

I

Groupes

1. Un **groupe** est un *couple* $(G, *)$ constitué d'un ensemble non vide G et d'une loi de composition interne $*$.

Un abus de langage aussi courant que pratique consiste à parler du groupe G au lieu du groupe $(G, *)$. Cela n'a de sens que si la structure algébrique définie par la loi $*$ est connue sans ambiguïté.

1.1 \Leftrightarrow Un couple constitué d'un ensemble G et d'une loi de composition interne

$$[(x, y) \mapsto x * y]$$

est un **groupe** lorsque

1. La loi $*$ est **associative** :

$$\forall x, y, z \in G, \quad x * (y * z) = (x * y) * z$$

2. Il existe un élément $e \in G$ qui est **neutre** pour $*$:

$$\forall x \in G, \quad x * e = e * x = x$$

3. Tout élément $x \in G$ admet un **inverse** $x' \in G$ pour $*$:

$$\forall x \in G, \exists x' \in G, \quad x * x' = x' * x = e.$$

1.2 Il arrive souvent que la loi de composition soit omise. On abrège alors le produit $x * y$ en xy .

1.3 \Leftrightarrow Le groupe $(G, *)$ est **commutatif** lorsque

$$\forall x, y \in G, \quad x * y = y * x.$$

1.4 Dans la définition [1.1], la loi de composition d'un groupe est comprise comme une sorte de multiplication.

1.5 Il arrive souvent que la loi de composition d'un groupe commutatif soit en fait une sorte d'addition : on n'hésite pas, dans ce cas, à noter $+$ cette loi de composition et à adapter en conséquence les axiomes de la structure de groupe.

1.6 \Leftrightarrow L'ensemble G est un **groupe additif** lorsqu'il est muni d'une loi de composition interne

$$[(x, y) \mapsto x + y]$$

telle que :

1. La loi $+$ est **associative** :

$$\forall x, y, z \in G, \quad (x + y) + z = x + (y + z)$$

et **commutative** :

$$\forall x, y \in G, \quad x + y = y + x$$

2. Il existe un élément $0_G \in G$ qui est **neutre** pour $+$:

$$\forall x \in G, \quad x + 0_G = 0_G + x = x$$

3. Tout élément $x \in G$ admet un **opposé** $x' \in G$:

$$\forall x \in G, \exists x' \in G, \quad x + x' = x' + x = 0_G.$$

2.1 \rightarrow **Unicité du neutre**

Un groupe possède un seul élément neutre.

2.2 \rightarrow **Unicité de l'inverse**

Tout élément d'un groupe G admet un unique symétrique dans ce groupe.

2.3 Les notations employées varient avec la loi de composition interne :

— Si la loi est comprise comme une multiplication, le neutre peut être noté 1_G ou 1 et le symétrique de $x \in G$ est noté x^{-1} .

— Si la loi est comprise comme une composition, le neutre peut être noté I .

— Si la loi est comprise comme une addition, le neutre est noté 0_G ou 0 et le symétrique de $x \in G$ est noté $-x$.

2.4 \rightarrow **Inverse d'un produit**

$$\forall x, y \in G, \quad (x * y)^{-1} = y^{-1} * x^{-1}$$

3. **Puissances**

Soient $(G, *)$, un groupe et x , un élément de G .

3.1 \Leftrightarrow On pose $x^0 = e$ et, pour tout entier $n \geq 1$,

$$x^{n+1} = x^n * x \quad \text{et} \quad x^{-n} = (x^{-1})^n.$$

3.2

$$\forall x \in G, \forall n \in \mathbb{Z}, \quad (x^{-1})^n = (x^n)^{-1}$$

3.3 \rightarrow **Commutativité des puissances**

$$\forall x \in G, \forall n, p \in \mathbb{Z}, \quad x^{n+p} = x^n * x^p = x^p * x^n$$

3.4

$$\forall x \in G, \forall n, p \in \mathbb{Z}, \quad (x^n)^p = x^{np}$$

4. De manière analogue, le groupe $(\mathbb{Z}, +)$ agit sur tout groupe additif $(G, +)$: pour tout $x \in G$, on pose

1.

$$0_{\mathbb{Z}} \cdot x = 0_G$$

2.

$$\forall n \in \mathbb{N}^*, \quad (n+1) \cdot x = (n \cdot x) + x$$

3.

$$\forall n \leq -1, \quad n \cdot x = (-n) \cdot (-x)$$

4.1

$$\forall x \in G, \forall n, p \in \mathbb{Z}, \quad (n+p) \cdot x = (n \cdot x) + (p \cdot x)$$

4.2

$$\forall x \in G, \forall n, p \in \mathbb{Z}, \quad n \cdot (p \cdot x) = (np) \cdot x$$

I.1 **Sous-groupes**

5. \Leftrightarrow Soit $(G, *)$, un groupe. Une partie H de G est un **sous-groupe** de $(G, *)$ lorsque $(H, *)$ est un groupe.

