

Formalismes, Ensembles et Structures

3. Structures algébriques usuelles

Edouard Marchais

EPITA
edouard.marchais@epita.fr



Edouard Marchais (EPITA) 1 / 48

Introduction

- Beaucoup d'**ensembles mathématiques** possèdent des propriétés communes. Il est intéressant d'étudier ces propriétés, en premier lieu, dans le cas général pour les appliquer, en second lieu, à tous les cas particuliers.
- Nous étudierons successivement les structures de **groupe**, d'**anneau** et de **corps** que l'on rencontre très fréquemment en algèbre, en analyse et en géométrie.
- La notion de groupe apparaît, en 1830 avec Évariste Galois, largement incompris de ses contemporains; il faut attendre l'aube du XXe siècle pour que les structures algébriques s'imposent dans tous les domaines des mathématiques (David Hilbert, Félix Klein, Elie Cartan).

Edouard Marchais (EPITA) 3 / 48

Table des matières

- 1 Lois de composition interne
 - Loi de composition interne - Partie stable
 - Propriétés d'une l.c.i.
- 2 Structure de groupe
 - Définition d'un groupe
 - Propriétés
- 3 Sous-groupe
 - Définition et caractérisation
 - Exemples
- 4 Morphisme de groupes
 - Définition générale d'un morphisme
 - Définition générale d'un morphisme
- 5 Structure d'anneau
 - Noyau d'un morphisme de groupes
 - Image d'un morphisme de groupes
 - Définition générale d'un morphisme
 - Propriétés
 - Sous-anneau
 - Structure de corps
- 6 Anneau des entiers relatifs
 - Définition et caractérisation
 - Division euclidienne dans $\mathbb{Z}$
 - Division euclidienne dans $(\mathbb{Z}, +)$
 - Nombres premiers
- 7 Exercices

Edouard Marchais (EPITA) 2 / 48

1. Lois de composition interne

1.1 Loi de composition interne - Partie stable

- Soit E un ensemble. On appelle **loi de composition interne** dans E (en abrégé : l.c.i.) une application de $E \times E$ dans E , notée :

$$\begin{array}{lcl} E \times E & \longrightarrow & E \\ (a, b) & \longmapsto & a \star b \end{array}$$

- Une partie F de E est dite **stable** par la l.c.i. $\star$, si :

$$\forall (a, b) \in F^2 \quad a \star b \in F$$

- On appelle **l.c.i. induite** par $\star$ dans F la restriction de $\star$ à $F \times F$.
- **Exemples :**
 - La partie $\mathbb{R}_-$ de $\mathbb{R}$ est stable par $+$.
 - La partie $\mathbb{R}_+$ est stable par $\times$.
 - La partie $\mathbb{R}_-$ n'est pas stable par $\times$.

Edouard Marchais (EPITA) 4 / 48

- Une l.c.i. $\star$ dans un ensemble E est dite :
 - commutative**, si : $\forall (a, b) \in E^2 \quad a \star b = b \star a$;
 - associative**, si : $\forall (a, b, c) \in E^3 \quad a \star (b \star c) = (a \star b) \star c$
- Si $\star$ est associative, on peut écrire directement et sans ambiguïté :

$$a \star b \star c \quad \text{ou} \quad \bigstar_{1 \leq i \leq n} a_i$$

- Exemples :**

$$a_1 \times a_2 \times \cdots \times a_n = \prod_{i=1}^n a_i \quad \text{et} \quad a_1 + a_2 + \cdots + a_n = \sum_{i=1}^n a_i$$

- Le symétrique d'un élément, s'il existe, est donc **unique**.
- Le plus souvent, une l.c.i. associative est notée de façon **additive** : $a + b$ ou **multiplicative** : ab .
- La notation additive n'est employée que pour une l.c.i. **commutative**.

Un élément $e \in E$ est dit :

- élément neutre**, si : $\forall a \in E \quad a \star e = e \star a = a$

Si E possède un élément neutre e , un élément a de E est dit :

- symétrisable**, si : $\exists a' \in E \quad a \star a' = a' \star a = e$

a' est appelé **symétrique** de a .

