

Structure algébriques fondamentales

Aperçu

1. Loi de composition
2. La structure de groupe
3. La structure d'anneau
4. La structure d'espace vectoriel
5. La structure d'algèbre

Structure algébriques fondamentales

1. Loi de composition

- 1.1 Loi de composition ; associativité ; commutativité
- 1.2 Élément neutre ; éléments inversibles
- 1.3 Loi associées à un même loi de composition interne
- 1.4 Morphismes

2. La structure de groupe

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

1. Loi de composition

1.1 Loi de composition ; associativité ; commutativité

1.2 Élément neutre ; éléments inversibles

1.3 Loi associées à un même loi de composition interne

1.4 Morphismes

2. La structure de groupe

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 1 Soit E un ensemble. On appelle **loi de composition interne** sur E une application

$$T : E \times E \rightarrow E.$$

La valeur $T(x, y)$ de T pour un couple $(x, y) \in E \times E$ s'appelle le **composé** de x et de y pour cette loi.

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

D 3 Soit une loi de composition interne $(x, y) \mapsto x \star y$ sur un ensemble E .

► On dit que \star est **associative** si

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

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

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

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

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

E 4

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

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

1. Loi de composition

1.1 Loi de composition ; associativité ; commutativité

1.2 Élément neutre ; éléments inversibles

1.3 Loi associées à un même loi de composition interne

1.4 Morphismes

2. La structure de groupe

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 5 Soit une loi de composition interne $(x, y) \mapsto x \star y$ sur un ensemble E . Un élément e de E est dit **élément neutre** si

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

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

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

E 6 L'application Id_E est l'élément neutre de la loi de composition \circ dans $\mathcal{F}(E, E)$.

E 7 La loi $x \star y = \frac{x+y}{2}$ dans \mathbb{R} possède-t-elle un élément neutre?

D 8 Soient une loi de composition interne $(x, y) \mapsto x \star y$ sur un ensemble E possédant un élément neutre e et x et x' deux éléments de E .

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

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

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

P 9 *Soit E muni d'une loi de composition interne \star , associative et possédant un élément neutre e .*

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

D 10 Soit une loi de composition interne $(x, y) \mapsto x \star y$ sur un ensemble E . On dit qu'un élément $a \in E$ est **régulier** ou **simplifiable** pour la loi \star lorsque

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

P 11 *Soit E muni d'une loi de composition interne \star , associative et possédant un élément neutre e . Tout élément inversible est simplifiable.*

1. Loi de composition

1.1 Loi de composition ; associativité ; commutativité

1.2 Élément neutre ; éléments inversibles

1.3 Loi associées à un même loi de composition interne

1.4 Morphismes

2. La structure de groupe

3. La structure d'anneau


4. La structure d'espace vectoriel

5. La structure d'algèbre

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

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

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

¹ : $a \in X \star Y \iff \exists (x, y) \in X \times Y, a = x \star y$.

D 12 Une partie A d'un ensemble E est dite **stable** pour un loi de composition interne \star sur E si le composé de deux éléments de A appartient à A :

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

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

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

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

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

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

E 13 Soit $X = E = \mathbb{R}$, pour $f, g, s, p \in \mathcal{F}(\mathbb{R}, \mathbb{R})$, on aura

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

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

1. Loi de composition

1.1 Loi de composition ; associativité ; commutativité

1.2 Élément neutre ; éléments inversibles

1.3 Loi associées à un même loi de composition interne

1.4 Morphismes

2. La structure de groupe

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 14 Un **morphisme** de (E, \star) dans (F, \top) est une application f de E dans F telle que

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

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

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

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

E 15 L'application $A \mapsto \mathbb{C}_E A$ de $\mathcal{P}(E)$ dans lui-même est un isomorphisme de $(\mathcal{P}(E), \cap)$ dans $(\mathcal{P}(E), \cup)$ et également un isomorphisme de $(\mathcal{P}(E), \cup)$ dans $(\mathcal{P}(E), \cap)$ (loi de Morgan). Ce n'est cependant pas un automorphisme car la loi n'est pas la même au départ et à l'arrivée.