6. Soit H , un sous-groupe de $(G, *)$.

6.1 L'élément neutre du groupe $(H, *)$ est aussi l'élément neutre de $(G, *)$.

6.2 Pour tout $x \in H$, le symétrique de x dans H est aussi le symétrique de x dans G .

6.3 \rightarrow **Caractérisation d'un sous-groupe**

Soit $(G, *)$, un groupe. Une partie H de G est un sous-groupe si, et seulement si, l'élément neutre e_G appartient à H et

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

6.4 \rightarrow **Sous-groupe d'un groupe additif**

Une partie H est un sous-groupe de $(G, +)$ si, et seulement si, l'élément nul 0_G appartient à H et

$$\forall x, y \in H, \quad x - y \in H.$$

7. → Intersection de sous-groupes

Soit $(H_k)_{k \in I}$, une famille de sous-groupes de $(G, *)$. Leur intersection

$$H = \bigcap_{k \in I} H_k$$

est un sous-groupe de $(G, *)$.

8. Exemples de groupes

8.1 Quel que soit le groupe $(G, *)$, le singleton $\{e_G\}$ et G lui-même sont des sous-groupes de $(G, *)$.

8.2 Les ensembles de nombres \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des groupes additifs, mais \mathbb{N} n'est pas un groupe additif. Les parties $n\mathbb{Z}$, où $n \in \mathbb{N}^*$, sont des sous-groupes de $(\mathbb{Z}, +)$. →[23.6]

Tout espace vectoriel est aussi un groupe additif.

8.3 Les ensembles \mathbb{R}^* et \mathbb{R}_+^* , l'ensemble \mathbb{U} des nombres complexes dont le module est égal à 1 et, pour tout entier $n \geq 1$, l'ensemble \mathbb{U}_n des racines n -ièmes de l'unité sont des groupes multiplicatifs.

Pour tout entier $n \geq 1$, l'ensemble $GL_n(\mathbb{R})$ des matrices inversibles de taille n est un groupe multiplicatif.

L'ensemble $SL_n(\mathbb{R}) = [\det M = 1]$, l'ensemble $O_n(\mathbb{R})$ des matrices orthogonales, l'ensemble $SO_n(\mathbb{R})$ des matrices de rotation sont des sous-groupes de $GL_n(\mathbb{R})$.

8.4 Pour tout entier $n \geq 1$, l'ensemble \mathfrak{S}_n des permutations de $\{1, \dots, n\}$ est un groupe pour \circ .

L'ensemble \mathfrak{A}_n des permutations dont la signature est égale à 1 est un sous-groupe de \mathfrak{S}_n .

L'ensemble $O(\mathbb{R}^n)$ des isométries vectorielles de \mathbb{R}^n est un groupe pour \circ .

Si A est une partie quelconque de \mathbb{R}^n (un point, une droite, une sphère...), l'ensemble des isométries $f \in O(\mathbb{R}^n)$ qui fixent A :

$$\forall x \in A, \quad f(x) = x$$

est un sous-groupe de $O(\mathbb{R}^n)$.

Si A est une partie finie de \mathbb{R}^n (les quatre sommets d'un carré, ceux d'un tétraèdre...), l'ensemble des isométries $f \in O(\mathbb{R}^n)$ qui laissent A invariant :

$$\forall x \in A, \quad f(x) \in A$$

est un sous-groupe de $O(\mathbb{R}^n)$.

L'ensemble des translations de \mathbb{R}^n est un groupe pour \circ .

8.5 Pour tout ensemble E , l'ensemble $\mathfrak{P}(E)$ des parties de E est un groupe pour la différence symétrique Δ . L'élément neutre est l'ensemble vide \emptyset . Chaque partie A est son propre symétrique.

8.6 La structure de groupe intervient dans la définition des structures d'espace vectoriel, d'anneau et de corps.

1.2 Morphismes de groupes

9. \Leftarrow Soient $(G, *)$ et (H, \otimes) , deux groupes. Une application

$$\varphi : G \rightarrow H$$

est un **morphisme (de groupes)** lorsque

$$\forall x, y \in G, \quad \varphi(x * y) = \varphi(x) \otimes \varphi(y).$$

10. Si φ est un morphisme de groupes de $(G, *)$ dans (H, \otimes) , alors

$$\varphi(e_G) = e_H$$

$$\forall x \in G, \quad \varphi(x^{-1}) = [\varphi(x)]^{-1}$$

$$\forall x \in G, \forall n \in \mathbb{Z}, \quad \varphi(x^n) = [\varphi(x)]^n.$$

11. Si $\varphi : G \rightarrow H$ et $\psi : H \rightarrow K$ sont deux morphismes de groupes, alors leur composée

$$\psi \circ \varphi : G \rightarrow K$$

est un morphisme de groupes.