Supposons la l.c.i. $\star$ associative; si un élément a possède deux symétriques a' et a'' , on a :

$$\begin{aligned} a'' \star a \star a' &= (a'' \star a) \star a' = e \star a' = a' \\ a'' \star a \star a' &= a'' \star (a \star a') = a'' \star e = a'' \quad \text{donc} \quad a' = a'' \end{aligned}$$

	notation additive	notation multiplicative
associativité	$a + (b + c) = (a + b) + c$	$a(bc) = (ab)c$
neutre	$a + 0 = 0 + a = a$	$ae = ea = a$
symétrique de a	opposé : $-a$ $a + (-a) = (-a) + a = 0$	inverse : a^{-1} $aa^{-1} = a^{-1}a = e$
itéré : $\forall n \in \mathbb{N}^*$ si $n = 0$ si a est symétrisable $\forall b \in \mathbb{N}^*$	$na = a + a + \cdots + a$ $0a = 0$ $(-n)a = a(-n)$	$a^n = aa \cdots a$ $a^0 = e$ $a^{-n} = (a^{-1})^n$
$\forall (n, m) \in \mathbb{Z}^2$	$na + ma = (n + m)a$	$a^n a^m = a^{n+m}$

2. Structure de groupe

2.1 Définition d'un groupe

On appelle **groupe** un ensemble G muni d'une loi de composition interne $\star$ telle que

- ① $\star$ est associative :

$$\forall (a, b, c) \in G^3 \quad a \star (b \star c) = (a \star b) \star c$$

- ② G possède un élément neutre e :

$$\forall a \in G \quad a \star e = e \star a = a$$

- 3 Tous les éléments de G sont symétrisables :

$$\forall a \in G \quad \exists a' \in G \quad a \star a' = a' \star a = e$$

Si de plus $\star$ est commutative, le groupe est dit **commutatif** ou **abélien**

2.2 Propriétés

- 1 Un groupe est non vide : il contient au moins son élément neutre.
- 2 L'élément neutre est unique.
- 3 Le symétrique d'un élément est unique.
- 4 Pour tout élément a de G , $ax = ay \Rightarrow x = y$ (il suffit de multiplier à gauche par a^{-1}). De même : $xa = ya \Rightarrow x = y$ (multiplier à droite par a^{-1}). On dit que a est **régulier**.
- 5 Pour tout $(a, b) \in G^2$, l'équation $ax = b$ a une solution unique : $x = a^{-1}b$. De même l'équation $xa = b$ a une solution unique : $x = ba^{-1}$.
- 6 $\forall (a, b) \in G^2 \quad (ab)^{-1} = b^{-1}a^{-1}$

- **Examples :**

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$
- $(\text{Bij}(E), \circ)$, où $\text{Bij}(E)$ est l'ensemble des bijections de E dans E .

- Dans la suite, la l.c.i. d'un groupe quelconque est souvent notée multiplicativement (ou additivement, uniquement si le groupe est abélien). S'il n'y a pas d'ambiguïté, on notera le groupe G sans préciser la l.c.i.

3. Sous-groupe

3.1 Définition et caractérisation

- On appelle **sous-groupe** d'un groupe G toute partie H de G , stable par la l.c.i. du groupe et qui, munie de la l.c.i. induite, est encore un groupe.
- **Exemple** : $\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$.

Théorème 1

Une partie H d'un groupe G est un sous-groupe si et seulement si :

- 1 H est **non vide**.
- 2 H est **stable** par la l.c.i. de G .
- 3 H contient les **symétriques** de tous ses éléments.

