $(H, \star)$  possède le même élément neutre que  $(G, \star)$ .
  - (ii) Si  $x \in H$ , alors  $x$  a même inverse dans  $(H, \star)$  et dans  $(G, \star)$ .

**Démonstration**

- (i) Soient  $e_H$  et  $e_G$  les éléments neutres respectifs. Alors  $e_H \star e_G = e_H = e_H \star e_H$  car  $e_H \in G$  et  $e_G$  neutre sur  $G$  d'une part, et  $e_H$  neutre sur  $H$  d'autre part. Puis, par régularité à gauche de  $e_H$  dans  $G$ ,  $e_G = e_H$ .
- (ii) Si  $x \in H$ , alors  $x$  a un symétrique  $\text{sym}_H(x) \in H \subset G$  tel que  $x \star \text{sym}_H(x) = \text{sym}_H(x) \star x = e_H = e_G$  et donc par unicité,  $x$  inversible dans  $G$  et  $\text{sym}_G(x) = \text{sym}_H(x)$ . ■

**Voir exercice du TD : 7****Propriété 6 : caractérisation des sous-groupes**

Soit  $(G, \star)$  un groupe (multiplicatif). Les propositions suivantes sont équivalentes :

- (i)  $H$  est un sous-groupe de  $(G, \star)$
- (ii)  $\left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ H \text{ est stable par } \star : \forall x, y \in H, x \star y \in H \\ H \text{ est stable par inverse} : \forall x \in H, x^{-1} \in H \end{array} \right.$
- (iii)  $\left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ \forall x, y \in H, x \star y^{-1} \in H \end{array} \right.$

**Remarque**

**R8** – En notation additive, (ii) devient  $\left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (0_G \in H) \\ H \text{ est stable par } \star : \forall x, y \in H, x + y \in H \\ H \text{ est stable par opposé} : \forall x \in H, -x \in H \end{array} \right.$  et (iii) devient  $\left\{ \begin{array}{l} H \subset G, H \neq \emptyset \quad (0_G \in H) \\ \forall x, y \in H, x - y \in H \end{array} \right.$

**Démonstration**

- $(i) \Rightarrow (ii)$  : si  $H \subset G$ ,  $H \subset G$ ,  $H \neq \emptyset$ ,  $H$  stable par  $\star$  (ici) et, d'après la propriété précédente,  $H$  est bien stable par inverse.
- $(ii) \Rightarrow (iii)$  : facile.
- $(iii) \Rightarrow (i)$  : si on a (iii), alors  $H \subset G$ . La loi  $\star$  est associative sur  $G$  donc a fortiori, elle l'est aussi sur  $H$ . Comme  $H$  est non vide, on a  $x \in H$  avec  $x \star x^{-1} = e_G \in H$ . Alors pour tout  $x \in H$ ,  $e_G \star x^{-1} = x^{-1} \in H$ .  $e_G$  est neutre pour  $\star$  sur  $G$  donc l'est aussi sur  $H$ . L'inverse  $x^{-1}$  d'un élément de  $x \in H$  dans  $G$  est dans  $H$ , donc tout élément de  $H$  est symétrisable dans  $H$ . Donc  $H$  est bien un sous-groupe de  $(G, \star)$ . ■

**Remarque**

**R9** – Un sous-groupe d'un groupe abélien est facilement encore commutatif.



**Exemple**

- E 8 –  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  sont des sous-groupes (additifs et abéliens) de  $(\mathbb{C}, +)$ .
- E 9 –  $\mathbb{R}^D$  où  $D \neq \emptyset$  est un sous-groupe additif abélien de  $(\mathbb{C}^D, +)$ .
- E 10 –  $\mathbb{Q}^*, \mathbb{Q}_+^*, \mathbb{R}^*, \mathbb{R}_+^*, \mathbb{U}, \mathbb{U}_n$  pour  $n \in \mathbb{N}^*$  sont des sous-groupes multiplicatifs abéliens de  $(\mathbb{C}^*, \times)$ . (On rappelle que  $\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}$  et pour  $n \in \mathbb{N}^*, \mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\} = \{e^{\frac{2ik\pi}{n}}, k \in \llbracket 0, n-1 \rrbracket\}$ .)



Voir exercice du TD : 9, 10, 12

**Exercice 3 : Théorème de Lagrange**

- Soit  $(G, *)$  un groupe d'ordre (c'est-à-dire de cardinal) fini,  $H$  un sous-groupe de  $G$ .
1. Montrer que la relation définie par  $x \mathcal{R} y \iff x^{-1} * y \in H$  est une relation d'équivalence sur  $G$ .
  2. Vérifier que les classes d'équivalence ont toutes le même cardinal.
  3. Démontrer le théorème de Lagrange :  $|H|$  divise  $|G|$ .

**b**

**Intersection et réunion (MPI)**

**Propriété 7 : Intersection de sous-groupes**

Soit  $(G, \star)$  un groupe et  $(H_i)_{i \in I}$  une famille de sous-groupes de  $(G, \star)$ . Alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $(G, \star)$ .

**Démonstration**

- $(H_i)_{i \in I} \subset G$  car  $\forall i \in I, H_i \subset G$ .
- $(H_i)_{i \in I} \neq \emptyset$  car  $\forall i \in I, e_G \in H_i$ .
- Si  $x, y \in (H_i)_{i \in I}$ , alors  $\forall i \in I, x \star y^{-1} \in H_i$  donc  $x \star y^{-1} \in \bigcap_{i \in I} H_i$ . ■

**Exercice 4 : Réunion de sous-groupes**

Soit  $(G, \star)$  un groupe,  $H, K$  sont des sous groupes de  $(G, \star)$ , alors

$$H \cup K \text{ sous-groupe de } G \iff H \subset K \text{ ou } K \subset H.$$

- $\Leftarrow$  : ok
- $\Rightarrow$  : Si  $H \cup K$  sous-groupe de  $G$  et  $H \not\subset K$ , on va montrer que  $K \subset H$ .  
On a  $h \in H \setminus K$ .  
Soit  $k \in K$ . Alors  $k \star h \in H \cup K$  par stabilité de  $\star$  sur  $H \cup K$ .  
Si  $k \star h \in K$ , alors  $h = k^{-1} \star (k \star h) \in K$ , ce qui n'est pas possible.  
C'est donc que  $k \star h \in H$  et donc  $k = (k \star h) \star h^{-1} \in H$ .  
Finalement, on a bien  $K \subset H$ .

**c**

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

**Notation 2**

Pour tout  $a \in \mathbb{Z}$ , on note  $a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}$ .

**Remarque**

R 10 – On vérifie avec la caractérisation que  $a\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .

Avec  $a\mathbb{Z} = \{\dots, -2a, -a, 0, a, 2a, \dots\}$ , il s'agit du plus petit sous-groupe (au sens de l'inclusion) contenant  $a$ . On dit qu'il est engendré par  $a$  (sur le même principe que les Vect en algèbre linéaire.)

**Propriété 8 : Sous-groupes de  $(\mathbb{Z}, +)$** 

Les sous-groupes  $G$  de  $(\mathbb{Z}, +)$  sont exactement les  $a\mathbb{Z}$  pour  $a \in \mathbb{N}$ .  
De plus, si  $G \neq \{0\}$ ,  $a = \min(G \cap \mathbb{N}^*)$ .

**Démonstration**

- On a déjà que, si  $a \in \mathbb{N}$ ,  $a\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$  par la caractérisation.
  - Réciproquement, considérons  $G$  un sous-groupe de  $(\mathbb{Z}, +)$ .
    - ★ Soit  $G = \{0\}$  et alors  $G = a\mathbb{Z}$  avec  $a = 0$ .
    - ★ Soit  $G \neq \{0\}$  et on peut trouver  $p \in G \setminus \{0\}$ . Soit  $p > 0$  et alors  $p \in G \cap \mathbb{N}^* \neq \emptyset$ , soit  $p < 0$  et alors  $-p \in G \cap \mathbb{N}^* \neq \emptyset$ . On peut donc introduire  $a = \min(G \cap \mathbb{N}^*)$ .  
Montrons que  $G = a\mathbb{Z}$  par double inclusion.
      - $a \in G$ , puis par stabilité et récurrence, pour tout  $n \in \mathbb{N}$ ,  $na \in G$  et par stabilité par passage à l'opposé,  $-an \in G$ . Finalement,  $a\mathbb{Z} \subset G$ .
      - Réciproquement, si  $x \in G \subset \mathbb{Z}$ , par division euclidienne, on a  $(q, r) \in \mathbb{Z}^2$  tel que  $x = aq + r$  et  $0 \leq r < a$ . Or  $x \in G$  et  $aq \in a\mathbb{Z} \subset G$  donc, comme on a un sous-groupe  $r = x - aq \in G \cap \mathbb{N}$ . Mais comme  $r < a = \min(G \cap \mathbb{N}^*)$ ,  $r \notin \mathbb{N}^*$  et donc  $r = 0$ .  
Finalement,  $x = aq \in a\mathbb{Z}$ .
- On a donc bien  $G = a\mathbb{Z}$ .

**6 Morphismes (MP2I)****a Définition****Définition 5 : Morphisme de groupe**

Soient  $(G, \star)$  et  $(G', \bullet)$  deux groupes.

$f : (G, \star) \rightarrow (G', \bullet)$  est un **morphisme de groupes** si et seulement si

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

Lorsque  $(G, \star) = (G', \bullet)$ , on parle d'**endomorphisme** de groupes.

Lorsque  $f$  est bijective, on parle d'**isomorphisme**.

Lorsqu'il existe un isomorphisme entre  $G$  et  $G'$ , on dit que  $G$  et  $G'$  sont **isomorphes**.

Lorsque  $f$  est bijective et  $G = G'$ , on parle d'**automorphisme**.

**Exemple**

E 11 –  $\ln : (\mathbb{R}_+, \times) \rightarrow (\mathbb{R}, +)$  isomorphisme de groupes.

E 12 –  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \times)$  isomorphisme de groupes.

E 13 –  $\begin{cases} (\mathbb{R}, +) & \rightarrow & (\mathbb{U}, \times) \\ \theta & \mapsto & e^{i\theta} \end{cases}$  morphisme de groupes (non injectif).

E 14 – Si  $n \in \mathbb{N}^*$ ,  $\sigma \in \mathfrak{S}_n$ ,  $\varepsilon(\sigma)$  sa signature  $^\sigma$ , alors  $\varepsilon : (\mathfrak{S}_n, \circ) \rightarrow (\{-1, 1\}, \times)$  est un morphisme de groupes, c'est-à-dire

$$\forall \sigma, \sigma' \in \mathfrak{S}_n, \varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma) \times \varepsilon(\sigma').$$

E 15 –  $\det : (\mathcal{GL}(E), \circ) \rightarrow (\mathbb{R}^*, \times)$  et  $\det : (\mathcal{GL}_n(\mathbb{K}), \times) \rightarrow (\mathbb{R}^*, \times)$  sont des morphismes de groupes.

$\alpha$ . C'est-à-dire  $(-1)^{I(\sigma)}$  où  $I(\sigma)$  est le nombre d'inversions de  $\sigma$  ou encore  $(-1)^N$  si  $\sigma$  s'écrit comme produit (composée) de  $N$  transpositions.