12. Exemples de morphismes

12.1 Les fonctions

$$\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times) \quad \text{et} \quad \ell n : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$$

sont des morphismes de groupes.

12.2 L'application $[u \mapsto T_u]$ qui, à un vecteur $u \in \mathbb{R}^2$, associe la translation T_u de vecteur u est un morphisme de $(\mathbb{R}^2, +)$ dans le groupe des translations de \mathbb{R}^2 .

12.3 L'application

$$\left[\theta \mapsto \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \right]$$

est un morphisme de $(\mathbb{R}, +)$ dans $(SO_2(\mathbb{R}), \times)$. C'est aussi un morphisme de $(\mathbb{Z}, +)$ ou de $(2\pi\mathbb{Z}, +)$ dans $(SO_2(\mathbb{R}), \times)$.

12.4 La **signature** ε est un morphisme de \mathfrak{S}_n dans $(\{\pm 1\}, \times)$.

12.5 Le **déterminant** est un morphisme de $GL_n(\mathbb{R})$ dans \mathbb{R}^* .

12.6 Automorphisme intérieur

Pour tout élément a d'un groupe (G, \star) , l'application

$$[x \mapsto a^{-1} \star x \star a]$$

est un morphisme de G dans G .

13. → Soit φ , un morphisme de groupes de (G, \star) dans (H, \otimes) .

13.1 L'image par φ d'un sous-groupe de (G, \star) est un sous-groupe de (H, \otimes) .

13.2 L'image réciproque par φ d'un sous-groupe de (H, \otimes) est un sous-groupe de (G, \star) .

14. Surjectivité d'un morphisme

Soit φ , un morphisme de groupes de (G, \star) dans (H, \otimes) .

14.1 \Leftarrow L'image d'un morphisme de groupes $\varphi : G \rightarrow H$ est définie par

$$\text{Im } \varphi = \{ \varphi(x), x \in G \}.$$

14.2 L'image d'un morphisme $\varphi : G \rightarrow H$ est un sous-groupe de (H, \otimes) .

14.3 \rightarrow Le morphisme $\varphi : G \rightarrow H$ est surjectif si, et seulement si, son image est égale au groupe d'arrivée : $\text{Im } \varphi = H$.

15. Injectivité d'un morphisme

Soit φ , un morphisme de groupes de (G, \star) dans (H, \otimes) .

15.1 \Leftarrow Le **noyau** d'un morphisme de groupes $\varphi : G \rightarrow H$ est défini par

$$\text{Ker } \varphi = \{ x \in G : \varphi(x) = e_H \}.$$

15.2 Le noyau d'un morphisme $\varphi : G \rightarrow H$ est un sous-groupe de (G, \star) .

15.3 \rightarrow Le morphisme $\varphi : G \rightarrow H$ est injectif si, et seulement si, son noyau est réduit à l'élément neutre :

$$\text{Ker } \varphi = \{ e_G \}.$$

16. Morphismes bijectifs

Soient (G, \star) et (H, \otimes) , deux groupes.

16.1 \Leftarrow Un morphisme de groupes $\varphi : G \rightarrow H$ est un **isomorphisme (de groupes)** lorsqu'il est bijectif.

16.2 \Leftarrow Un **automorphisme (de groupes)** est un isomorphisme de G sur G .

16.3 \rightarrow Si $\varphi : G \rightarrow H$ est un isomorphisme de groupes, alors sa bijection réciproque $\varphi^{-1} : H \rightarrow G$ est un isomorphisme de groupes.

1.3 Produits de groupes

17. Il n'y a pas de différence essentielle entre le produit de deux groupes et le produit d'un nombre fini quelconque de groupes : la généralisation des résultats est évidente.

18. Soient (G, \star) et (H, \otimes) , deux groupes. Sur le produit

$$G \times H = \{ (g, h), g \in G, h \in H \},$$

on définit l'opération \bullet par

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \star g_2, h_1 \otimes h_2).$$

- 18.1 L'ensemble $G \times H$ est un groupe pour l'opération \bullet .
 18.2 \Leftrightarrow Le groupe $(G \times H, \bullet)$ est appelé le **groupe produit** de (G, \star) et de (H, \otimes) .
 18.3 Le groupe produit $(G \times H, \bullet)$ est commutatif si, et seulement si, les deux groupes (G, \star) et (H, \otimes) sont commutatifs.