- En notation additive : $\begin{cases} 1) & H \neq \emptyset \\ 2) & \forall (x, y) \in H^2 \quad x + y \in H \\ 3) & \forall x \in H \quad -x \in H \end{cases}$
- En notation multiplicative : $\begin{cases} 1) & H \neq \emptyset \\ 2) & \forall (x, y) \in H^2 \quad xy \in H \\ 3) & \forall x \in H \quad x^{-1} \in H \end{cases}$

3.2 Exemples

- On montre facilement, à l'aide du théorème de caractérisation d'un sous-groupe, que : $\{e\}$ et G sont des sous-groupes de G .
- L'intersection de deux sous-groupes de G est un sous-groupe de G .
- $\mathcal{U} = \{z \in \mathbb{C}, |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
- $\mathcal{U}_n = \{z \in \mathbb{C}, z^n = 1\}$ est un sous-groupe de $(\mathcal{U}, \times)$.
- L'ensemble des suites convergentes est un sous-groupe de $(\mathbb{R}^{\mathbb{N}}, +)$.
- L'ensemble des fonctions continues est un sous-groupe de $(\mathbb{R}^{\mathbb{R}}, +)$.
- L'ensemble des isométries du plan P est un sous-groupe de $(\text{Bij}(E), \circ)$.
- L'ensemble des déplacements de P est un sous-groupe du groupe des isométries de P .
- L'ensemble des symétries centrales et translations de P est un sous-groupe du groupe des déplacements de P .

Démonstration :

Adoptons la notation multiplicative et notons e l'élément neutre de G .

- Si H est un sous-groupe de G , il est non vide et stable par $\times$.
 - Soit e l'élément neutre de H . $e'e' = e'e'$; comme e' est régulier, $e' = e$.
 - Soit $x \in H$. x a un inverse x^{-1} au sens de G et un inverse x' au sens de H . $x'x = e = x^{-1}x$, d'où $x' = x^{-1}$; donc $x^{-1} \in H$: H contient les inverses de tous ses éléments.
- Soit H une partie de G vérifiant les points 1), 2) et 3). H est stable. Vérifions que, munie de sa loi induite, c'est un groupe. La loi induite est évidemment associative.

Comme $H \neq \emptyset$, il existe $x \in H$; alors $x^{-1} \in H$, d'où $xx^{-1} \in H$, c'est-à-dire $e \in H$. H possède donc un élément neutre. De plus, tout élément de H a un inverse dans G qui, d'après 3), est dans H : H est un groupe, donc un sous-groupe de G .

4. Morphisme de groupes

4.1 Définition générale d'un morphisme

Soit E et F deux ensembles munis respectivement des l.c.i. $\star$ et $\bullet$. On appelle **morphisme** de $(E, \star)$ dans $(F, \bullet)$ une application f de E dans F telle que :

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

Exemples :

$$\begin{array}{l|l|l} (\mathbb{Z}, +) & \longrightarrow & (\mathbb{R}_+^*, \times) \\ n & \longrightarrow & 2^n \end{array} \quad \begin{array}{l|l} (\mathbb{R}_+^*, \times) & \longrightarrow & (\mathbb{R}, +) \\ x & \longrightarrow & \ln x \end{array}$$

$$\begin{array}{l|l} (\mathbb{C}, \times) & \longrightarrow & (\mathbb{C}, \times) \\ z & \longrightarrow & \bar{z} \end{array}$$

- La composée de deux morphismes est un morphisme.
- Un morphisme d'un ensemble dans lui-même avec la même l.c.i. est appelé **endomorphisme**.
- Un morphisme bijectif est appelé **isomorphisme**.
La bijection réciproque d'un isomorphisme est un **isomorphisme**.
Deux ensembles sont dits **isomorphes** s'il existe un isomorphisme de l'un dans l'autre.
- Un endomorphisme bijectif est appelé **automorphisme**.
L'ensemble des automorphismes de $(E, \star)$ est un sous-groupe de $(\text{Bij}(E), \bullet)$, noté $\text{Aut}(E)$.

4.3 Noyau d'un morphisme de groupes

- Soit G et G' deux groupes multiplicatifs, d'éléments neutres respectifs e et e' et f un morphisme de G dans G' .
- On appelle **noyau** de f l'ensemble des éléments de G qui ont pour image l'élément neutre de G' . On le note :

$$\text{Ker } f = \{x \in G, f(x) = e'\} = f(\{e'\})$$

Théorème 2

Pour tout morphisme f du groupe G dans le groupe G' :

- $\text{Ker } f$ est un sous-groupe de G .
- $\text{Ker } f = \{e\}$ si et seulement si f est injectif.