Voir exercice du TD : 8, 15, 16

**Propriété 9 : Image du neutre et du symétrique par un morphisme de groupes**

Si  $f : (G, \star) \rightarrow (G', \bullet)$  est un morphisme de groupes, alors  $f(e_G) = e_{G'}$  et pour tout  $x \in G$ ,  $f(\text{sym}(x)) = \text{sym}(f(x))$ .

**Remarque**

R 11 – En notation multiplicative :  $f(x^{-1}) = (f(x))^{-1}$ .

En notation additive :  $f(-x) = -f(x)$ .

On peut avoir un mix des deux : par exemple, si c'est additif au départ et multiplicatif à l'arrivée, ça devient  $f(-x) = (f(x))^{-1}$ .

**Démonstration**

$f(e_G) = f(e_G \star e_G) = f(e_G) \star f(e_G)$  donc comme  $f(e_G)$  est inversible,  $f(e_G) = e_{G'}$ .

$f(x) \bullet f(\text{sym}(x)) = f(x \star \text{sym}(x)) = f(e_G) = e_{G'}$

et  $f(\text{sym}(x)) \star f(x) = f(\text{sym}(x) \star x) = f(e_G) = e_{G'}$  ■

**Propriété 10 : Image d'une itérée**

En notation multiplicative, si  $f : (G, \star) \rightarrow (G', \bullet)$  est un morphisme de groupes, pour tout  $x \in G$  et pour tout  $k \in \mathbb{Z}$ ,  $f(x^k) = (f(x))^k$ .

**Démonstration**

Par récurrence pour  $k \in \mathbb{N}$ , puis par passage à l'inverse et d'après la propriété précédente pour  $k \in \mathbb{Z}^-$ . ■

**Propriété 11 : Composée de morphismes**

Si  $f : (G, \star) \rightarrow (G', \bullet)$  et  $g : (G', \bullet) \rightarrow (G'', \Delta)$  sont des morphismes de groupes, alors  $g \circ f$  en est encore un.



**Noyau et image**

**Définition 6 : Image et noyau d'un morphisme**

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupes.

■ On appelle **noyau** de  $f$  l'ensemble

$$\text{Ker } f = f^{(-1)}(\{e_{G'}\}) = \{x \in G \mid f(x) = e_{G'}\} \subset G.$$

Ainsi,  $x \in \text{Ker } f \iff f(x) = e_{G'}$ .

■ On appelle **image** de  $f$  l'ensemble

$$\text{Im } f = f(G) = \{f(x), x \in G\} \subset G'.$$

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

**Exemple**

$$E 16 - f : \begin{array}{l} (\mathbb{R}, +) \longrightarrow (\mathbb{U}, \times) \\ \theta \longmapsto e^{i\theta} \end{array} : \text{Ker } f = 2\pi\mathbb{Z}.$$

**Propriété 12 : Caractérisations de l'injectivité et de la surjectivité**

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupe.

- $f$  est injectif si et seulement si  $\text{Ker } f = \{e_G\}$ .
- $f$  est surjectif si et seulement si  $\text{Im } f = G'$ .

**Remarque**

R 12 – Ainsi,  $f$  est injective si et seulement si  $f(x) = e_{G'} (= f(e_G)) \implies x = e_G$  !

**Démonstration**

- Remarquons qu'on a toujours  $e_G \in \text{Ker } f$  car  $f(e_G) = e_{G'}$ .  
Si  $f$  est injectif, alors  $x \in \text{Ker } f \iff f(x) = e_{G'} = f(e_G) \iff x = e_G$ , donc  $\text{Ker } f = \{e_G\}$ .  
Si  $\text{Ker } f = \{e_G\}$  et si  $f(x) = f(x')$ , alors (en notation multiplicative)

$$e_{G'} = f(x) \bullet (f(x'))^{-1} = f(x) \bullet f(x'^{-1}) = f(x \star x'^{-1})$$

donc  $x \star x'^{-1} \in \text{Ker } f$  donc  $x \star x'^{-1} = e_G$  donc  $x = x'$ .  
 $f$  est bien injectif.

- La caractérisation est valable pour les fonctions en général. Par définition,

$$f \text{ est surjective} \iff \text{Im } f = \{f(x), x \in G\} = G'$$

**Exemple**

E 17 – La fonction  $f$  de l'exemple précédent est donc non injective car  $\text{Ker } f = 2\pi\mathbb{Z} \neq \{0\}$ .

**Propriété 13 : Images directe et réciproque d'un sous-groupe**

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupes.

- Si  $H$  est un sous-groupe de  $(G, \star)$ , alors  $f(H)$  est un sous-groupe de  $(G', \bullet)$
- Si  $H'$  est un sous-groupe de  $(G', \bullet)$ ,  $f^{(-1)}(H')$  est un sous-groupe de  $(G, \star)$ .

**Démonstration**

- $f(H)$  est un sous groupe de  $(G', \bullet)$  :
  - ★  $f(H) \subset G'$
  - ★  $f(H) \neq \emptyset$  car  $H \neq \emptyset$
  - ★ Si  $y, y' \in \text{inf}(H)$ , on a  $x, x' \in H$  tels que  $y = f(x)$  et  $y' = f(x')$ .  $f$  étant un morphisme de groupes,

$$y \bullet y'^{-1} = f(x) \bullet f(x')^{-1} = f(\underbrace{x \star x'^{-1}}_{\in H}) \in f(H).$$

- $f^{(-1)}(H')$  est un sous groupe de  $G$  :

- \*  $f^{(-1)}(H') \subset G$
- \*  $f^{(-1)}(H') \neq \emptyset$  car  $e_G \in f^{(-1)}(H')$  car  $f(e_G) = e_{G'} \in H'$ .
- \* Si  $x, x' \in f^{(-1)}(H')$ ,  $f$  étant un morphisme de groupes,  $f(x \star x'^{-1}) = \underbrace{f(x)}_{\in H'} \cdot \underbrace{f(x')^{-1}}_{\in H'} \in H'$ , donc  $x \star x'^{-1} \in f^{(-1)}(H')$ . ■

**Corollaire 4 : Cas particulier du noyau et de l'image**

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupes.  
 Alors  $\text{Ker } f$  est un sous-groupe de  $(G, \star)$  et  $\text{Im } f$  est un sous-groupe de  $(G', \bullet)$ .

**Démonstration**

- $\text{Ker } f = f^{(-1)}(\{e_{G'}\})$  avec  $\{e_{G'}\}$  sous-groupe de  $(G', \bullet)$
- $\text{Im } f = f(G)$  avec  $G$  sous-groupe de  $(G, \star)$ . ■

**Exemple**

E 18 –  $f : \begin{cases} (\mathbb{R}, +) & \rightarrow & (\mathbb{C}^*, \times) \\ \theta & \mapsto & e^{i\theta} \end{cases}$  étant un morphisme de groupes,  $\text{Im } f = \mathbb{U}$  est un sous-groupe de  $(\mathbb{C}^*, \times)$  et  $\text{Ker } f = 2\pi\mathbb{Z}$  est un sous-groupe de  $(\mathbb{R}, +)$ .  
 $\mathbb{U}$  est aussi le noyau du morphisme  $|\cdot| : \mathbb{C}^* \rightarrow \mathbb{R}^*$ .

E 19 –  $f : \begin{cases} (\mathbb{C}^*, \times) & \rightarrow & (\mathbb{C}^*, \times) \\ z & \mapsto & z^n \end{cases}$  étant un morphisme de groupes,  $\text{Ker } f = \mathbb{U}_n$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ . C'est aussi l'image du morphisme  $k \in \mathbb{Z} \mapsto e^{\frac{2ik\pi}{n}}$ .

**C Isomorphismes**

**Propriété 14 : Réciproque d'un isomorphisme**

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un isomorphisme de groupes.  
 Alors  $f^{-1}$  est un isomorphisme du groupe  $(G', \bullet)$  sur le groupe  $(G, \star)$ .

**Démonstration**

$f^{-1}$  est bijective, et si  $y, y' \in G'$ , alors, comme  $f$  est un morphisme de groupes,

$$f^{-1}(y \bullet y') = f^{-1}(f(f^{-1}(y)) \bullet f(f^{-1}(y'))) = f^{-1}(f(f^{-1}(y) \star f^{-1}(y'))) = f^{-1}(y) \star f^{-1}(y').$$

**Remarque**

R 13 – « Être isomorphe à » est une relation d'équivalence sur l'ensemble des groupes.



## 7 Groupes monogènes (MPI)

### a Sous-groupes engendré par une partie

#### Définition 7 : Groupe engendré par une partie

Soit  $(G, *)$  un groupe,  $A$  partie non vide de  $G$ .  
On appelle **sous-groupe engendré par  $A$**  le plus petit (au sens de l'inclusion) sous-groupe de  $G$  contenant  $A$ , noté  $\langle A \rangle$ .  
On dit alors que  $A$  est une **partie génératrice** de  $\langle A \rangle$ .

#### Remarque

R 14 – À mettre en parallèle avec la définition de Vect en algèbre linéaire.

#### Propriété 15 : Éléments de $\langle A \rangle$

Les éléments de  $\langle A \rangle$  sont exactement les produits (pour  $*$ ) d'éléments de  $A$  ou de  $A^{-1}$ .  
Autrement dit,  $x \in \langle A \rangle$  si et seulement s'il existe  $k \in \mathbb{N}$ ,  $(a_1, \dots, a_k) \in A^k$  et  $(\varepsilon_1, \dots, \varepsilon_k) \in \{-1, 1\}^k$  tel que

$$x = a_1^{\varepsilon_1} * \dots * a_k^{\varepsilon_k}.$$

#### Démonstration

On note  $H$  l'ensemble de tels éléments.  
On vérifie que  $H$  est un sous-groupe de  $(G, *)$  par caractérisation (partie non vide de  $G$  stable par  $*$  et par inverse).  
Puis tout sous-groupe de  $G$  contenant  $A$  contient nécessairement  $H$  par stabilité.  
Donc  $H$  est bien le plus petit sous-groupe de  $G$  contenant  $A$  :  $H = \langle A \rangle$ . ■

#### Remarque

R 15 – On a aussi que  $\langle A \rangle$  est l'intersection de tous les sous-groupes contenant  $A$  (car c'est un sous-groupe, contenant  $A$ , plus petit que tous les autres.)

#### Exemple

E 20 –  $\mathfrak{S}_n$  est engendré par les cycles.

(Toute permutation se décompose en produit de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.)

E 21 –  $\mathfrak{S}_n$  est engendré par les transpositions.

(Les cycles eux-mêmes se décomposent en produit de transpositions. Cette fois, il n'y a plus unicité de la décomposition, mais seulement de la parité du nombre de termes.)

E 22 – Soit  $\mathbb{K}$  un corps.  $\mathcal{GL}_n(\mathbb{K})$  est engendré par les matrices de transvection  $T_{i,j}(\lambda)$  (avec  $i \neq j$ ), de dilatation  $D_i(a)$  (avec  $a \neq 0$ ) et de permutation  $P_{i,j}$ .