D 16 S'il existe un isomorphisme de (E, \star) dans (F, T) , on dit que (E, \star) et (F, T) sont **isomorphes**.

R Si (E, \star) et (F, T) sont isomorphes, alors l'une de ces deux lois est associative (resp. commutative) si et seulement si l'autre l'est.

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

1. Loi de composition

2. La structure de groupe

2.1 Groupes

2.2 Groupe produit

2.3 Sous-groupes

2.4 Morphismes de groupes

2.5 Noyau et image d'un morphisme de groupes

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

1. Loi de composition

2. La structure de groupe

2.1 Groupes

2.2 Groupe produit

2.3 Sous-groupes

2.4 Morphismes de groupes

2.5 Noyau et image d'un morphisme de groupes

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 17 On appelle **groupe** un couple formé d'un ensemble G et d'une loi de composition interne \star sur l'ensemble G associative, possédant un élément neutre et pour laquelle tout élément est inversible. Autrement dit,

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

► $\exists e_G \in G, \forall x \in G, e_G \star x = x \star e_G = x.$

► $\forall x \in G, \exists x' \in G, x \star x' = x' \star x = e_G.$

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

Les groupes sont en général notés multiplicativement (xy) ou additivement ($x + y$). Les convention suivantes sont utilisés

Notation	multiplicative	additive
$x \star y$	xy	$x + y$
élément neutre	e_G ou e	0_G ou 0
inverse	x^{-1}	$-x$
puissance	x^n	nx

E 18


1. (Groupes additifs) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes. L'élément neutre est 0 et l'opposé de x est $-x$. En revanche, $(\mathbb{N}, +)$ n'est pas un groupe car si $n \in \mathbb{N}$ est strictement positif, il n'a pas d'inverse pour $+$.
2. (Groupes multiplicatifs) (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \times) , (\mathbb{R}_+^*, \times) , (\mathbb{C}^*, \times) sont des groupes commutatifs. L'élément neutre est 1 et l'inverse de x est $\frac{1}{x}$.

3. (Groupes des permutations d'un ensemble X) Soit X un ensemble et $S(X)$ l'ensemble des permutations de X . Si f, g sont des permutations de X , il en est de même de $f \circ g$; $(f, g) \mapsto f \circ g$ définit donc une loi de composition interne sur l'ensemble $S(X)$; cette loi de composition interne est associative ; elle admet un élément neutre, à savoir l'application identique Id_X ; enfin, si f est une permutation de X , il en est de même de l'application réciproque f^{-1} et celle-ci est évidemment inverse de f pour la loi de composition interne considérée. Ainsi, $(S(X), \circ)$ est un groupe ; on l'appelle le **groupe des permutations de l'ensemble X** . C'est l'étude de ces groupes par Galois (lorsque X est un ensemble fini) qui a conduit, historiquement, à la notion générale et « abstraite » de groupe.

4. (Similitudes directe du plan) L'ensemble des similitudes directes du plan est un groupe (non commutatif) pour la composition \circ . En prenant l'écriture analytique complexe $z \mapsto az + b$ avec $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$, l'élément neutre est l'identité $z \mapsto z$ et l'inverse de $z \mapsto az + b$ est $z \mapsto \frac{1}{a}z - \frac{b}{a}$.

P 19 Soit $(G, .)$ un groupe. Alors

1. G est non-vide : il contient au moins son élément neutre.
2. L'élément neutre de G est unique.
3. Le symétrique de tout élément de G est unique.
4. $\forall x \in G, (x^{-1})^{-1} = x$.
5. $\forall (x, y) \in G^2, (xy)^{-1} = y^{-1}x^{-1}$.
6. $\forall x \in G, \forall (n, m) \in \mathbb{Z}^2, x^{n+m} = x^n x^m$.
7. Dans un groupe, tout élément est simplifiable. En effet, pour tout $a \in G$, on a
 - ▶ $\forall (x, y) \in G^2, ax = ay \implies x = y$.
 - ▶ $\forall (x, y) \in G^2, xa = ya \implies x = y$.