- Soit G et G' deux groupes multiplicatifs, d'éléments neutres respectifs e et e' et f un morphisme de G dans G' .

$$f(e) = e'$$

- En effet, $f(e) = f(ee) = f(e)f(e)$ et $f(e) = f(e)e'$, d'où $f(e)f(e) = f(e)$ et, comme $f(e)$ est régulier, $f(e) = e'$.

$$\forall x \in G \quad f(x') = f(x)^{-1}$$

- En effet, $f(xx^{-1}) = f(x)f(x^{-1})$ et $f(xx^{-1}) = f(e) = e$ d'où $f(x)f(x^{-1}) = e'$ c'est-à-dire $f(x^{-1}) = f(x)^{-1}$.

Démonstration :

(Adoptons la notation multiplicative)

- 1 Comme $f(e) = e'$, $e \in \text{Ker } f$, donc $\text{Ker } f \neq \emptyset$.
 $\forall (x, y) \in (\text{Ker } f)^2, f(xy) = f(x)f(y) = e'e' = e$, donc $xy \in \text{Ker } f$: $\text{Ker } f$ est stable.
 $\forall x \in \text{Ker } f, f(x^{-1}) = f(x)^{-1} = e'^{-1} = e'$, donc $x^{-1} \in \text{Ker } f$: $\text{Ker } f$ contient les inverses de tous ses éléments. $\text{Ker } f$ est donc un sous-groupe de G .
- 2 Si f est injectif, $\forall x \in \text{Ker } f, f(x) = e' = f(e)$, donc $x = e$. $\text{Ker } f = \{e\}$.
Réciproquement, si $\text{Ker } f = \{e\}$, soit $(x, y) \in G^2$ tel que $f(x) = f(y)$.
Alors $f(x)f(y)^{-1} = e'$; d'où $f(xy^{-1}) = e'$, d'où $xy^{-1} \in \text{Ker } f$, d'où $xy^{-1} = e$.
Donc $x = y$: f est injectif.

Exemple :

L'application

$$\left| \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ x & \longrightarrow & e^{ix} \end{array} \right.$$

est un morphisme de groupes dont le noyau est

$$\text{Ker } f = \{x \in \mathbb{R}, e^{ix} = 1\} = 2\pi\mathbb{Z},$$

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

Soit G et G' deux groupes, et f un morphisme de G dans G' . On appelle **image** de f l'ensemble des éléments de G' qui ont un antécédent dans G .

On le note :

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

Théorème 3

Pour tout morphisme f du groupe G dans le groupe G' :

- $\text{Im } f$ est un sous-groupe de G' .
- $\text{Im } f = G'$ si et seulement si f est surjectif.

Démonstration :

- ① (Adoptons la notation multiplicative)

$e' = f(e) \in \text{Im } f$, donc $\text{Im } f \neq \emptyset$.

$\forall (y, y') \in \text{Im } f, \exists (x, x') \in G^2, y = f(x) \text{ et } y' = f(x')$.

D'où $yy' = f(x)f(x') = f(xx') \in \text{Im } f$: $\text{Im } f$ est stable.

$\forall y \in \text{Im } f, \exists x \in G, y = f(x)$. D'où $y^{-1} = f(x)^{-1} = f(x^{-1}) \in \text{Im } f$.

$\text{Im } f$ contient les inverses de tous ses éléments. $\text{Im } f$ est donc un sous-groupe de G' .

- ② $f(G) = G'$ est la définition même de la surjectivité de f .

Exemple :

L'image du morphisme

$$\left| \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ x & \longrightarrow & e^{ix} \end{array} \right.$$

est

$$\text{Im } f = \mathcal{U} = \{z \in \mathbb{C}, |z| = 1\},$$

qui est un sous-groupe de $(\mathbb{C}^*, \times)$.

5. Structure d'anneau

5.1 Anneau

On appelle **anneau** un ensemble A muni de deux l.c.i., notées respectivement $+$ et $\times$, telles que :

- ① $(A, +)$ est un groupe abélien. Le neutre est noté 0_A (élément nul).
- ② La l.c.i. $\times$ est associative.
- ③ A possède un élément neutre pour la l.c.i. $\times$ noté 1_A (élément unité).
- ④ $\times$ est distributive par rapport à $+$, c'est-à-dire :

$$\forall (a, b, c) \in A^3 \quad a(b + c) = ab + ac \text{ et } (b + c)a = ba + ca$$

Si de plus $\times$ est commutative, l'anneau est dit commutatif.