(C'est une conséquence du pivot de Gauss : par opérations élémentaires, on peut transformer une matrice inversible en  $I_n$ .)

## b Groupes monogènes et cycliques

### Propriété 16 : Sous-groupe engendré par un élément

Soit  $a \in G$ . Le sous-groupe **engendré par**  $a$  noté  $\langle a \rangle$  plutôt que  $\langle \{a\} \rangle$  est

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

On dit que  $a$  en est un **générateur**.

#### Remarque

R 16 – En notation additive, on a  $\langle a \rangle = \{ka, k \in \mathbb{Z}\}$ .

### Définition 8 : Groupe monogène

Un groupe  $G$  est dit **monogène** s'il est engendré par un seul élément, c'est-à-dire s'il existe  $a \in G$  tel que  $G = \langle a \rangle$ .

Un groupe  $G$  est dite **cyclique** si et seulement s'il est monogène et fini.

#### Exemple

E 23 – Tout sous-groupe de  $(\mathbb{Z}, +)$  est monogène.

E 24 –  $(\mathbb{U}_n, \times)$  est cyclique engendré par  $e^{\frac{2i\pi}{n}}$ .

**Exercice 5 : Montrer que les générateurs de  $\mathbb{U}_n$  sont les  $e^{\frac{2ik\pi}{n}}$  avec  $k \wedge n = 1$ , appelées racines primitives  $n^{\text{e}}$  de l'unité.**

C'est une conséquence du théorème de Bézout.

En effet, si  $k \wedge n = 1$ , alors on a une relation de Bézout  $ku + nv = 1$  avec  $u, v \in \mathbb{Z}$ . Alors pour tout  $a \in \mathbb{Z}$ ,

$$e^{\frac{2ia\pi}{n}} = e^{\frac{2i(auk+nv)a\pi}{n}} = e^{\frac{2iauk\pi}{n}} = \left(e^{\frac{2ik\pi}{n}}\right)^{au}$$

donc  $\mathbb{U}_n = \langle e^{\frac{2ik\pi}{n}} \rangle$ .

Si, réciproquement,  $\mathbb{U}_n = \langle e^{\frac{2ik\pi}{n}} \rangle$ , alors on a  $a \in \mathbb{Z}$  tel que  $e^{\frac{2i\pi}{n}} = e^{\frac{2iak\pi}{n}}$  donc on a  $\ell \in \mathbb{Z}$  tel que  $1 = ak + n\ell$  donc  $n \wedge k = 1$  par théorème de Bézout.

#### Exemple : À observer sur un dessin

E 25 – Générateurs de  $\mathbb{U}_6$  et détails de la génération pour  $k = 5$  par exemple.

## c Ordre d'un élément dans un groupe

$(G, *)$  est un groupe d'élément neutre  $e$ .

### Définition 9 : Ordre d'un élément

On dit que  $a \in G$  est d'**ordre fini** s'il existe  $k \in \mathbb{N}^*$  tel que  $a^k = e$ .

Dans ce cas, on appelle **ordre de**  $a$  le plus petit  $k \in \mathbb{N}^*$  tel que  $a^k = e$ .

**Remarque**

R 17 –  $f : \begin{cases} \mathbb{Z} & \longrightarrow G \\ k & \longmapsto a^k \end{cases}$  est un morphisme de groupe donc son noyau est de la forme  $m\mathbb{Z}$  où  $m \in \mathbb{N}$ .

Soit  $m = 0$  et  $a$  n'est pas d'ordre fini (sa seule puissance égale à  $e$  est  $a^0$ .)

Soit  $m > 0$  et  $m$  est le plus petit élément  $> 0$  du noyau de  $f$  : il s'agit de l'ordre de  $a$ .

**Exemple : À observer sur un dessin**

E 26 – Dans  $\mathbb{U}_6$ ,  $e^{5i\pi/3}$  est d'ordre 6 et  $e^{2i\pi/3}$  est d'ordre 3.

**Exercice 6 : Sans calcul !**

Montrer que  $\begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$  est d'ordre fini.

**Exercice 7**

Caractériser dans  $(\mathbb{U}, \times)$  les  $e^{i\theta}$  qui sont d'ordre fini.

**Propriété 17 : de l'ordre d'un élément**

Soit  $a$  un élément de  $G$  d'ordre fini  $m$ .

- Si  $k \in \mathbb{Z}$ ,  $a^k = e$  si et seulement si  $k \in m\mathbb{Z}$  i.e.  $m$  divise  $k$ .
- $\langle a \rangle = \{a^k, k \in \llbracket 0, m-1 \rrbracket\}$  et  $|\langle a \rangle| = m$ .

**Démonstration**

■ Avec  $f : \begin{cases} \mathbb{Z} & \longrightarrow G \\ k & \longmapsto a^k \end{cases}$ ,  $\text{Ker } f = m\mathbb{Z}$  d'où le résultat.

■ On a déjà  $\{a^k, k \in \llbracket 0, m-1 \rrbracket\} \subset \langle a \rangle$ .

Puis, si  $k \in \mathbb{Z}$ , par division euclidienne, on a  $q, r \in \mathbb{Z}$  tel que  $k = mq + r$  avec  $0 \leq r \leq m-1$  et alors  $a^k = (a^m)^q * a^r = a^r$  d'où l'autre inclusion.

Puis, les termes sont deux à deux distincts car si  $a^k = a^\ell$  avec  $0 \leq k \leq \ell \leq m-1$ , alors  $a^{\ell-k} = e$  donc par minimalité de  $m$ ,  $k = \ell$ .

D'où le cardinal égal à  $m$ . ■

**Remarque**

R 18 – Ainsi,  $a^k = a^\ell$  peut se traduire par la congruence  $k \equiv \ell \pmod{m}$ .

**Exercice 8**

Soit  $(G, *)$  un groupe commutatif. On suppose que  $g_1$  et  $g_2$  sont d'ordres  $n_1$  et  $n_2$ .

1. On suppose  $n_1$  et  $n_2$  premiers entre eux. Montrer que  $g_1 * g_2$  est d'ordre fini et calculer cet ordre.
2. Si  $G = \mathcal{GL}_2(\mathbb{R})$ ,  $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  et  $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ , vérifier que  $A$  et  $B$  sont d'ordre fini, mais pas  $AB$ .
3. Si  $n_1$  et  $n_2$  ne sont pas premiers entre eux, montrer que  $g_1 * g_2$  n'est pas nécessairement d'ordre  $n_1 n_2$  ou  $n_1 \vee n_2$ .



4. ■ Si  $d_1$  est un diviseur de  $n_1$ , montrer qu'il existe un élément d'ordre  $d_1$  dans  $G$ .  
 ■ En déduire que  $G$  admet des éléments d'ordre  $n_1 \vee n_2$ .  
 ■ Si  $G$  est fini, montrer que  $G$  admet un élément d'ordre le ppcm de l'ordre des éléments de  $G$ .
1.  $(g_1 * g_2)^{n_1 n_2} = g_1^{n_1 n_2} g_2^{n_1 n_2} = e$  donc  $g_1 * g_2$  est d'ordre fini  $n | n_1 n_2$ .  
 On a  $g_1^n * g_2^n = e$  donc  $g_1^n = g_2^{-n}$  donc  $g_1^{n n_2} = g_2^{-n n_2} = e$  donc  $n_1 | n n_2$ .  
 Or  $n_1 \wedge n_2 = 1$  donc, par lemme de Gauß,  $n_1 | n$ . Par symétrie,  $n_2 | n$  aussi.  
 Et comme  $n_1 \wedge n_2 = 1$ ,  $n_1 n_2 | n$ .  
 Par positivité,  $n = n_1 n_2$ .
2.  $A^2 = -I_2$  donc  $A^4 = I_2$  et  $B^3 = I_2$ . Pour tout  $n \in \mathbb{N}^*$ ,  $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq 0_2$ .
3. Si  $g_1$  est d'ordre  $n_1 \geq 2$ , et  $g_1^{-1}$  est d'ordre  $n_1$  et  $g_1 * g_1^{-1} = e$  est d'ordre  $1 \notin \{n_1, n_1^2\} \dots$
4. ■  $n_1 = d_1 k_1$  et  $g_1^{k_1}$  est d'ordre  $d_1$ .  
 ■ On écrit les décompositions primaires :  $n_1 = p_1^{\alpha_1} \dots p_m^{\alpha_m}$  et  $n_2 = p_1^{\beta_1} \dots p_m^{\beta_m}$  avec des exposants éventuellement nuls. Puis,  $n_1 \wedge n_2 = p_1^{\max(\alpha_1, \beta_1)} \dots p_m^{\max(\alpha_m, \beta_m)}$ .  
 Avec la première partie de la question, on construit à partir de  $g_1$  ou de  $g_2$  des éléments d'ordre  $p_i^{\max(\alpha_i, \beta_i)}$ , puis avec la question 1, on obtient en les composant un élément d'ordre  $n_1 \wedge n_2$ .  
 ■ Si  $G$  est fini, on répond à la question en itérant le procédé précédent avec tous les éléments de  $G$  en remarquant que  $n_1 \vee \dots \vee n_k = (\dots((n_1 \vee n_2) \vee n_2) \dots)$ .

**Propriété 18 : Morphie des groupes monogènes**

Tout groupe monogène infini est isomorphe à  $(\mathbb{Z}, +)$ .  
 Tout groupe monogène fini (donc cyclique) de cardinal  $n$  est isomorphe à  $(\mathbb{U}_n, +)$

**Démonstration**

Si  $G$  est engendré par  $a$  et infini,  $f : \begin{matrix} (\mathbb{Z}, +) & \longrightarrow & (G, *) \\ k & \longmapsto & a^k \end{matrix}$  alors  $f$  est un morphisme de groupes surjectif car  $G = \langle a \rangle$ ,  
 et injectif car si  $k \in \text{Ker } f$ ,  $a^k = 1$  donc  $a$  d'ordre fini, donc  $G$  est fini.

Si  $G$  est engendré par  $a$  et de cardinal  $n$ , alors  $a$  est d'ordre  $n$ , donc  $a^n = e$ ,  $f : \begin{matrix} (\mathbb{U}_n, +) & \longrightarrow & (G, *) \\ e^{\frac{2ik\pi}{n}} & \longmapsto & a^k \end{matrix}$  est bien  
 définie (que l'on prenne  $k$  dans  $\mathbb{Z}$  ou dans  $\llbracket 0, n-1 \rrbracket$ , la valeur de  $a^k$  est la même car  $a^n = e$ ), est un morphisme de groupe et est surjectif, donc est un isomorphisme car  $n = |\mathbb{U}_n| = |G|$ . ■

**Propriété 19 : de l'ordre**

Soit  $(G, *)$  un groupe fini de neutre  $e$ .  
 (i) Tout élément de  $G$  est d'ordre fini.  
 (ii) L'ordre de tout élément de  $G$  divise le cardinal de  $G$ .  
 (iii) Pour tout  $a \in G$ ,  $a^{|G|} = e$ .