19. Morphismes

- 19.1 \Leftrightarrow Les **projections canoniques** sont les applications définies par

$$\pi_G : G \times H \rightarrow G \quad \text{et} \quad \pi_H : G \times H \rightarrow H \\ (g, h) \mapsto g \quad \text{et} \quad (g, h) \mapsto h.$$

- 19.2 \Leftrightarrow Les **injections canoniques** sont les applications définies par

$$i_G : G \rightarrow G \times H \quad \text{et} \quad i_H : H \rightarrow G \times H \\ g \mapsto (g, e_H) \quad \text{et} \quad h \mapsto (e_G, h).$$

- 19.3 Les projections canoniques π_G et π_H sont des morphismes de groupes surjectifs.
 19.4 Les injections canoniques i_G et i_H sont des morphismes de groupes injectifs.
 19.5 \rightarrow Une application

$$\theta : L \rightarrow G \times H \\ x \mapsto (\varphi(x), \psi(x))$$

est un morphisme de groupes de (L, \top) dans $(G \times H, \bullet)$ si, et seulement si, les applications $\varphi : L \rightarrow G$ et $\psi : L \rightarrow H$ sont des morphismes de groupes.

I.4 Sous-groupe engendré par un élément

20. Parties génératrices d'un groupe

On considère un groupe (G, \star) et une partie S de G .

- 20.1 L'intersection G_1 des sous-groupes H de G contenant S est un sous-groupe de G qui contient S .
 Tout sous-groupe de G qui contient S contient aussi G_1 .
 20.2 L'ensemble G_2 des $x \in G$ tels que

$$\exists n \in \mathbb{N}^*, \exists (s_1, \dots, s_n) \in S^n, \exists (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n, \\ x = s_1^{\alpha_1} \star \dots \star s_n^{\alpha_n}.$$

est un sous-groupe de G qui contient S .

Tout sous-groupe de G qui contient S contient aussi G_2 .

- 20.3 \Leftrightarrow Soient (G, \star) , un groupe et S , une partie de G . Le **sous-groupe engendré par S** , noté $\langle S \rangle$, est le plus petit sous-groupe H de G tel que $S \subset H$.

21. Exemples

- 21.1 Si a_1, \dots, a_p commutent deux à deux, un élément x de G appartient au sous-groupe engendré par a_1, \dots, a_p si, et seulement si,

$$\exists (\alpha_1, \dots, \alpha_p) \in \mathbb{Z}^p, \quad x = a_1^{\alpha_1} \star \dots \star a_p^{\alpha_p}$$

ou, dans le cas où $\star = +$,

$$\exists (\alpha_1, \dots, \alpha_p) \in \mathbb{Z}^p, \quad x = \sum_{k=1}^p \alpha_k a_k.$$

- 21.2 Le groupe $(\mathbb{Z}, +)$ est engendré par 1.

- 21.3 Le groupe (\mathbb{U}_n, \times) des racines n -ièmes de l'unité est engendré par $\exp(2i\pi/n)$.

- 21.4 Le groupe symétrique (\mathfrak{S}_n, \circ) est engendré par les transpositions $\tau_{i,j}$, $1 \leq i < j \leq n$.

Il est aussi engendré par les transpositions $\tau_{1,i}$, $1 \leq i \leq n$, ainsi que par la transposition $\tau_{1,2}$ et le cycle $(1 \ 2 \ 3 \ \dots \ n)$.

Il est enfin engendré par la famille des cycles.

- 21.5 Le groupe $(GL_n(\mathbb{R}), \times)$ est engendré par les matrices de transvection et les matrices de dilatation.

22. \rightarrow Dans un groupe multiplicatif, le sous-groupe $\langle a \rangle$ engendré par un élément $a \in G$ peut être décrit en extension :

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

Dans un groupe additif,

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

23. Groupes monogènes

- 23.1 \Leftrightarrow Un groupe (G, \star) est **monogène** lorsqu'il est engendré par un élément de G :

$$\exists a \in G, \quad \langle a \rangle = G.$$

- 23.2 Un groupe monogène est commutatif.

- 23.3 Le groupe $(\mathbb{Z}, +)$ est monogène.

- 23.4 Pour tout entier $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z}$ est un sous-groupe monogène de $(\mathbb{Z}, +)$. \rightarrow [8.2]

- 23.5 Si G est un sous-groupe de $(\mathbb{Z}, +)$ qui n'est pas réduit à $\{0\}$, alors l'ensemble $G_0 = G \cap \mathbb{N}^*$ possède un plus petit élément.

- 23.6 \rightarrow Tout sous-groupe H de $(\mathbb{Z}, +)$ est monogène et il existe un, et un seul, entier $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

24. Groupes cycliques

- 24.1 \Leftrightarrow Un groupe (G, \star) est **cyclique** lorsqu'il est monogène et fini.

- 24.2 \Leftrightarrow L'**ordre d'un groupe** (G, \star) est le cardinal de l'ensemble G .

- 24.3 Le groupe (\mathbb{U}_n, \times) est cyclique.

25. Classification des groupes monogènes

Pour tout élément a de G , on considère l'application φ_a de \mathbb{Z} dans G définie par

$$\varphi_a = [k \mapsto a^k]$$

ou par $\varphi_a = [k \mapsto k \cdot a]$ si l'opération sur G est une addition.