Exemples : $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{R}^{\mathbb{N}}, +, \times)$, $(\mathbb{R}^{\mathbb{R}}, +, \times)$

Exemple : Dans l'anneau $\mathbb{R}^{\mathbb{R}}$, les fonctions $f : x \mapsto x + |x|$ et $g : x \mapsto x - |x|$ sont des diviseurs de zéro, car fg est la fonction nulle, alors que ni f ni g ne sont nulles.

- On peut généraliser la distributivité de $\times$ par rapport à $+$:

$$\sum_{i=1}^n ab_i = a \sum_{i=1}^n b_i$$

- On peut appliquer la formule du binôme à deux éléments d'un anneau, s'ils commutent :

$$ab = ba \quad \Rightarrow \quad \forall n \in \mathbb{N} \quad (a + b)^n = \sum_{p=0}^n \binom{n}{p} a^{n-p} b^p$$

5.2 Propriétés

On peut définir dans un anneau A une l.c.i., notée $-$, par :

$$\forall (a, b, c) \in A^3 \quad a - b = a + (-b)$$

- $\forall (a, b, c) \in A^3 \quad a(b - c) = ab - ac$.
En effet, $a(b - c) + ac = a((b - c) + c) = ab$.
- De même, $\forall (a, b, c) \in A^3 \quad (b - c)a = ba - ca$.
- $\forall a \in A \quad a 0_A a = 0_A a$.
Il suffit de choisir $b = c$ dans les égalités précédentes.
- La réciproque n'est pas toujours vraie : on appelle **diviseurs de zéro** des éléments non nuls dont le produit est 0_A .

- De même, pour la factorisation de $a^n - b^n$:

$$\begin{aligned} \forall n \in \mathbb{N}^* \quad 1 - x^n &= (1 - x) \sum_{p=0}^{n-1} x^p \\ &= \sum_{p=0}^{n-1} x^p (1 - x) \end{aligned}$$

Si $1 - x$ est inversible, on retrouve la formule donnant la somme des termes d'une suite géométrique :

$$1 + x + x^2 + \cdots + x^{n-1} = (1 - x^n)(1 - x)^{-1}$$

On appelle **sous-anneau** d'un anneau A , toute partie B de A stable par $+$ et $\times$ et qui, munie des l.c.i. induites, est encore un anneau avec la même unité.

Théorème 4

Une partie B d'un anneau A est un sous-anneau de A si et seulement si :

- 1 $1_A \in B$.
- 2 $\forall (x, y) \in B^2 \quad x - y \in B$.
- 3 $\forall (x, y) \in B^2 \quad xy \in B$.

Exemples :

- L'ensemble des fonctions polynomiales, l'ensemble des fonctions continues, l'ensemble des fonctions bornées sont des sous-anneaux de $\mathbb{R}^{\mathbb{R}}$.
- L'ensemble des suites convergentes, l'ensemble des suites périodiques sont des sous-anneaux de $\mathbb{R}^{\mathbb{N}}$.

Démonstration :

- Soit B un sous-anneau de A . Il contient 1_A . Il est stable par $+$ et contient les opposés de ses éléments, donc il est stable par $-$. De plus, il est stable par $\times$.
- Soit B une partie de A vérifiant les points 1), 2) et 3). D'après 1) et 2), $(B, +)$ est un sous-groupe de $(A, +)$ (caractérisation condensée).

De plus, il est stable par $\times$ et la l.c.i. induite est évidemment associative et distributive par rapport à $+$. D'après 1), B possède un élément unité qui est le même que celui de A : $(B, +, \times)$ est un sous-anneau de A .

5.4 Structure de corps

On appelle **corps** un anneau (généralement supposé commutatif), non réduit à $\{0\}$, dont tout élément non nul est inversible.

Si $\mathbb{K}$ est un corps, le groupe de ses éléments inversibles est $\mathbb{K} \setminus \{0\}$.