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

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

sauf si x et y commutent.

1. Loi de composition

2. La structure de groupe

2.1 Groupes

2.2 Groupe produit

2.3 Sous-groupes

2.4 Morphismes de groupes

2.5 Noyau et image d'un morphisme de groupes

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

T 20 Soient deux groupes (E, \top) et (F, \perp) . On définit une loi \star sur $E \times F$ par

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

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

1. Loi de composition

2. La structure de groupe

2.1 Groupes

2.2 Groupe produit

2.3 Sous-groupes

2.4 Morphismes de groupes

2.5 Noyau et image d'un morphisme de groupes

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 21 Soit (G, \star) un groupe. On appelle **sous-groupe** de G une partie H de G possédant les propriétés suivantes

1. L'élément neutre de G appartient à H

$$e_G \in H;$$

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

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

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

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

P 22 *Soient (G, \star) un groupe et H un sous-groupe de G . Alors (H, \star) est lui-même un groupe pour la loi de composition induite sur H par la loi de composition de G . Réciproquement, si H est une partie du groupe G telle que (H, \star) est un groupe, alors H est un sous-groupe de G .*

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

E 23

1. Si (G, \star) est un groupe d'élément neutre e , alors $\{e\}$ est un sous-groupe de G . De même, G est un sous-groupe de G . Le sous-groupe $\{e\}$ est appelé **sous-groupe trivial** de G .
2. Tout sous-groupe de G , distinct de $\{e\}$ et G est appelé **sous-groupe propre** de G .

3. $2\mathbb{Z} = \{ 2k \mid k \in \mathbb{Z} \}$ est un sous-groupe de $(\mathbb{Z}, +)$.

En effet, 0 est pair. Soient $x, y \in 2\mathbb{Z}$, il existe donc $x', y' \in \mathbb{Z}$ tel que $x = 2x'$ et $y = 2y'$. On a donc

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

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

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

c'est-à-dire, $-x \in 2\mathbb{Z}$.

4. Chacun des groupe $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ est un sous-groupe de tous les suivants.
5. Chacun des groupe $(\mathbb{Q}^*, .)$, $(\mathbb{R}^*, .)$, $(\mathbb{C}^*, .)$ est un sous-groupe de tous les suivants.
6. \mathbb{R}_+^* est un sous-groupe de $(\mathbb{R}^*, .)$ mais n'est pas un sous-groupe de $(\mathbb{R}, +)$.

7. L'ensemble \mathbb{U} des nombres complexes de module un est un sous-groupe de \mathbb{C}^\star .
En effet, 1 est de module un ($1 \in \mathbb{U}$), si z est de module un, alors $1/z$ est de module un (car $|1/z| = 1/|z|$), et si z, w sont de module un, alors zw aussi (car $|zw| = |z| |w|$).

P 24 *Soient (G, \star) un groupe, H et K deux sous-groupe de G . Alors $H \cap K$ est un sous-groupe de G .*

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

P 25

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

1. Loi de composition

2. La structure de groupe

2.1 Groupes

2.2 Groupe produit

2.3 Sous-groupes

2.4 Morphismes de groupes

2.5 Noyau et image d'un morphisme de groupes

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 26 Soit (G, \star) et (H, \top) deux groupes. On appelle **morphisme de groupes** ou **homomorphisme de groupes** une application $f : G \rightarrow H$ telle que

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

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

E 27

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

P 28 Soit f un morphisme du groupe G dans le groupe H . Alors

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

P 29

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

T 30 Soit f un morphisme du groupe G dans le groupe H .

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

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

est un sous-groupe de H .

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

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

est un sous-groupe de G .