**Démonstration**

(i)  $\langle a \rangle$  est un sous-groupe de  $G$ , donc d'ordre fini. Donc on a  $i < j$  tel que  $a^i = a^j$  et  $a^{j-i} = e$  avec  $j - i \in \mathbb{N}^*$ .  
 (ii) L'ordre de  $a$  est la cardinal du sous-groupe  $\langle a \rangle$  de  $G$ , donc d'après le théorème de Lagrange (HP), il divise celui de  $G$ .  
 Seule la démonstration dans le cas commutatif est au programme.  
 En effet, dans ce cas, on considère le produit  $\left( \prod_{x \in G} x \right) \in G$  et on effectue le changement de variable (bijectif)  
 $x \mapsto a * x$ .  
 Par commutativité, on obtient  $\prod_{x \in G} x = \prod_{x \in G} (a * x) = a^{|G|} \prod_{x \in G} x$ . Comme  $\prod_{x \in G} x$  est régulier (car inversible), on en



déduit que  $a^{|G|} = e$ .

(iii) Conséquence du (ii).

### Exercice 9 : Quels sont les sous-groupes finis de $(\mathbb{C}^*, \times)$ ?

Soit  $G$  un sous-groupe fini de  $(\mathbb{C}^*, \times)$ . Tous ses éléments sont d'ordre fini, divisant l'ordre du groupe. Soit  $d = |G|$ . Tous les éléments de  $G$  vérifient  $z^d = 1$ . Donc  $G$  est inclus dans  $\mathbf{U}_d$ . Mais ils ont même cardinal, ils sont donc égaux.

## ANNEAUX ET CORPS

### 1 Anneaux (MP2I)

#### Définition 10 : Distributivité

Soit  $E$  un ensemble et  $\star$  et  $\top$  deux lois de composition interne sur  $E$ , on dit que  $\star$  est **distributive** sur  $\top$  lorsque  $\forall (x, y, z) \in E^3$ ,

$$x \star (y \top z) = (x \star y) \top (x \star z),$$

$$(y \top z) \star x = (y \star x) \top (z \star x).$$

#### Définition 11 : Anneau

On dit que  $(A, +, \times)$  est un **anneau** lorsque

- (i)  $(A, +)$  est un groupe abélien. L'élément neutre est noté  $0_A$ .
- (ii)  $\times$  est une loi de composition interne associative admettant un élément neutre appelé unité de  $A$ , noté  $1_A$ .
- (iii)  $\times$  est distributive sur  $+$ .

Lorsque, de plus,  $\times$  est commutative, on dit que  $(A, +, \times)$  est un **anneau commutatif**.

#### Exemple

**E 27** –  $(\mathbb{Z}, +, \times)$ ,  $(\mathbb{Q}, +, \times)$ ,  $(\mathbb{R}, +, \times)$ ,  $(\mathbb{C}, +, \times)$ ,  $(\mathbb{C}^D, +, \times)$  et  $(\mathbb{R}^D, +, \times)$  (avec  $D \neq \emptyset$ ),  $(\mathbb{C}^{\mathbb{N}}, +, \times)$  et  $(\mathbb{R}^{\mathbb{N}}, +, \times)$  sont des anneaux commutatifs.

**E 28** –  $(\mathcal{M}_n(\mathbb{R}), +, \times)$  et  $(\mathcal{M}_n(\mathbb{C}), +, \times)$  sont des anneaux non commutatifs si  $n \geq 2$ .

#### Remarque

**R 19** –  $0_A$  est **absorbant** :

$$\forall a \in A, \quad a \times 0_A = 0_A \times a = 0_A.$$

En effet,  $0_A = a \times (0_A + 0_A) = a \times 0_A + a \times 0_A$  donc  $a \times 0_A = 0_A$ . Idem à droite.

**R 20** – Si  $1_A = 0_A$ , alors pour tout  $a \in A$ ,  $a = a \times 1_A = a \times 0_A = 0_A$ , donc  $A = \{0_A\}$ .

**R 21** – Si  $A \neq \{0_1\}$ , alors  $0_A$  n'est pas inversible (pour  $\times$ ).

**R 22** – Pour tout  $a, b \in A$ ,  $-ab = (-a) \times b = a \times (-b)$ .

## 2 Groupe des inversibles (MP2I)

### Définition 12 : Inversibles d'un anneau

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

$a \in A$  est dit **inversible** si et seulement s'il est symétrisable pour  $\times$ .

Son symétrique est appelé **inverse** de  $a$ , noté  $a^{-1}$ .

On note  $U_A$  ou  $U(A)$  ou  $A^*$  l'ensemble des inversibles de  $A$ .

### Remarque

R23 – On parle parfois d'unités de  $A$ , d'où la notation...

### Exemple

E29 –  $U_{\mathbb{R}} = \mathbb{R}^*$

E30 –  $U_{\mathbb{Z}} = \{-1, 1\} \neq \mathbb{Z}^*$

E31 –  $U_{\mathbb{C}^{\mathbb{N}}} = \{\text{suites jamais nulles}\}$

E32 –  $U_{\mathbb{C}^D} = \{\text{fonctions jamais nulles}\}$

E33 –  $U_{\mathcal{M}_n(\mathbb{K})} = \mathcal{GL}_n(\mathbb{K})$

### Propriété 20 : Groupe des inversibles

Si  $(A, +, \times)$  anneau, alors  $(U_A, \times)$  est un groupe appelé **groupe des inversibles** de  $A$ .

### Démonstration

On a déjà l'associativité, l'élément neutre car  $A$  est un anneau. Comme de plus, tout élément inversible est lui-même inversible et comme le produit de deux éléments inversibles l'est encore, on a bien une structure de groupe. ■

## 3 Calculs dans un anneau (MP2I)

### Propriété 21 : Calculs dans un anneau

Soit  $(A, +, \times)$  un anneau. Soient  $a, b \in A$  et  $n \in \mathbb{N}$ .

■ Si  $a \times b = b \times a$ ,

$$(ab)^n = a^n b^n.$$

■ **Formule du binôme de Newton** : Si  $a \times b = b \times a$ ,

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

■ **Factorisation** <sup>□</sup> de  $a^n - b^n$  : Si  $a \times b = b \times a$

$$\begin{aligned} a^n - b^n &= (a-b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}) \\ &= (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}. \end{aligned}$$



- **Somme géométrique** : En particulier, pour tout  $x \in A$  ;

$$1_A - x^n = (1_A - x) \times \sum_{k=0}^{n-1} x^k$$

a. parfois appelée formule de Bernoulli

### Remarque

R24 – Si  $a$  et  $b$  ne commutent pas,

$$(ab)^n = abab \cdots ab$$

$$(a+b)^2 = a^2 + ab + ba + b^2$$

$$(a+b)^3 = a^3 + a^2b + aba + ba^2 + ab^2 + bab + b^2a + b^3$$

etc.

### Démonstration

- Par récurrence sur  $n$ .

- **Formule du binôme** :

- ★ **Preuve par dénombrement** :

$$(a+b)^n = \underbrace{(a+b)(a+b) \cdots (a+b)}_{n \text{ fois}}$$

En développant, on obtient des termes de la forme  $x_1 x_2 \cdots x_n$  avec  $x_i = a$  ou  $b$ . Si on veut  $k$  termes  $a$ , on  $\binom{n}{k}$  chois, et le terme vaut  $a^k b^{n-k}$  car  $a$  et  $b$  commutent.

- ★ **Preuve par récurrence** sur  $n$ , c'est simple si  $n = 0$  ou  $1$ . Si c'est vrai pour  $n-1$ ,

$$\begin{aligned} (a+b)^n &= (a+b)(a+b)^{n-1} = (a+b) \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-1-k} \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k} a^{k+1} b^{n-k-1} + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-k} \end{aligned}$$

(associativité, distributivité,  $a$  et  $b$  commutent, dans la seconde somme)

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

(changement d'indice  $k \mapsto k-1$ )

$$= \sum_{k=0}^n \binom{n-1}{k-1} a^k b^{n-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} a^k b^{n-k}$$

(les termes ajoutés sont nuls)

$$= \sum_{k=0}^n \left( \binom{n-1}{k-1} + \binom{n-1}{k} \right) a^k b^{n-k}$$

(associativité, distributivité,

Donc  $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$  d'après la formule de Pascal étendue au coefficients avec  $k < 0$ .

- **Factorisation de  $a^n - b^n$**  :

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

( $a$  et  $b$  commutent, associativité, distributivité)

$$= a^n b^0 - a^0 b^n = a^n - b^n$$

(somme télescopique)

## 4 Corps (MP2I)

### Définition 13 : Corps

Soit  $\mathbb{K}$  un ensemble,  $+$ ,  $\times$  deux lois de composition internes sur  $\mathbb{K}$ . On dit que  $(\mathbb{K}, +, \times)$  est un **corps** lorsque

- $(\mathbb{K}, +, \times)$  est un anneau commutatif.
- $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$  est non vide et tous ses éléments sont inversibles (c'est-à-dire  $\mathbb{K} \neq \{0_{\mathbb{K}}\}$  et  $U_{\mathbb{K}} = \mathbb{K}^{\times} = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$ .)

ou, de manière équivalente,

- $(\mathbb{K}, +)$  est un groupe abélien,
- $(\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \times)$  est un groupe,
- $\times$  est commutative et distributive sur  $+$ .

### Exemple

E 34 –  $\mathbb{R}, \mathbb{Q}, \mathbb{C}$  munis des lois  $+$  et  $\times$  sont des corps, mais pas  $\mathbb{Z}$ .



Voir exercice du TD : 28

## 5 Intégrité (MP2I)

### Définition 14 : Anneau intègre

Un anneau  $(A, +, \times)$  est dit **intègre** si

- $A$  est commutatif,
- $A \neq \{0_A\}$  c'est-à-dire  $1_A \neq 0_A$ ,
- $A$  n'admet aucun diviseur de zéro, c'est-à-dire

$$\forall a, b \in A, a \times b = 0_A \implies a = 0_A \text{ ou } b = 0_A.$$

### Exemple

E 35 –  $\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{Q}$  sont des anneaux intègres.  $\mathbb{R}^{\mathbb{N}}$  et plus généralement  $\mathbb{R}^D$  avec  $D$  contenant au moins deux éléments ne le sont pas.

### Propriété 22 : Généralisation

Soit  $(A, +, \times)$  un anneau intègre,  $n \in \mathbb{N}^*$  et  $(a_1, \dots, a_n) \in A^n$ .  
Si pour tout  $k \in \llbracket 1, n \rrbracket$ ,  $a_k \neq 0_A$ , alors  $a_1 \times \dots \times a_n \neq 0_A$ .

### Démonstration

Par contraposée et récurrence. ■

**Propriété 23 : Régularité dans un anneau intègre**

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

Tout élément non nul de  $A$  est régulier (ie simplifiable) pour  $\times$

**Démonstration**

Si  $a, b, c \in A$  et  $a \neq 0_A$  tels que  $ab = ac$ , alors  $a(b - c) = 0_A$  et donc  $b - c = 0_A$  soit  $b = c$ . ■

**Propriété 24 : Intégrité d'un corps**

Tout corps est un anneau commutatif intègre. La réciproque est fausse.