Exemples : $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.

On appelle **sous-corps** d'un corps $\mathbb{K}$ une partie de $\mathbb{K}$ stable par $+$ et $\times$ et qui, munie des l.c.i. induites, est encore un corps.

(Il a nécessairement la même unité que $\mathbb{K}$, car ses éléments sont réguliers pour $\times$.)

6. Multiples et diviseurs d'un entier

6.1 Multiples et diviseurs d'un entier

Soit $(a, b) \in \mathbb{Z}^2$; s'il existe $n \in \mathbb{Z}$ tel que $a = nb$, on dit que :

- a est un multiple de b .
- b est un diviseur de a (ou « b divise a », notation : $b|a$).

L'ensemble des multiples de b est noté $b\mathbb{Z}$. Nous conviendrons de noter $D(a)$ l'ensemble des diviseurs de a .

6.2 Division euclidienne dans $\mathbb{Z}$

Théorème 5

Soit $(a, b) \in \mathbb{Z}^2$ tel que $b \neq 0$.

Il existe un couple unique $(q, r) \in \mathbb{Z}^2$ tel que

$$a = bq + r$$

et $0 \leq r \leq |b|$.

q est appelé **quotient** et r **reste** de la division de a par b .

Propriétés : (Les démonstrations, très simples, sont laissées en exercices)

- 1 La somme de deux multiples de b est un multiple de b .
- 2 L'opposé d'un multiple de b est un multiple de b .
- 3 Tout multiple d'un multiple de b est un multiple de b .
- 4 Si b divise deux entiers, il divise leur somme.
- 5 Tout diviseur d'un diviseur de a est un diviseur de a .
- 6 0 est un multiple de tout entier. Tout entier divise 0.
- 7 Si b divise a et a divise b , alors $a = \pm b$.
- 8 Restreintes à $\mathbb{N}$, les relations « divise » et « est multiple de » sont des relations d'ordre partielles.

6.3 Division euclidienne dans $(\mathbb{Z}, +)$

Théorème 6

Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$. Tout sous-groupe de $\mathbb{Z}$ est de cette forme.

Un entier p strictement supérieur à 1 est dit premier si ses seuls diviseurs positifs sont 1 et p .

Application : Crible d'Ératosthène

- On obtient la liste des nombres premiers inférieurs à n en supprimant, pour tout entier p de 2 à n , tous les multiples de p autres que p .
- Dans la pratique, pour savoir si un entier n est premier, on cherche à le diviser par tous les entiers premiers inférieurs ou égaux à $\sqrt{n}$.
- En effet, si $n = pq$, $p > n \Rightarrow q < n$.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figure: Le crible d'Ératosthène (mathématicien grec, 284-192 av. J.-C.)

7. Exercices

7.1 Vrai ou faux ?

- 0 est élément neutre de la soustraction dans $\mathbb{Z}$.
- $(\mathbb{Z}, \times)$ est un groupe abélien.
- $\mathbb{N}$ est un sous-groupe de $(\mathbb{Z}, +)$.
- Le noyau d'un morphisme de groupe est le singleton $\{e\}$.
- Tous les éléments d'un anneau sont réguliers pour les deux opérations.
- Tous les éléments d'un anneau sont inversibles.
- Un diviseur de zéro d'un anneau n'est jamais inversible.
- $(\mathbb{Q}, +, \times)$ est un corps commutatif.
- La somme de deux diviseurs d'un entier est un diviseur de cet entier.
- Tout diviseur de deux entiers est un diviseur de leur somme.
- Deux nombres premiers distincts n'ont pas de diviseurs communs.

- a) Faux ; $0 - 2 \neq 2$. b) Faux ; 2 n'est pas inversible dans $\mathbb{N}$.
 c) Faux ; $-2 \notin \mathbb{N}$. d) Faux en général, sauf lorsque ce morphisme est injectif. e) Faux ; 0 n'est pas régulier pour la multiplication. f) Faux ; 0 n'est pas inversible. g) Vrai. h) Vrai. i) Faux. j) Vrai. k) Faux ; ils ont un diviseur commun, qui est 1 (c'est le seul).