1. Loi de composition

2. La structure de groupe

2.1 Groupes

2.2 Groupe produit

2.3 Sous-groupes

2.4 Morphismes de groupes

2.5 Noyau et image d'un morphisme de groupes

3. La structure d'anneau

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 31 Soit f un morphisme du groupe G dans le groupe H . L'image réciproque de l'élément neutre de H est appelé **noyau** de f et se note $\ker(f)$.

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

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

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

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

P 32 Soit f un morphisme du groupe G dans le groupe H .

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

T 33 Soient G et H deux groupes et f un morphisme de G dans H .

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

E 34 L'application $f : (\mathbb{C}^\star, \cdot) \rightarrow (\mathbb{R}^\star, \cdot)$ est un morphisme de groupes.

$$z \mapsto |z|$$

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

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

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

1. Loi de composition

2. La structure de groupe

3. La structure d'anneau

3.1 Anneaux

3.2 Éléments inversibles d'un anneau; corps

3.3 Calculs dans un anneau

3.4 Sous-anneaux

3.5 Idéaux d'un anneau commutatif

3.6 Anneau intègre

3.7 Morphisme d'anneaux

4. La structure d'espace vectoriel

5. La structure d'algèbre

1. Loi de composition

2. La structure de groupe

3. La structure d'anneau

3.1 Anneaux

3.2 Éléments inversibles d'un anneau; corps

3.3 Calculs dans un anneau

3.4 Sous-anneaux

3.5 Idéaux d'un anneau commutatif

3.6 Anneau intègre

3.7 Morphisme d'anneaux

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 35 Soit \top et \star deux lois de composition internes sur un ensemble E . On dit que la loi \star est **distributive** par rapport à la loi \top si l'on a

$$x \star (y \top z) = (x \star y) \top (x \star z) \quad (1)$$

$$(y \top z) \star x = (y \star x) \top (z \star x) \quad (2)$$

pour x, y, z dans E .

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

D 36 On appelle **anneau** un ensemble A muni de deux lois de composition appelées respectivement **addition** et **multiplication**, satisfaisant aux axiomes suivants :

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

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

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

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

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

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

E 37 $A = \{ 0, i \}.$

Voici quelques anneaux que nous rencontrerons en MP2I

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

1. Loi de composition

2. La structure de groupe

3. La structure d'anneau

3.1 Anneaux

3.2 Éléments inversibles d'un anneau; corps

3.3 Calculs dans un anneau

3.4 Sous-anneaux

3.5 Idéaux d'un anneau commutatif

3.6 Anneau intègre

3.7 Morphisme d'anneaux

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 38 Soit $(A, +, .)$ un anneau.

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

^aOn dit aussi que x est une **unité** de A , mais nous n'utiliserons pas cette terminologie dangereuse.

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

E 39 $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

P 40 *Le groupe multiplicatif de $(\mathbb{Z}, +, \cdot)$ est $\{-1, 1\} = \mathbb{U}_2$.*

D 41 On dit qu'un anneau \mathbb{K} est un **corps** s'il est commutatif, non réduit à 0 et si tout élément non nul de \mathbb{K} est inversible.

E 42 Les corps usuels sont \mathbb{Q} , \mathbb{R} et \mathbb{C} .

1. Loi de composition

2. La structure de groupe

3. La structure d'anneau

3.1 Anneaux

3.2 Éléments inversibles d'un anneau; corps

3.3 Calculs dans un anneau

3.4 Sous-anneaux

3.5 Idéaux d'un anneau commutatif

3.6 Anneau intègre

3.7 Morphisme d'anneaux

4. La structure d'espace vectoriel

5. La structure d'algèbre

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

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

P 43 Soient A un anneau et x, y des éléments de l'anneau A .

1. $x.0 = 0.x = 0$.

2. $x.(-y) = (-x).y = -(xy)$ et $(-x)(-y) = xy$.