**Démonstration**

Si  $ab = 0_{\mathbb{K}}$  et si  $a \neq 0_{\mathbb{K}}$ , alors  $a$  est inversible et  $b = a^{-1}ab = a^{-1}0_{\mathbb{K}} = 0_{\mathbb{K}}$  car  $0_{\mathbb{K}}$  est un élément absorbant. Pour la réciproque,  $(\mathbb{Z}, +, \times)$  est un anneau commutatif intègre qui n'est pas un corps. ■



Voir exercice du TD : 22

## 6 Anneau produit (MPI)

**Propriété 25 : Anneau produit**

Soit  $(A, +, \times)$  et  $(B, \oplus, \otimes)$  des anneaux.

Pour tout  $(a, b)$  et  $(a', b')$  dans  $A \times B$ , on pose

$$(a, b) + (a', b') = (a + a', b \oplus b')$$

$$(a, b) \times (a', b') = (a \times a', b \otimes b')$$

Alors  $(A \times B, +, \times)$  a une structure d'anneau.

Si, de plus, les lois  $\times$  et  $\otimes$  sont commutatives, alors  $\times$  l'est.

**Démonstration**

- On a bien  $(A \times B, +)$  groupe (produit) abélien.
- $\times$  est bien une loi de composition interne sur  $A \times B$ .  
Un calcul facile mais pénible à écrire permet de vérifier que les associativités de  $\times$  et  $\otimes$  donnent celle de  $\times$ .  
Un calcul facile mais pénible à écrire permet de vérifier que les distributivités de  $\times$  sur  $+$  et  $\otimes$  sur  $\oplus$  donnent celle de  $\times$  sur  $+$ .
- Si  $1_A$  et  $1_B$  sont les unités de  $A$  et  $B$ , alors  $(1_A, 1_B)$  est bien neutre sur  $A \times B$ . ■

**Remarque**

R25 – Cela se généralise à un nombre d'anneaux quelconque  $(A_1, +, \times), \dots, (A_p, +, \times)$  avec pour tout  $(x_1, \dots, x_p)$

et  $(y_1, \dots, y_p)$  dans  $A_1 \times \dots \times A_p$ ,

$$(x_1, \dots, x_p) + (y_1, \dots, y_p) = \left( x_1 +_{(1)} y_1, \dots, x_p +_{(p)} y_p \right)$$

$$(x_1, \dots, x_p) \times (y_1, \dots, y_p) = \left( x_1 \times_{(1)} y_1, \dots, x_p \times_{(p)} y_p \right)$$

### Propriété 26 : Inversion dans un anneau produit

Si  $(A, +, \times)$  et  $(B, +, \times)$  sont deux anneaux, alors  $U_{A \times B} = U_A \times U_B$ .  
De plus, si  $(a, b) \in U_{A \times B}$ , alors

$$(a, b)^{-1} = (a^{-1}, b^{-1}).$$

#### Démonstration

$$\begin{aligned} (a, b) \in U_{A \times B} &\iff \exists (c, d) \in A \times B, (a, b) \times (c, d) = (c, d) \times (a, b) = (1_A, 1_B) \\ &\iff \exists (c, d) \in A \times B, ac = ca = 1_A \text{ et } bd = db = 1_B \\ &\iff (a, b) \in U_A \times U_B \end{aligned}$$

et on a bien alors  $(a, b)^{-1} = (a^{-1}, b^{-1})$ . ■

## 7 Sous-anneau et sous-corps (MP2I)

### Définition 15 : Sous-anneau

Soit  $(A, +, \times)$  un anneau. On dit que  $B$  est un **sous-anneau** de  $(A, +, \times)$  lorsque

- $B \subset A$
- **Important** :  $1_A \in B$
- $(B, +|_{B^2}, \times|_{B^2})$  est un anneau.

#### Remarque

**R 26** – Une partie peut avoir une structure d’anneau pour les lois induites sans avoir la même unité (ce n’est pas un sous-anneau au sens de la définition précédente.) C’est le cas trivialement de  $\{0_A\}$ .

#### Exemple

**E 36** – Soit, dans l’anneau des matrices  $2 \times 2$ , l’ensemble  $B$  des matrices  $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$  pour  $a \in \mathbb{K}$ . Alors  $(B, +, \times)$  est un anneau d’unité  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq I_2$ .

**Propriété 27 : Caractérisation des sous-anneaux**

$B$  est un sous-anneau de  $(A, +, \times)$  si et seulement si

$$\left\{ \begin{array}{l} B \subset A \\ (B, +) \text{ est un sous-groupe de } (A, +) \\ B \text{ est stable par } \times : \forall x, y \in B, x \times y \in B \\ 1_A \in B \end{array} \right.$$

ou, de manière équivalente,

$$\left\{ \begin{array}{l} B \subset A \\ 1_A \in B \\ \forall x, y \in B, x + y \in B, -x \in B \text{ et } x \times y \in B \end{array} \right.$$

ou encore

$$\left\{ \begin{array}{l} B \subset A \\ 1_A \in B \\ \forall x, y \in B, x - y \in B \text{ et } x \times y \in B \end{array} \right.$$

**Démonstration**

Même principe que pour les sous-groupes, la présence de  $1_A$  n'étant automatique que si  $B$  possède un élément inversible, d'où la nécessité d'imposer  $1_A \in B$ .

**Exemple**

E 37 – **Anneau des entiers de Gauss**<sup>a</sup> :  $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$  est un sous-anneau de  $(\mathbb{C}, +, \times)$ .

E 38 –  $\mathcal{F}_n^+(\mathbb{K})$  est un sous-anneau de  $(\mathcal{M}_n(\mathbb{K}), +, \times)$

E 39 – L'ensemble  $\mathcal{B}(\mathbb{R})$  des fonctions bornées est un sous-anneau de  $(\mathbb{R}^{\mathbb{R}}, +, \times)$ .

a.



**Carl Friedrich Gauss** (Brunswick 1777 - Göttingen 1855) est un mathématicien, astronome et physicien allemand. Surnommé *le prince des mathématiciens*, il est considéré comme l'un des plus grands mathématiciens de tous les temps. Gauss était un génie particulièrement précoce : à 7 ans (ou 10 selon les sources), il donne la formule calculant  $1 + 2 + \dots + 100$ . À 19 ans, il fut le premier à démontrer la loi de réciprocité quadratique. Parmi ses autres prouesses, on peut citer la démonstration du théorème fondamental de l'algèbre, dans sa thèse en 1799, l'invention de la théorie des congruences, la résolution de problèmes de construction à la règle et au compas... Il est considéré comme le fondateur de la géométrie différentielle.

**Définition 16 : Sous-corps**

Soit  $(\mathbb{K}, +, \times)$  un corps. On dit que  $(\mathbb{L}, +, \times)$  est un **sous-corps** de  $(\mathbb{K}, +, \times)$  lorsque  $\mathbb{L} \subset \mathbb{K}$  et  $(\mathbb{L}, +|_{\mathbb{L}}, \times|_{\mathbb{L}})$  est un corps.



**Propriété 28 : Caractérisation des sous-corps**

$(\mathbb{L}, +, \times)$  est un sous-corps de  $(\mathbb{K}, +, \times)$  si et seulement si

$$\begin{cases} \mathbb{L} \subset \mathbb{K} \\ (\mathbb{L}, +) \text{ est un sous-groupe de } (\mathbb{K}, +) \\ (\mathbb{L} \setminus \{0_{\mathbb{K}}\}, \times) \text{ est un sous-groupe de } (\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \times) \end{cases}$$

ou, de manière équivalente,

$$\begin{cases} \mathbb{L} \subset \mathbb{K} \\ \mathbb{L} \setminus \{0_{\mathbb{K}}\} \neq \emptyset \quad (1_{\mathbb{K}} \in \mathbb{L}) \\ \forall x, y \in \mathbb{L}, \quad x - y \in \mathbb{L} \\ \forall x, y \in \mathbb{L} \setminus \{0_{\mathbb{K}}\}, \quad xy^{-1} \in \mathbb{L} \end{cases}$$

**Démonstration**

Le sens  $\Rightarrow$  ne pose pas de problème. Pour le sens  $\Leftarrow$ , on a bien un sous-anneau dont tous les éléments non nuls sont inversibles car  $1_{\mathbb{K}} = xx^{-1} \in \mathbb{L}$ . ■



Voir exercice du TD : 23

## 8 Morphismes d'anneaux (MP2I)

**Définition 17 : Morphisme d'anneaux**

Soient  $(A, +, \times)$  et  $(A', \oplus, \otimes)$  deux anneaux.

$f: (A, +, \times) \rightarrow (A', \oplus, \otimes)$  est un **morphisme d'anneaux** si et seulement si

- (i)  $\forall (a, b) \in A^2, \quad f(a + b) = f(a) \oplus f(b)$   
(ie  $f: (A, +) \rightarrow (A', \oplus)$  morphisme de groupes)
- (ii)  $\forall (a, b) \in A^2, \quad f(a \times b) = f(a) \otimes f(b)$
- (iii)  $f(1_A) = 1_{A'}$

On parle aussi, d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** d'anneaux.

$\text{Ker } f = f^{(-1)}(\{0_{A'}\}) = \{a \in A \mid f(a) = 0_{A'}\}$  est le **noyau** de  $f$ .

$\text{Im } f = f(A) = \{f(x), x \in A\}$  est l'**image** de  $f$ .

**Remarque**

**R27** – Comme on a en particulier un morphisme de groupes additifs, on peut utiliser les propriétés de ceux-ci :

- $f(0_A) = 0_{A'}$ ,
- Pour tout  $a \in A, f(-a) = -f(a)$ ,
- $f$  est injective si et seulement si  $\text{Ker } f = \{0_A\}$ .

**R28** – En général,  $\text{Ker } f$  n'est pas un sous-anneau de  $A$ . C'est un sous-groupe additif stable par multiplication... Nous les étudions juste après !

**Exemple**

$$E40 - f : \begin{array}{l} \mathbb{R}[X] \longrightarrow \mathbb{C} \\ P \longrightarrow \tilde{P}(i) \end{array} ; \text{Ker } f = (X^2 + 1)\mathbb{R}[X] \text{ n'est pas un sous-anneau de } \mathbb{R}[X].$$

**Propriété 29 : des morphismes d'anneaux**

Soit  $f : (A, +, \times) \rightarrow (B, \oplus, \otimes)$  est un morphisme d'anneaux.

- (i) Si  $a$  est inversible dans  $A$ , alors  $f(a)$  l'est dans  $B$  et  $f(a^{-1}) = (f(a))^{-1}$ .
- (ii) Si  $f$  est un isomorphisme alors  $f^{-1} : (B, \oplus, \otimes) \rightarrow (A, +, \times)$  est aussi un isomorphisme d'anneau.
- (iii) Si  $g : (B, \oplus, \otimes) \rightarrow (C, \dot{+}, \dot{\times})$  est aussi un morphisme d'anneau, alors  $g \circ f : (A, +, \times) \rightarrow (C, \dot{+}, \dot{\times})$  l'est encore.

**Démonstration**

- (i)  $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_{A'}$  et de même  $f(a^{-1})f(a) = 1_{A'}$ .
- (ii) Même principe que pour les morphismes de groupes.
- (iii) Simple vérification. ■

**Définition 18 : Morphisme de corps**

Soient  $(\mathbb{K}, +, \times)$  et  $(\mathbb{K}', \oplus, \otimes)$  deux corps.