- ④ Étudier les propriétés (commutativité, associativité, élément neutre, symétrique d'un élément,...) des l.c.i. $\cap$, $\cup$ et Δ dans $\mathcal{P}(E)$.
- ⑤ Soit E un ensemble muni de deux l.c.i. $\circ$ et $\star$ admettant des éléments neutres respectifs e et f , et telles que :
 $\forall (x, y, u, v) \in E^4 \quad (x \star y) \circ (u \star v)$. Montrer que :
 - ① $e = f$
 - ② $\circ = \star$
 - ③ $\star$ est associative et commutative.
- ⑥ Soit E et F deux ensembles non vides et $\star$ une l.c.i. sur F . On définit, dans l'ensemble F^E des applications de E dans F , la l.c.i. $\bullet$ par : $\forall (f, g) \in (F^E)^2 \quad \forall x \in E \quad (f \bullet g)(x) = f(x) \star g(x)$.
 - ① Montrer que, si $\star$ est commutative, il en est de même de $\bullet$.
 - ② Montrer que, si $\star$ est associative, il en est de même de $\bullet$.
 - ③ Montrer que, si $\star$ admet un élément neutre e , il en est de même de $\bullet$. Donner des exemples.

7.3 Groupes

- ① On définit sur $\mathbb{R}$ la l.c.i. $\star$ par $a \star b = a + b - ab$.
 - ① $(\mathbb{R}, \star)$ est-il un groupe?
 - ② Déterminer un sous-ensemble de $\mathbb{R}$ qui soit un groupe pour la loi $\star$.
- ② Dans $\mathbb{R}^2$ on a la l.c.i. $\star : (x, y) \star (x', y') = (x + x', ye^{x'} + y'e^{-x})$.
Démontrer que $(\mathbb{R}^2, \star)$ est un groupe. Est-il abélien ?
- ③ Montrer que l'ensemble des éléments d'un groupe qui commutent avec tous les autres est un sous-groupe. On l'appelle centre du groupe.
- ④ Montrer que l'ensemble $\{z \in \mathbb{C}, \exists n \in \mathbb{N}^* \quad z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
- ⑤ Soit G un groupe noté multiplicativement, H un sous-groupe de G et a un élément quelconque de G . Montrer que $a^{-1}Ha$ est un sous-groupe de G .

$\cap$ est une l.c.i. dans $\mathcal{P}(E)$, commutative, associative. E est élément neutre ; aucun élément autre que E n'a de symétrique.

$\cup$ est une l.c.i. dans $\mathcal{P}(E)$, commutative, associative. $\emptyset$ est élément neutre ; aucun élément autre que $\emptyset$ n'a de symétrique.

Δ est une l.c.i. dans $\mathcal{P}(E)$, commutative, associative. $\emptyset$ est élément neutre ; tout élément A de $\mathcal{P}(E)$ est son propre symétrique.

1) Choisir $(x, y, u, v) = (e, f, f, e)$.

2) Choisir $(x, y, u, v) = (x, e, e, z)$.

3) Choisir $(x, y, u, v) = (x, y, e, z)$,
puis $(x, y, u, v) = (e, y, z, e)$.

Ceci permet de transférer certaines structures d'un ensemble F à l'ensemble des applications d'un ensemble quelconque dans F .

Exemple : L'ensemble des suites numériques et l'ensemble des fonctions numériques sont, comme $\mathbb{R}$, des anneaux commutatifs.

Attention : La structure de corps ne se transmet pas, car il peut y avoir d'autres éléments que l'élément nul qui n'ont pas d'inverse.

1) Il s'agit bien d'une loi interne dans $\mathbb{R}$; elle est commutative, associative. 0 est élément neutre, mais 1 n'a pas de symétrique : $(\mathbb{R}, *)$ n'est pas un groupe.

2) Avant de conclure trop rapidement, vérifier soigneusement que $\mathbb{R} \setminus \{1\}$ est stable par $*$; la l.c.i. induite est encore associative, d'élément neutre 0, et tout élément a de $\mathbb{R} \setminus \{1\}$ possède un inverse $\frac{a}{a-1}$ qui appartient aussi à $\mathbb{R} \setminus \{1\}$.
 $(\mathbb{R} \setminus \{1\}, *)$ est un groupe abélien.