(Règle des signes)

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

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

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

P 44 Conséquence de la distributivité

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

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

T 45 Soient A un anneau, $(x, y) \in A^2$ deux éléments qui commutent ($xy = yx$), alors pour tout entier $n \in \mathbb{N}$,

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

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

C 46 Calcul d'une progression géométrique

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

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

1. Loi de composition

2. La structure de groupe

3. La structure d'anneau

3.1 Anneaux

3.2 Éléments inversibles d'un anneau; corps

3.3 Calculs dans un anneau

3.4 Sous-anneaux

3.5 Idéaux d'un anneau commutatif

3.6 Anneau intègre

3.7 Morphisme d'anneaux

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 47 Soit $(A, +, \cdot)$ un anneau et B une partie de A . On dit que B est un sous anneau de A lorsque

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

P 48 *Si B est un sous anneau de A , alors B muni des deux lois induites a une structure d'anneau.*

1. Loi de composition

2. La structure de groupe

3. La structure d'anneau

3.1 Anneaux

3.2 Éléments inversibles d'un anneau; corps

3.3 Calculs dans un anneau

3.4 Sous-anneaux

3.5 Idéaux d'un anneau commutatif

3.6 Anneau intègre

3.7 Morphisme d'anneaux

4. La structure d'espace vectoriel

5. La structure d'algèbre

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

D 49 Soit $(A, +, \cdot)$ un anneau *commutatif* et I une partie de A . On dit que I est un **idéal** de A lorsque

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

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

1. Loi de composition

2. La structure de groupe

3. La structure d'anneau

3.1 Anneaux

3.2 Éléments inversibles d'un anneau; corps

3.3 Calculs dans un anneau

3.4 Sous-anneaux

3.5 Idéaux d'un anneau commutatif

3.6 Anneau intègre

3.7 Morphisme d'anneaux

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 50 Soient A un anneau et x un élément de l'anneau A . On dit que x est **régulier** (ou **simplifiable**) si pour tout $y \in A$, on a les implications

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

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

R

► On dit que x est un **diviseur à droite de 0** s'il existe $y \neq 0$ tel que $yx = 0$.

► On dit que x est un **diviseur à gauche de 0** s'il existe $y \neq 0$ tel que $xy = 0$.

Lorsque A est commutatif, il est inutile de préciser « à gauche » ou « à droite ».

D 51 On dit qu'un anneau A est **intègre** s'il est commutatif, non réduit à 0, et si le produit de deux éléments non nuls de A est non nul, ou encore

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

P 52 Soit A un anneau intègre, alors on a une règle de simplification pour la multiplication

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

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

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

1. Loi de composition

2. La structure de groupe

3. La structure d'anneau

3.1 Anneaux

3.2 Éléments inversibles d'un anneau; corps

3.3 Calculs dans un anneau

3.4 Sous-anneaux

3.5 Idéaux d'un anneau commutatif

3.6 Anneau intègre

3.7 Morphisme d'anneaux

4. La structure d'espace vectoriel

5. La structure d'algèbre

D 53 Soient A, A' deux anneaux. Une application $f : A \rightarrow A'$ est appelée **morphisme d'anneaux** si elle vérifie les conditions suivantes:

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

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

P 54 Soit $f : A \rightarrow A'$ un morphisme d'anneaux.

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

T 55 Soit $f : A \rightarrow A'$ un morphisme d'anneaux.

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

1. Loi de composition
2. La structure de groupe
3. La structure d'anneau
4. La structure d'espace vectoriel
5. La structure d'algèbre

D 56 Étant donné un corps $(\mathbb{K}, +, \cdot)$, d'éléments neutres $0_{\mathbb{K}}$ et $1_{\mathbb{K}}$, on appelle **espace vectoriel sur \mathbb{K}** un ensemble E muni d'une structure algébrique définie par la donnée

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

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

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

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

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

qui satisfait aux axiomes suivants ^a

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

^aRègle bien connue : pour économiser les parenthèses, on convient que la multiplication est prioritaire sur l'addition.

1. Loi de composition
2. La structure de groupe
3. La structure d'anneau
4. La structure d'espace vectoriel
5. La structure d'algèbre

D 57 On appelle \mathbb{K} -algèbre un quadruplet $(A, +, *, \cdot)$ tel que

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