$f : (\mathbb{K}, +, \times) \rightarrow (\mathbb{K}', \oplus, \otimes)$  est un **morphisme de corps** si et seulement si il s'agit d'un morphisme d'anneaux.

**Remarque**

R29 – Avec (i) et (ii),  $f(1_{\mathbb{K}}) = (f(1_{\mathbb{K}}))^2$  et comme  $\mathbb{K}'$  est intègre,  $f(1_{\mathbb{K}})$  vaut  $1_{\mathbb{K}'}$  ou  $0_{\mathbb{K}'}$ . S'il vaut  $0_{\mathbb{K}'}$  et si (ii) est vérifiée, alors  $f \equiv 0_{\mathbb{K}'}$ .

**Exemple**

E41 –  $\text{id}_{\mathbb{C}}, z \mapsto \bar{z}$  sont des automorphismes (involutifs) du corps  $\mathbb{C}$ .

E42 – Tout morphisme de corps est injectif, car si  $x \neq 0_{\mathbb{K}}$ ,  $x$  est inversible donc  $f(x)$  est inversible, donc  $f(x) \neq 0_{\mathbb{K}'}$  donc  $x \notin \text{Ker } f$ , donc  $\text{Ker } f = \{0_{\mathbb{K}}\}$ .



Voir exercice du TD : 25 à 27, 31

**IDÉAL D'UN ANNEAU COMMUTATIF (MPI)****1 Généralités****Définition 19 : Idéal**

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

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

**Remarque**

**R30** – Finalement,  $I$  est un **idéal** de  $(A, +, \times)$  lorsque

- $I \subset A$
- $I \neq \emptyset$
- $\forall x, y \in I, x - y \in I$
- $\forall a \in A, \forall x \in I, ax \in I$ .

Comme  $-1_A \in A$ , on peut se contenter de

- $I \subset A$
- $I \neq \emptyset$
- $\forall x, y \in I, x + y \in I$
- $\forall a \in A, \forall x \in I, ax \in I$ .

**Exemple**

**E43** –  $2\mathbb{Z}$  est un idéal de  $(\mathbb{Z}, +, \times)$ .

**E44** – L'ensemble des suites convergant vers 0 est un idéal de l'anneau des suites bornées.

**Remarque**

**R31** – Si un idéal contient l'unité  $1_A$  ou plus généralement un élément inversible, il est égal à  $A$  tout entier.

**Propriété 30 : Idéaux triviaux**

Soit  $(A, +, \times)$  un anneau commutatif.  $\{0_A\}$  et  $A$  sont des idéaux (triviaux) de  $(A, +, \times)$ .  
Ce sont les seuls idéaux si de plus  $(A, +, \times)$  est un corps.

**Démonstration**

Simple vérification. Dans le cas d'un corps, comme tous les éléments non nuls sont inversibles, s'il y en a un dans  $I$ , en le multipliant par son inverse on obtient  $1_A \in I$  puis  $I = A$ . ■

**Propriété 31 : Noyau d'un morphisme d'anneaux**

Soit  $f : (A, +, \times) \rightarrow (A', \oplus, \otimes)$  un morphisme d'anneaux. Alors  $\text{Ker } f$  est un idéal de  $(A, +, \times)$ .

**Démonstration**

- $0_A \in \text{Ker } f \neq \emptyset$
- Si  $x, y \in \text{Ker } f, f(x - y) = f(x) - f(y) = 0_{A'}$  donc  $x - y \in \text{Ker } f$ .
- Si  $x \in \text{Ker } f$  et  $a \in A, f(ax) = f(a)f(x) = 0_{A'}$  donc  $ax \in \text{Ker } f$ .

**Remarque**

**R32** –  $\text{Im } f$  est un sous-anneau de  $(A', \oplus, \otimes)$ .

En général,  $\text{Ker } A$  n'est pas un sous-anneau de  $(A, +, \times)$ .

**Exercice 10**

Montrer que si  $f : (A, +, \times) \rightarrow (A', \oplus, \otimes)$  est un morphisme d'anneaux :

- L'image réciproque d'un sous-anneau de  $(A', \oplus, \otimes)$  est un sous-anneau de  $(A, +, \times)$ .
- L'image directe d'un sous-anneau de  $(A, +, \times)$  est un sous-anneau de  $(A', \oplus, \otimes)$ .
- L'image réciproque d'un idéal de  $(A', \oplus, \otimes)$  par  $f$  est un idéal de  $(A, +, \times)$ .
- L'image directe d'un idéal de  $(A, +, \times)$  par  $f$  est un idéal de  $(f(A) = \text{Im } f, \oplus, \otimes)$ .



Voir exercice du TD : 17 à 21, 29, 30

## 2 Somme et intersection d'idéaux

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

### Propriété 32 : Somme et intersection d'idéaux

(i) Soient  $I_1, \dots, I_n$  des idéaux de  $(A, +, \times)$ . On note

$$I_1 + \dots + I_n = \{x_1 + \dots + x_n, \forall j \in \llbracket 1, n \rrbracket, x_j \in I_j\}$$

Il s'agit d'un idéal de  $(A, +, \times)$ .

Il s'agit plus précisément du plus petit idéal de  $(A, +, \times)$  (au sens de l'inclusion) contenant tous les idéaux  $I_j$  pour  $1 \leq j \leq n$ .

(ii) Soient  $(I_j)_{j \in J}$  une famille d'idéaux de  $(A, +, \times)$ .

Alors  $\bigcap_{j \in J} I_j$  est un idéal de  $(A, +, \times)$ .

Il s'agit du plus grand idéal de  $(A, +, \times)$  (au sens de l'inclusion) contenu dans les idéaux  $I$  et  $J$ .

### Démonstration

(i) ■  $I_1 + \dots + I_n$  est un idéal :

★  $0_A = 0_A + \dots + 0_A \in I_1 + \dots + I_n$

★ Si  $x, y \in I_1 + \dots + I_n$ , on a  $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \prod_{j=1}^n I_j$  tels que  $x = x_1 + \dots + x_n$  et  $y = y_1 + \dots + y_n$ .

Alors  $x + y = (x_1 + y_1) + \dots + (x_n + y_n) \in I_1 + \dots + I_n$ .

★ Si  $x = x_1 + \dots + x_n \in I_1 + \dots + I_n$  et  $a \in A$  alors  $ax = ax_1 + \dots + ax_n \in I_1 + \dots + I_n$ .

■  $I_1 + \dots + I_n$  contient tous les  $I_j$  car ceux-ci contiennent  $0_A$ .

■ Si  $K$  est un idéal de  $A$  contenant tous les  $I_j$ , alors par stabilité par  $+$ ,  $I_1 + \dots + I_n \subset K$ .

(ii) ■  $\bigcap_{j \in J} I_j$  est un idéal :

★  $0_A \in \bigcap_{j \in J} I_j$

★ Si  $x, y \in \bigcap_{j \in J} I_j$ ,  $x + y \in \bigcap_{j \in J} I_j$ .

★ Si  $x \in \bigcap_{j \in J} I_j$  et  $a \in A$  alors  $ax \in \bigcap_{j \in J} I_j$ .

■  $\bigcap_{j \in J} I_j$  est contenu dans tous les  $I_j$ .

■ Si  $K$  est un idéal de  $A$  contenu dans tous les  $I_j$ , alors  $K \subset \bigcap_{j \in J} I_j$ .

### 3 Idéal principal

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

#### Propriété 33 : Idéal engendré par un élément

Soit  $x \in A$ . On note

$$(x) = xA = \{xa, a \in A\}.$$

C'est un idéal de  $A$ , appelé **idéal engendré** par  $x$ .

#### Remarque

**R33** – C'est aussi le plus petit idéal contenant  $x$ , et donc l'intersection de tous les idéaux contenant  $x$  par unicité du plus petit élément.

Cette notion se généralise à plus d'un élément, un peu comme avec les Vect en algèbre linéaire.

Ainsi, l'idéal engendré par un nombre quelconque d'éléments est l'ensemble des combinaisons linéaires (finies) de ces éléments, à coefficients dans  $A$ .

#### Définition 20 : Idéal et anneau principal (HP)

- Tout idéal de la forme  $xA$  (donc engendré par un seul élément) est dit **principal**.
- Un anneau commutatif est dit **principal** lorsque
  - (i) C'est un anneau intègre.
  - (ii) Tous ses idéaux sont principaux.

#### Théorème 1 : Principauté de $\mathbb{Z}$

L'anneau  $\mathbb{Z}$  est principal.

#### Démonstration

C'est un anneau intègre et ses idéaux qui sont aussi ses sous-groupes sont tous principaux. ■

#### Remarque

**R34** – Les idéaux de  $\mathbb{Z}$  sont donc principaux, c'est-à-dire engendré par un élément. Tous les générateurs sont associés.

Donc, quitte à choisir un générateur positif (ou nul), on a de plus unicité de celui-ci.

### 4 Divisibilité dans un anneau intègre

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

#### Définition 21 : Divisibilité

Soient  $a, b \in A$ .

On dit que  $b$  **divise**  $a$  ou que  $a$  est multiple de  $b$  lorsqu'il existe  $q \in A$  tel que  $a = bq$ . On note  $b|a$ .

$a$  et  $b$  sont dit associés lorsque  $a|b$  et  $b|a$ .

**Propriété 34 : Caractérisation avec les idéaux**

Soient  $a, b \in A$ .  
 $b$  divise  $a$  si et seulement si  $a \in bA$  si et seulement si  $aA \subset bA$ .

**Remarque**

R 35 – Soit encore ssi tous les multiples de  $a$  sont des multiples de  $b$ .

**Propriété 35 : Éléments associés**

On rappelle que  $(A, +, \times)$  est un anneau commutatif **intègre**. Soient  $a, b \in A$ .  
 $a$  et  $b$  sont associés si et seulement si  $aA = bA$  si et seulement s'il existe  $u \in U_A$  tel que  $b = ua$ .

**Exemple**

E 45 – Dans  $\mathbb{Z}$ ,  $a, b$  sont associés si et seulement si  $a = \pm b$ .

## IV ARITHMÉTIQUE SUR $\mathbb{Z}$ (MP2I)

### 1 PGCD

**Définition 22 : PGCD**

Soient  $a, b \in \mathbb{Z}$ .

$I = (a) + (b) = a\mathbb{Z} + b\mathbb{Z} = \{au + bv, u, v \in \mathbb{Z}\}$  est un idéal non réduit à  $\{0\}$  de  $(\mathbb{Z}, +, \times)$  qui est un anneau principal.

Son unique générateur positif est appelé **pgcd de  $a$  et  $b$** , noté  $a \wedge b$ .

On a donc, par définition,  $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ .

**Propriété 36 : Relation de Bézout**

Si  $a, b \in \mathbb{Z}$ , on peut trouver  $a, b \in \mathbb{Z}$  tels que  $au + bv = a \wedge b$ .