- 25.1 L'application φ_a est un morphisme de groupes de $(\mathbb{Z}, +)$ dans (G, \star) .

- 25.2 L'image de φ_a est le sous-groupe $\langle a \rangle$.

- 25.3 Il existe un, et un seul, entier $n \in \mathbb{N}$ tel que le noyau de φ_a soit égal à $n\mathbb{Z}$. Si $n \geq 1$, le sous-groupe $\langle a \rangle$ est constitué de n éléments :

$$\langle a \rangle = \{e_G, a, \dots, a^{n-1}\}$$

et $a^n = e_G$.

- 25.4 \rightarrow Un groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.

Un groupe cyclique d'ordre $n \in \mathbb{N}$ est isomorphe à (\mathbb{U}_n, \times) .

I.5 Ordre d'un élément

- 26.1 \Leftrightarrow L'**ordre d'un élément** $a \in G$ est l'ordre du sous-groupe $\langle a \rangle$.

- 26.2 \rightarrow Si $a \in G$ est un élément d'ordre d , alors

$$\langle a \rangle = \{e_G, a, a^2, \dots, a^{d-1}\}.$$

Si G est un groupe additif,

$$\langle a \rangle = \{0_G, a, 2 \cdot a, \dots, (d-1) \cdot a\}.$$

- 26.3 \rightarrow Si l'ordre d'un élément $a \in G$ est égal à d , alors

$$a^n = e_G \iff d \mid n.$$

Dans un groupe additif,

$$n \cdot a = 0_G \iff d \mid n.$$

- 26.4 Un groupe G d'ordre n est cyclique si, et seulement si, il existe un élément $a \in G$ d'ordre n .

27. Théorème de Lagrange

- 27.1 Soit (G, \star) , un groupe commutatif d'ordre $n \in \mathbb{N}^*$.

Pour tout $a \in G$, l'application $[x \mapsto a \star x]$ est une bijection de G sur G , donc

$$\prod_{x \in G} x = \prod_{x \in G} (a \star x)$$

et $a^n = e_G$.

- 27.2 \rightarrow Si (G, \star) est un groupe fini, alors l'ordre de tout élément a de G divise l'ordre de G .

- 27.3 Le théorème [27.2] est vrai également pour les groupes non commutatifs. \rightarrow [100]

Entraînement**28. Questions pour réfléchir**

- 1.a L'élément neutre d'un groupe est son propre symétrique.
- 1.b Si un élément d'un groupe est son propre symétrique, s'agit-il de l'élément neutre ?
2. Si x, y et z sont trois éléments d'un groupe $(G, *)$ tels que $x * z = y * z$, alors $x = y$.
3. Soit $G = \mathfrak{P}(E)$.
- 3.a Il existe un élément neutre dans G pour l'opération \cap , mais seul E admet un symétrique dans G pour cette opération.
- 3.b Il existe un élément neutre dans G pour l'opération \cup , mais seul \emptyset admet un symétrique dans G pour cette opération.
4. Deux éléments x et y d'un groupe $(G, *)$ commutent :

$$x * y = y * x$$

si, et seulement si :

$$\forall n, p \in \mathbb{Z}, \quad x^n * y^p = y^p * x^n.$$

5. Si H est une partie non vide de G telle que

$$\forall x, y \in H, \quad x * y^{-1} \in H,$$

alors H est un sous-groupe de $(G, *)$.

6. Soient A et B , deux sous-groupes de $(G, *)$.
- 6.a S'il existe $a \in A \cap B^c$ et $b \in B \cap A^c$, alors $a * b$ n'appartient ni à A , ni à B .
- 6.b L'union $A \cup B$ est un sous-groupe de $(G, *)$ si, et seulement si, $A \subset B$ ou $B \subset A$.
7. Si A est une partie de \mathbb{C}^* constituée de n éléments et stable par multiplication, alors $A = \mathbb{U}_n$.
8. Si une partie finie non vide d'un groupe G est stable par multiplication, alors c'est un sous-groupe de G .
9. Réécrire les propriétés [10] en supposant que G et H soient des groupes *additifs*.
10. Si $\varphi : G \rightarrow H$ et $\psi : G \rightarrow H$ sont deux morphismes de groupes, leur produit, défini par

$$\forall x \in G, \quad (\varphi \otimes \psi)(x) = [\varphi(x)] \otimes [\psi(x)],$$

est-il un morphisme de groupes ?

11. L'application

$$[M \mapsto {}^t M M]$$

est un morphisme de groupes de $\text{GL}_n(\mathbb{R})$ dans lui-même. Relier les groupes $O_n(\mathbb{R})$ et $\text{SO}_n(\mathbb{R})$ à ce morphisme.