Il s'agit bien d'une loi interne dans $\mathbb{R}^2$. Vérifier soigneusement l'associativité. $(0, 0)$ est élément neutre. Tout couple (x, y) admet pour symétrique le couple $(-x, -y)$. $(\mathbb{R}^2, *)$ est bien un groupe ; il n'est pas abélien (essayer).

Utiliser le théorème de caractérisation d'un sous-groupe.

Réutiliser le théorème de caractérisation d'un sous-groupe.

Réutiliser le théorème de caractérisation d'un sous-groupe.
(Attention : Ce théorème fait partie de ceux qu'on utilise le plus souvent dans les concours.)

- ❶ Soit A un anneau. Un élément x de A est dit *nil-potent* si :
 $\exists n \in \mathbb{N} \quad x^n = 0$.
- ❶ Démontrer que, si xy est nilpotent, yx l'est aussi.
 - ❷ Démontrer que, si x et y sont deux éléments nilpotents qui commutent, alors xy et $x + y$ sont nilpotents.
 - ❸ Soit x un élément nilpotent. Démontrer que $1 - x$ est inversible et calculer son inverse.
- ❷ Soit A un anneau tel que $\forall x \in A \quad x^2 = x$.
- ❶ Démontrer que $\forall x \in A \quad x + x = 0$.
 - ❷ Démontrer que l'anneau A est commutatif.

- 1) En supposant que $(xy)^n = 0$, multiplier à droite par x et à gauche par y .
- 2) Si $x^n = 0$, $y^p = 0$ et $xy = yx$, alors $(xy)^n = x^n y^n = 0$.

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

Montrer que tous les termes de cette somme sont nuls (distinguer suivant que $k < n$ ou $k \geq n$).

- 3) Soit x un élément tel que $x^n = 0$. Calculer $(1 - x) \sum_{k=0}^{n-1} x^k$.

- 1) $\forall x \in A \quad (x+x)^2 = x+x$. Développer et simplifier pour aboutir à $x+x=0$.
- 2) $\forall x \in A \quad (x+y)^2 = x+y$. Développer et simplifier pour aboutir à $xy+yx=0$. En déduire que $xy=yx$.

7.5 Anneau des entiers relatifs

- ❶ Trouver deux entiers positifs a et b sachant que $a < 4000$ et que la division euclidienne de a par b donne un quotient de 82 et un reste de 47.
- ❷ On divise deux entiers a et b par leur différence $a - b$. Comparer les quotients et les restes obtenus.
- ❸ Soit a, b, n trois entiers tels que $a > 1$, $b \geq 1$ et $n \geq 0$. On note g le quotient de la division euclidienne de $a - 1$ par b . Trouver le quotient de la division euclidienne de $ab^n - 1$ par b^{n+1} .
- ❹ Les entiers 11, 111, 1111, 11111, 111111, 1111111, 11111111 sont-ils premiers ?

$$(a, b) = (3\,983, 48).$$

Écrire :

$$a = (a - b)q_1 + r_1 \quad \text{avec} \quad 0 \leq r_1 < a - b$$

$$b = (a - b)q_2 + r_2 \quad \text{avec} \quad 0 \leq r_2 < a - b$$

En déduire :

$$r_1 = r_2 \quad \text{et} \quad q_1 = q_2 + 1.$$

$$a - 1 = bq + r \quad \text{avec} \quad 0 \leq r < b$$

$$\text{d'où} \quad ab^n - 1 = b^{n+1}q + rb^n + b^n - 1$$

Vérifier que $rb^n + b^n - 1 < b^{n+1}$, et conclure.

Soit a_n l'entier qui s'écrit en base 10 avec n chiffres 1. Si n est pair, a_n est divisible par 11. Si n est divisible par 3, a_n est aussi divisible par 3. Ainsi, a_3 , a_4 et a_6 ne sont pas premiers. On vérifie que a_5 est divisible par 41, et a_7 par 239. Ainsi, le seul nombre premier dans les entiers donnés est 11.
 (Le nombre premier suivant de cette suite est a_{19} ...)