**Démonstration**

Immédiat avec la nouvelle définition. ■

**Propriété 37 : Caractérisation**

Soit  $(a, b) \in \mathbb{Z}^2$ .

$$d = a \wedge b \iff \begin{cases} d \in \mathbb{N} \\ d|a \text{ et } d|b \\ \forall c \in \mathbb{Z}, (c|a \text{ et } c|b) \implies c|d \end{cases}$$

Il s'agit donc du plus grand diviseur positif au sens de la division.

Par conséquent, les diviseurs de  $a \wedge b$  sont exactement les diviseurs communs de  $a$  et de  $b$ .

**Démonstration**

Soit  $d = a \wedge b$ . Alors, par définition,  $d \in \mathbb{N}$  et  $a \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ ,  $b \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ .  
 Soit  $c \in \mathbb{Z}$  tel que  $c|a$  et  $c|b$  alors, avec une relation de Bézout,  $c|d = au + bv$ .

Réciproquement, soit  $d$  tel que  $\begin{cases} d \in \mathbb{N} \\ d|a \text{ et } d|b \\ \forall c \in \mathbb{Z}, (c|a \text{ et } c|b) \implies c|d \end{cases}$

Alors, avec le premier sens,  $a \wedge b|d$  et  $d|a \wedge b$  et donc, par positivité,  $d = a \wedge b$ . ■

**Propriété 38 : Propriété d'Euclide**

Si  $a, b, q \in \mathbb{Z}$ ,  $a \wedge b = (a - bq) \wedge b$  (pas nécessairement une division euclidienne).

**Démonstration**

Les diviseurs communs sont les mêmes. ■



Voir exercice du TD : 34

**Définition 23 : Nombre entiers premiers entre eux**

$a, b \in \mathbb{Z}$  sont dits **premiers entre eux** lorsque  $a \wedge b = 1$ , c'est-à-dire lorsque les seuls diviseurs communs  $\pm 1$ .

**Théorème 2 : de Bézout**

Soit  $a, b \in \mathbb{Z}$ .

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z}, au + bv = 1$$

**Démonstration**

Le sens direct a déjà été vu.

Réciproquement, si  $au + bv = 1$ , alors  $1 \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$  donc  $1|a \wedge b$  donc  $a \wedge b = 1$  par positivité. ■

**Corollaire 5**

Soient  $a, b, c \in \mathbb{Z}$ .

(i)  $a \wedge bc = 1 \iff a \wedge b = a \wedge c = 1$

(ii) Si  $d = a \wedge b$ , on a  $a', b' \in \mathbb{Z}$  tels que  $a = da'$ ,  $b = db'$  et  $a' \wedge b' = 1$ .

**Démonstration**

(i) Sens direct immédiat par Bézout. Sens réciproque : il suffit de multiplier les relations de Bézout. Voir CCINP 86.

(ii) Si  $d \neq 0$ , comme  $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ , on obtient  $\mathbb{Z} = a'\mathbb{Z} + b'\mathbb{Z}$  donc  $a' \wedge b' = 1$ . Sinon, tout couples  $(a', b')$  convient, donc... ■

**Théorème 3 : Lemme de Gauß**

Soient  $a, b, c \in \mathbb{Z}$ . Si  $a|bc$  et  $a \wedge b = 1$ , alors  $a|c$ .

**Démonstration**

On a  $u, v \in \mathbb{Z}$  tels que  $au + bv = 1$  donc  $c = acu + bcv$  est divisible par  $b$ .



Voir exercice du TD : 41, 47

**Méthode 1 : résolution des équations diophantiennes  $ax + by = c$** 

où  $a, b, c \in \mathbb{Z}^*$  sont fixés, on cherche les solutions entières.

On a facilement qu'il y a des solutions si et seulement si  $d = a \wedge b | c$ .

Lorsque  $c$  est le cas, on peut trouver une solution particulière  $(x_0, y_0)$  avec l'algorithme d'Euclide par exemple.

Alors, si  $(x, y)$  solution,  $ax + by = ax_0 + by_0$  puis  $a(x - x_0) = b(y_0 - y)$  donc  $a'(x - x_0) = b'(y_0 - y)$  avec  $a' \wedge b' = 1$  en divisant par  $d$ .

Par lemme de Gauß, on a  $k \in \mathbb{Z}$  tel que  $x = x_0 + b'k$  puis en réinjectant  $y = y_0 - a'k$ .

On vérifie enfin que la réciproque étant vraie. Ensemble des solutions :

$$\{(x_0 + b'k, y_0 - a'k), k \in \mathbb{Z}\}.$$

**Exercice 11 : Résoudre  $199x + 54y = 4$  dans  $\mathbb{Z}^2$ .**

Ici, par l'algorithme d'Euclide, on a

$$(1) 199 = 54 \times 3 + 37$$

$$(2) 54 = 37 \times 1 + 17$$

$$(3) 37 = 17 \times 2 + 3$$

$$(4) 17 = 3 \times 5 + 2$$

$$(5) 3 = 2 \times 1 + 1$$

Donc  $199 \wedge 54 = 1$  et  $(5) - (4) + 6(3) - 13(2) + 19(1)$  donne  $199 \times 19 - 54 \times 70 = 1$ .

On a donc comme solution particulière  $x_0 = 76$  et  $y_0 = -280$ .

Comme ci-dessus, on a ensuite  $(x, y)$  est solution de  $(E)$  si et seulement si  $199(x - x_0) + 54(y - y_0) = 0$  si et seulement si  $199(x - x_0) = 54(y_0 - y)$ . Comme  $199 \wedge 54 = 1$  et  $199 | 54(y_0 - y)$ , le théorème de Gauß donne alors  $k \in \mathbb{Z}$  tel que  $y_0 - y = 199k$  soit  $y = -280 - 199k$ . Puis, en remplaçant dans l'équation,  $x = x_0 + 54k = 76 + 54k$ . On vérifie aisément que la réciproque est vraie.

L'ensemble des solutions est donc  $\{(76 + 54k, -280 - 199k) \mid k \in \mathbb{Z}\}$ .



Voir exercice du TD : 33

**2 PPCM****Définition 24 : PPCM**

Le PPCM de deux entiers  $a, b$  est l'unique générateur positif  $a \vee b$  de l'idéal  $a\mathbb{Z} \cap b\mathbb{Z}$  des multiples communs à  $a$  et à  $b$ .

On a donc  $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$ .

**Remarque**

R 36 – Cette fois, il s'agit clairement de la même définition qu'en première année : le plus petit multiple commun positif.



**Propriété 39 : du PPCM**

- (i) Il s'agit du plus petit multiple positif commun à  $a$  et à  $b$  au sens de la division.  
 (ii) On a toujours que  $|ab| = (a \wedge b)(a \vee b)$ .

**3 Nombres premiers****Définition 25 : Nombre premier**

Un **nombre premier** est un entier naturel  $p \geq 2$  dont les seuls diviseurs positifs sont 1 et  $p$ .  
 On notera  $\mathcal{P}$  l'ensemble des nombres premiers.

**Remarque**

R 37 – 1 n'est pas premier.

R 38 – 2 est le seul nombre premier pair.

R 39 – Un nombre premier possède exactement 4 diviseurs :  $\pm 1$  et  $\pm p$ .

R 40 – Pour qu'un nombre entier  $n$  soit premier, il faut et il suffit qu'il n'ait pas de diviseur entre 2 et  $\sqrt{n}$ .



Voir exercice du TD : 35, 36, 38, 40, 44

**Propriété 40 : d'Euclide**

L'ensemble des nombres premiers est infini.

**Démonstration : tellement classique...**

Sinon, soient  $p_1, \dots, p_n$  les nombres premiers.

Alors  $N = p_1 \cdots p_n + 1$  n'aurait pas de diviseur premier... (Alors qu'il doit en avoir un, le plus petit  $\geq 2$ , par exemple.)



Voir exercice du TD : 37

**Propriété 41 : Diviseur premier ou non**

Si  $p \in \mathcal{P}$  et  $n \in \mathbb{Z}$ , alors  $p|n$  ou (exclusif)  $p \wedge n = 1$ .

**Démonstration**

Si  $p \wedge n$  divise  $p$  donc vaut soit 1 soit  $p$ ...

**Corollaire 6 : Nombre premier divisant un produit**

Soient  $p \in \mathcal{P}$  et  $a_1, \dots, a_n \in \mathbb{Z}$ .

$p|(a_1 \times \cdots \times a_n)$  si et seulement si  $p$  divise l'un des  $a_k$ .

**Théorème 4 : fondamental de l'arithmétique – Décomposition primaire**

Soit  $n \in \mathbb{Z}^*$ . On peut trouver  $k \in \mathbb{N}$ ,  $p_1, \dots, p_k$  premiers deux à deux distincts,  $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$  tels que

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

appelée décomposition primaire de  $n$ .

De plus, cette écriture est unique à l'ordre des facteurs près.

$p_1, \dots, p_k$  sont les diviseurs premiers de  $n$ .

**Définition 26 : Valuation  $p$ -adique**

Soit  $p \in \mathcal{P}$  et  $n \in \mathbb{Z}^*$ . On appelle **valuation  $p$ -adique** de  $n$  l'entier

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

**Remarque**

**R41** – La décomposition primaire se réécrit  $n = \pm \prod_{p \in \mathcal{P}, p|n} p^{v_p(n)} = \pm \prod_{p \in \mathcal{P}} p^{v_p(n)}$ .

**Propriété 42 : des valuations  $p$ -adiques**

Soient  $n, m \in \mathbb{Z}^*$ ,  $p \in \mathcal{P}$ .

- (i)  $v_p(n) \neq 0 \iff p|n$
- (ii)  $v_p(n \times m) = v_p(n) + v_p(m)$
- (iii)  $n|m \iff \forall p \in \mathcal{P}, v_p(n) \leq v_p(m)$
- (iv)  $v_p(n \wedge m) = \min(v_p(n), v_p(m))$  et  $v_p(n \vee m) = \max(v_p(n), v_p(m))$

**Remarque**

**R42** – Si  $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  et  $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$  avec des exposants éventuellement nuls, alors

$$a \wedge b = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}$$

$$a \vee b = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$$

**Exercice 12 : Montrer que  $\sqrt{n} \in \mathbb{Q}$  si et seulement si  $n$  est un carré parfait.**

Si  $\sqrt{n} = \frac{a}{b}$ , alors  $a^2 = n \times b^2$ ,  $\forall p \in \mathcal{P}$ ,  $2v_p(a) = v_p(n) + 2v_p(b)$  donc  $\forall p \in \mathcal{P}$ ,  $v_p(n) \in 2\mathbb{N}$ , donc  $n$  est un carré parfait.

Ou encore : si  $\sqrt{n} = \frac{a}{b}$  sous forme irréductible, alors  $a^2 = n \times b^2$  donc  $b^2 | a^2$ . Or  $a \wedge b = 1$  donc  $b^2 = a^2 \wedge b^2 = 1$  donc  $n = a^2$ .

**Exercice 13 : Exprimer le nombre de diviseurs positifs de  $n$  à l'aide de ses valuations  $p$ -adiques.**

Il s'agit de  $\prod_{p \in \mathcal{P}, p|n} (v_p(n) + 1)$  vu la propriété (iii).