12. Soit $\varphi : G \rightarrow H$, un morphisme de groupes.
- 12.a Si le groupe G est commutatif, alors $\text{Im } \varphi$ est un sous-groupe commutatif de H .
- 12.b Le noyau de φ est un **sous-groupe distingué** de G :

$$\forall a \in \text{Ker } \varphi, \forall x \in G, \quad x^{-1} a x \in \text{Ker } \varphi.$$

13. Si (G, \star) est un groupe commutatif, alors l'application

$$[x \mapsto x^n] : G \rightarrow G$$

est un morphisme de groupe pour tout entier $n \in \mathbb{Z}$.

14. Pour tout $a \in G$, l'application $[x \mapsto a^{-1} \star x \star a]$ est un automorphisme de G . Les points fixes de cet automorphisme sont les éléments de G qui commutent à a .

15. L'ensemble des automorphismes d'un groupe (G, \star) est un groupe pour \circ .

16. Suite de [19] –

$$\begin{array}{ll} \text{Im } i_G = \text{Ker } \pi_H & \text{Im } i_H = \text{Ker } \pi_G \\ \pi_G \circ i_G = I_G & \pi_H \circ i_H = I_H \end{array}$$

Étudier les morphismes $i_G \circ \pi_G$ et $i_H \circ \pi_H$.

17. Soient φ et ψ , deux morphismes de groupes de (G, \star) dans (H, \otimes) . L'application θ définie par

$$\forall x \in G, \quad \theta(x) = \varphi(x) \otimes \psi(x)$$

est-elle un morphisme de groupes ?

18. Le groupe (\mathbb{U}, \times) est-il monogène ?
19. Pour $n \geq 3$, le groupe symétrique (\mathfrak{S}_n, \circ) n'est pas cyclique.

29. Sous-groupes d'un groupe monogène [25]

29.1 L'image réciproque d'un sous-groupe H de (G, \star) par le morphisme $\varphi_a : \mathbb{Z} \rightarrow G$ est un sous-groupe de $(\mathbb{Z}, +)$.

29.2 Un sous-groupe d'un groupe monogène est monogène.

30. Groupes cycliques et morphismes

Soit $\langle a \rangle$, un groupe cyclique d'ordre $n \in \mathbb{N}^*$.

30.1 Soient f et g , deux morphismes de groupes de $\langle a \rangle$ dans H . Si $f(a) = g(a)$, alors $f = g$.

30.2 Pour tout morphisme de groupes $f : \langle a \rangle \rightarrow H$, l'ordre de $f(a)$ est un diviseur de n .

30.3 Soit $\langle y_0 \rangle$, un sous-groupe cyclique d'ordre q de H tel que q divise n .

1. Si $a^{k_1} = a^{k_2}$, alors $y_0^{k_1} = y_0^{k_2}$.

2. L'application $f = [a^k \mapsto y_0^k]$ est un morphisme de groupes de $\langle a \rangle$ dans H , dont l'image est $\langle y_0 \rangle$.

30.4 Exemples

1. Le seul morphisme de groupes de \mathbb{U}_5 dans \mathbb{U}_6 est le morphisme trivial : $[x \mapsto 1]$.

2. Si f est un automorphisme de \mathbb{U}_4 , alors $f(i)$ est un élément d'ordre 4. Les automorphismes de \mathbb{U}_4 sont $[x \mapsto x]$ et $[x \mapsto \bar{x}]$.

3. Il existe autant de morphismes de groupes de \mathbb{U}_n dans \mathbb{U}_m que d'éléments de \mathbb{U}_m dont l'ordre divise n .

31. Racines primitives de l'unité

Une racine n -ième de l'unité est une **racine primitive** lorsqu'elle engendre le groupe \mathbb{U}_n .

1. La racine n -ième de l'unité $\zeta_k = \exp(2ik\pi/n)$ est une racine primitive si, et seulement si, l'entier k est premier à n .

2. Décrire, en fonction de k , le sous-groupe de \mathbb{U}_n engendré par ζ_k .

II**Anneaux et corps**

32. La structure d'**anneau** permet d'ajouter, soustraire et multiplier. Dans un **corps**, on peut en outre diviser (mais pas par zéro!).

33. Structure d'anneau

Un **anneau** est un triplet $(A, +, \star)$ constitué d'un ensemble A et de deux lois de composition interne : une **addition**, notée $+$, et une **multiplication**, notée \star , qui suivent les règles de calcul suivantes.

33.1 Règles pour l'addition

Le couple $(A, +)$ est un groupe commutatif. L'élément neutre pour $+$ est noté 0_A (ou 0).

33.2 Règles pour la multiplication

La multiplication \star est une loi interne associative et il existe un élément neutre pour \star (structure d'**anneau unitaire**).

33.3 Distributivité

La multiplication est **distributive à gauche** par rapport à l'addition :

$$\forall x, y, z \in A, \quad x \star (y + z) = x \star y + x \star z$$

et **distributive à droite** :

$$\forall x, y, z \in A, \quad (y + z) \star x = y \star x + z \star x.$$

34. \Leftrightarrow L'anneau $(A, +, \star)$ est **commutatif** lorsque la multiplication interne \star est commutative :

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

35. \rightarrow Dans un anneau $(A, +, \star)$, il existe un, et un seul, élément neutre pour \star . Il est souvent noté 1_A et appelé **élément unité**.

36. Sous-anneaux

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

36.1 \Leftrightarrow Une partie B de l'anneau A est un **sous-anneau** lorsque $(B, +, \star)$ est un anneau qui admet 1_A pour élément unité.

36.2 → Une partie B de l'anneau A est un sous-anneau si, et seulement si, elle contient l'élément unité :

$$1_A \in B$$

et est stable par différence et par produit :

$$\forall x, y \in B, \quad x - y \in B \quad \text{et} \quad x * y \in B.$$

37. Exemples et contre-exemples

On identifie un anneau $(A, +, *)$ à l'ensemble A lorsque les opérations sont usuelles.

37.1 Anneaux de nombres

1. Les ensembles \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des anneaux. L'ensemble des **entiers de Gauss** :

$$\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$$

est un sous-anneau de \mathbb{C} .

2. L'ensemble \mathbb{N} n'est pas un anneau.

37.2 Anneau des polynômes

3. L'ensemble $\mathbb{R}[X]$ des polynômes à coefficients réels et l'ensemble $\mathbb{R}(X)$ des fractions rationnelles à coefficients réels sont des anneaux.

4. Quel que soit l'entier $n \geq 1$, l'ensemble $\mathbb{R}_n[X]$ des polynômes dont le degré est inférieur à n n'est pas un anneau.

37.3 Anneaux de matrices

5. L'ensemble $\mathfrak{M}_n(\mathbb{C})$ des matrices carrées à coefficients complexes est un anneau (non commutatif).

Les ensembles $U_n(\mathbb{C})$ et $L_n(\mathbb{C})$ des matrices carrées triangulaires supérieures et triangulaires inférieures sont des anneaux (non commutatifs).

L'ensemble $D_n(\mathbb{C})$ des matrices carrées diagonales est un anneau commutatif.

6. L'ensemble $GL_n(\mathbb{C})$ des matrices inversibles n'est pas un anneau, pas plus que l'ensemble $O_n(\mathbb{R})$ des matrices orthogonales.

37.4 Anneau des endomorphismes

L'ensemble $L(E)$ des endomorphismes de E est un anneau. La loi multiplicative est \circ , l'élément unité est I_E .

37.5 Anneau booléen

Pour tout ensemble E , le triplet $(\mathfrak{P}(E), \Delta, \cap)$ est un anneau commutatif.

37.6 Familles sommables

L'ensemble $\ell^1(\mathbb{N})$ des familles complexes sommables indexées par \mathbb{N} est un anneau pour l'addition des suites et le produit de Cauchy.

II.1 Règles de calculs dans un anneau

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

38.1 ≙ Pour tout $x \in A$, on convient de

$$x^0 = 1_A$$

et on définit par récurrence :

$$\forall n \in \mathbb{N}, \quad x^{*(n+1)} = x^{*n} * x.$$

On peut noter x^n au lieu de x^{*n} lorsqu'il n'y a pas d'ambiguïté sur la multiplication utilisée.

38.2 →

$$\forall n, p \in \mathbb{N}, \quad x^n * x^p = x^p * x^n = x^{n+p}$$

38.3 →

$$\forall n, p \in \mathbb{N}, \quad (x^n)^p = x^{np}$$

38.4 → L'élément nul est **absorbant** pour la multiplication.

$$\forall x \in A, \quad x * 0_A = 0_A * x = 0_A$$

38.5 → Règle des signes

$$\begin{aligned} \forall x, y \in A, \quad (-x) * y &= x * (-y) = -(x * y) \\ (-x) * (-y) &= x * y \end{aligned}$$

39. Soient x et y , deux éléments de l'anneau $(A, +, *)$ qui commutent :

$$x * y = y * x.$$

39.1

$$\forall (n, p) \in \mathbb{N}, \quad x^n * y^p = y^p * x^n$$

39.2

$$\forall n \in \mathbb{N}, \quad (x * y)^n = x^n * y^n$$

39.3 → Formule du binôme

Si x et y sont deux éléments qui commutent, alors

$$\forall n \in \mathbb{N}, \quad (x + y)^n = \sum_{k=0}^n \binom{n}{k} \cdot x^k * y^{n-k}.$$

39.4 → Série géométrique

Si x et y sont deux éléments qui commutent, alors pour tout $n \in \mathbb{N}$,

$$\begin{aligned} (x - y) * \left(\sum_{k=0}^n x^k * y^{n-k} \right) &= \left(\sum_{k=0}^n x^k * y^{n-k} \right) * (x - y) \\ &= x^{n+1} - y^{n+1}. \end{aligned}$$

Éléments remarquables d'un anneau

40. Éléments inversibles

40.1 ≙ Soit $(A, +, *)$, un anneau. Un élément x de A est **inversible** lorsqu'il existe $y \in A$ tel que

$$x * y = y * x = 1_A.$$

40.2 Si x est inversible dans l'anneau $(A, +, *)$, alors il existe un, et un seul, élément y de A tel que $x * y = y * x = 1_A$.