Voir exercice du TD : 39

## 4 Congruences

### Définition 27 : Congruence

Soit  $n \in \mathbb{N}^*$ . On dit que  $a, b \in \mathbb{Z}$  sont **congrus modulo**  $n$  et on note  $a \equiv b [n]$  lorsque  $n|(a-b)$  ie lorsqu'il existe  $k \in \mathbb{Z}$  tel que  $a = b + kn$ .

### Propriété 43 : Relation d'équivalence

*C'est une relation d'équivalence sur  $\mathbb{Z}$ .*

### Propriété 44 : Nombre d'entiers modulo $n$

$\forall a \in \mathbb{Z}, \exists ! r \in \llbracket 0, n-1 \rrbracket, a \equiv r [n]$ .  $r$  est le reste de la division euclidienne de  $k$  par  $n$ .  
Ainsi, la relation d'équivalence  $\equiv [n]$  possède exactement  $n$  classes d'équivalences.

#### Remarque

**R43** – On étudiera plus tard dans l'année l'ensemble  $\mathbb{Z}/n\mathbb{Z}$  des classes d'équivalences pour cette relation : les entiers modulo  $n$ .

### Propriété 45 : Compatibilité de $+$ et $\times$

Soient  $n \in \mathbb{N}^*$  et  $a, b, c, d \in \mathbb{Z}$  tels que  $a \equiv b [n]$  et  $c \equiv d [n]$ . Alors  $a + c \equiv b + d [n]$  et  $a \times c \equiv b \times d [n]$ .  
Plus généralement, si  $m \in \mathbb{N}$ ,  $a^m \equiv b^m [n]$ .

#### Remarque

**R44** – Ce qui dotera  $\mathbb{Z}/n\mathbb{Z}$  d'une structure d'anneau.

#### Remarque

**R45** – Les règles de divisibilité par 2, 3, 4, 5, 8, 9, 11 sont à connaître.

### Propriété 46 : Petit théorème de Fermat

Si  $p$  est premier et  $a \in \mathbb{Z}^*$  non divisible par  $p$ , alors

$$a^{p-1} \equiv 1 [p].$$

Dans tous les cas (que  $a$  soit divisible ou non par  $p$ ),

$$a^p \equiv a [p].$$

### Exercice 14 : CCINP 86

**Théorème 5 : de Fermat-Wiles, ou grand théorème de Fermat**

Si  $n \in \mathbb{N}$  tel que  $n \geq 3$ , alors l'équation

$$x^n + y^n = z^n$$

n'admet aucune solution dans  $\mathbb{N}_*^3$ .

Démonstration : Non exigible<sup>1</sup>



Voir exercice du TD : 42, 43, 45, 46

## V STRUCTURE D'ALGÈBRE (MPI)

### 1 Algèbre et sous-algèbre

**Définition 28 : Structure d'algèbre**

On dit que  $(\mathcal{A}, +, \times, \cdot)$  est une  $\mathbb{K}$ -algèbre lorsque

- $(\mathcal{A}, +, \cdot)$  est un  $\mathbb{K}$ -espace vectoriel,
- $(\mathcal{A}, +, \times)$  est un anneau,
- Pseudo-associativité :  $\forall \lambda \in \mathbb{K}, \forall x, y \in \mathcal{A},$

$$\lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y).$$

**Exemple**

E46 –  $(\mathbb{C}, +, \times, \cdot)$  est une  $\mathbb{R}$ -algèbre et une  $\mathbb{C}$ -algèbre.

E47 –  $(\mathbb{K}^X, +, \times, \cdot)$  est une  $\mathbb{K}$ -algèbre.

E48 –  $(\mathbb{K}^{\mathbb{N}}, +, \times, \cdot)$  est une  $\mathbb{K}$ -algèbre.

E49 –  $(\mathbb{K}[X], +, \times, \cdot)$  est une  $\mathbb{K}$ -algèbre.

E50 –  $(\mathbb{K}(X), +, \times, \cdot)$  est une  $\mathbb{K}$ -algèbre.

E51 – Si  $E$  est un  $\mathbb{K}$ -espace vectoriel,  $(\mathcal{L}(E), +, \circ, \cdot)$  est une  $\mathbb{K}$ -algèbre.

E52 – Si  $n \in \mathbb{N}^*$ ,  $(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$  est une  $\mathbb{K}$ -algèbre.

On a aussi une notion de sous-algèbre : c'est simultanément un sous-espace vectoriel et un sous-anneau, donc stable par combinaisons linéaires et par produit et contenant l'unité.

**Propriété 47 : Caractérisation des sous-algèbres**

Soit  $(\mathcal{A}, +, \times, \cdot)$  est une  $\mathbb{K}$ -algèbre.  $\mathcal{B}$  est une sous-algèbre de  $(\mathcal{A}, +, \times, \cdot)$  lorsque

- (i)  $\mathcal{B} \subset \mathcal{A}$
- (ii)  $1_{\mathcal{A}} \in \mathcal{B}$
- (iii)  $\forall x, y \in \mathcal{B}, \forall \lambda \in \mathbb{K}, x + \lambda y \in \mathcal{B}$
- (iv)  $\forall x, y \in \mathcal{B}, \forall \lambda \in \mathbb{K}, x \times y \in \mathcal{B}$

1. J'ai découvert une démonstration véritablement merveilleuse que ce cadre est trop étroit pour contenir...

**Exemple**

- E53 –  $\mathbb{K}[X]$  est une sous-algèbre de  $\mathbb{K}(X)$ .
- E54 –  $\mathcal{C}^k(I, \mathbb{K})$  est une sous-algèbre de  $\mathbb{K}^I$ .
- E55 – L'ensemble des suites convergentes est une sous-algèbre de  $\mathbb{K}^{\mathbb{N}}$ .
- E56 – L'ensemble  $\mathbb{K}[x]$  des fonctions polynomiales est une sous-algèbre de  $\mathbb{K}^{\mathbb{K}}$ .

L'intérêt principal des algèbres est de pouvoir évaluer un polynôme à coefficients dans  $\mathbb{K}$  en un élément d'une  $\mathbb{K}$ -algèbre :

**Définition 29 : Polynôme en un élément d'une algèbre**

Si  $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{K}[X]$  et  $x \in \mathcal{A}$ , on pose

$$P(x) = \sum_{k=0}^n a_k x^k = a_0 1_{\mathcal{A}} + a_1 x + \dots + a_n x^n.$$

Attention à ne pas oublier l'unité de  $\mathcal{A}$  !

## 2 Morphismes d'algèbres

**Définition 30 : Morphisme d'algèbre**

Soit  $(\mathcal{A}, +, \times, \cdot)$ ,  $(\mathcal{B}, +, \times, \cdot)$  et  $f : \mathcal{A} \rightarrow \mathcal{B}$ . On dit que  $f$  est un **morphisme d'algèbres** lorsque

(i)  $f$  est linéaire ie

$$\forall x, y \in \mathcal{A}, \forall \lambda \in \mathbb{K}, f(x + \lambda y) = f(x) + \lambda f(y)$$

(ii)  $\forall x, y \in \mathcal{A}, f(x \times y) = f(x) \times f(y)$

(iii)  $f(1_{\mathcal{A}}) = 1_{\mathcal{B}}$ .

**Exemple**

E57 – Si  $X \neq \emptyset$ ,  $\mathcal{A}$  une  $\mathbb{K}$ -algèbre,  $a \in X$ ,  $u_a : \begin{array}{l} \mathcal{A}^X \rightarrow \mathcal{A} \\ f \mapsto f(a) \end{array}$  est un morphisme de  $\mathbb{K}$ -algèbres. (morphisme d'évaluation).

E58 –  $f : \begin{array}{l} \mathbb{K}[X] \rightarrow \mathbb{K}[x] \\ P \mapsto \tilde{P} \end{array}$  est un isomorphisme d'algèbre si  $\mathbb{K}$  est infini, et  $g : \begin{array}{l} \mathbb{K}[X] \rightarrow \mathbb{K}(X) \\ P \mapsto \frac{P}{1} \end{array}$  est un morphisme d'algèbres injectif.

**Propriété 48 : Morphisme d'évaluation polynomiale**

Soit  $(\mathcal{A}, +, \times, \cdot)$  une  $\mathbb{K}$ -algèbre et  $x \in \mathcal{A}$ .

Alors l'application  $f : \begin{array}{l} \mathbb{K}[X] \rightarrow \mathcal{A} \\ P \mapsto P(x) \end{array}$  est un morphisme de  $\mathbb{K}$ -algèbres.

**Démonstration**

Soit  $P = \sum_{k \geq 0} a_k X^k, Q = \sum_{k \geq 0} b_k X^k \in \mathbb{K}[X]$  et  $\lambda \in \mathbb{K}$ . L'associativité et la distributivité des lois sur  $\mathcal{A}$ , toutes les sommes étant finies, permettent d'écrire :



- $(P + \lambda Q)(x) = \sum_{k \geq 0} (a_k + \lambda b_k) x^k = \sum_{k \geq 0} a_k x^k + \lambda \sum_{k \geq 0} b_k x^k = P(x) + \lambda Q(x).$
- $(PQ)(x) = \sum_{k, \ell \geq 0} a_k b_\ell x^k = \left( \sum_{k \geq 0} a_k x^k \right) \times \left( \sum_{\ell \geq 0} b_\ell x^\ell \right) = P(x) \times Q(x).$
- $f(1_{\mathbb{K}[X]}) = f(X^0) = x^0 = 1_{\mathcal{A}}.$

**Remarque**

R46 – En particulier, deux polynômes en  $x \in \mathcal{A}$  commutent toujours.

## VI COMPLÉMENT (HP) : SOUS-GROUPES DE $(\mathbb{R}, +)$

### Théorème 6 : Hors-Programme

Soit  $G$  est un sous-groupe de  $(\mathbb{R}, +)$ .

Alors  $G$  est soit dense dans  $\mathbb{R}$ , soit discret (de la forme  $\alpha\mathbb{Z}$ ).

### Exercice 15 : Démonstration

Traiter le cas où  $G = \{0\}$ . On suppose dorénavant que  $G \neq \{0\}$ .

Montrer que  $G \cap \mathbb{R}_+^*$  est non vide. En déduire que  $G \cap \mathbb{R}_+^*$  admet une borne inférieure. On note  $\alpha$  cette borne inférieure.

**Cas où  $\alpha = 0$**  Montrer que  $G$  est dense dans  $\mathbb{R}$  en s'inspirant de la démonstration de la densité de  $\mathbb{Q}$  dans  $\mathbb{R}$ .

**Cas où  $\alpha > 0$**  On s'inspire de la démonstration des sous-groupes de  $(\mathbb{Z}, +)$ .

Montrer qu'il existe  $x \in G$  tel que  $\alpha \leq x < 2\alpha$ .

En déduire que  $x = \alpha$ , puis que  $\alpha\mathbb{Z} \subset G$ .

Soit réciproquement  $x \in G$ . On simule une division euclidienne.

Montrer que l'on peut trouver  $q \in \mathbb{Z}$  tel que  $q\alpha \leq x < (q+1)\alpha$ .

En déduire que  $x = q\alpha$ . Conclure.