40.3 Si x et y sont deux éléments inversibles de $(A, +, *)$, alors $x * y$ est inversible et

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

40.4 → L'ensemble A^* des éléments inversibles de l'anneau $(A, +, *)$ est un groupe pour la loi $*$.

41. Éléments nilpotents

Soit $(A, +, *)$, un anneau.

41.1 ≙ Un élément x de A est dit **nilpotent** lorsqu'il existe $n \in \mathbb{N}$ tel que $x^n = 0_A$.

41.2 Un élément nilpotent n'est pas inversible.

41.3 ≙ L'**indice de nilpotence** de x est le plus petit élément de

$$\{n \in \mathbb{N} : x^n = 0_A\}.$$

41.4 Si x est nilpotent, alors l'indice de nilpotence de x est le seul entier $n \in \mathbb{N}^*$ tel que $x^n = 0_A$ et $x^{n-1} \neq 0_A$.

41.5 Si $x^n = 0_A$, alors $(1_A - x)$ est inversible et

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

42. Diviseurs de zéro

42.1 ≙ Soit $(A, +, *)$, un anneau. Un élément x non nul de A est un **diviseur de zéro à gauche** (resp. **à droite**) lorsqu'il existe un élément y non nul de A tel que $x * y = 0_A$ (resp. $y * x = 0_A$).

42.2 Un diviseur de zéro n'est pas inversible.

42.3 Tout élément nilpotent non nul est un diviseur de zéro.

42.4 ≙ Un **anneau intègre** est un anneau commutatif sans diviseur de zéro.

II.2 Structure de corps

43. ≙ Un **corps (commutatif)** est un anneau commutatif $(A, +, *)$ dans lequel tout élément $x \in A$ distinct de 0_A est inversible dans A .

44. Le seul élément nilpotent d'un corps est l'élément nul.

45. Il n'y a pas de diviseur de zéro dans un corps.

46. Exemples et contre-exemples

46.1 Les anneaux \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des corps. L'anneau \mathbb{Z} n'est pas un corps : les seuls éléments inversibles sont 1 et -1 .

46.2 L'anneau $\mathbb{R}(X)$ des fractions rationnelles est un corps, mais l'anneau $\mathbb{R}[X]$ des polynômes n'est pas un corps : les seuls éléments inversibles sont les polynômes constants non nuls.

46.3 Les anneaux $\mathcal{M}_n(\mathbb{R})$ et $L(E)$ ne sont en général pas des corps.

47. Sous-corps

Soit $(\mathbb{L}, +, \star)$, un corps.

47.1 \Leftrightarrow Une partie \mathbb{K} de \mathbb{L} est un **sous-corps** lorsque $(\mathbb{K}, +, \star)$ est un corps qui admet $1_{\mathbb{L}}$ pour élément unité. On dit aussi que \mathbb{L} est une **extension** de \mathbb{K} .

47.2 \rightarrow Une partie \mathbb{K} de \mathbb{L} est un sous-corps si, et seulement si, elle contient l'élément unité :

$$1_{\mathbb{L}} \in \mathbb{K}$$

est stable par différence :

$$\forall x, y \in \mathbb{K}, \quad x - y \in \mathbb{K}$$

et stable par produit et passage à l'inverse :

$$\forall x, y \in \mathbb{K}, \quad x \star y^{-1} \in \mathbb{K}.$$

47.3 Soit \mathbb{K} , un sous-anneau du corps \mathbb{L} .

Tout élément $x \in \mathbb{K}$ admet un inverse dans \mathbb{L} .

Le sous-anneau \mathbb{K} est un sous-corps de \mathbb{L} si, et seulement si, il contient l'inverse de chacun de ses éléments.

47.4 Sous-corps de \mathbb{C}

Soit \mathbb{K} , un sous-corps de \mathbb{C} .

1. Le corps \mathbb{K} contient le corps \mathbb{Q} des nombres rationnels.
2. Le corps \mathbb{K} est dénombrable si, et seulement si, il est de dimension finie en tant qu'espace vectoriel sur \mathbb{Q} .
3. Si $\mathbb{R} \subset \mathbb{K} \subset \mathbb{C}$, alors \mathbb{K} peut être considéré comme un espace vectoriel réel et $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

II.3 Anneau des polynômes à coefficients dans un corps

48.1 \rightarrow Soit \mathbb{K} , un corps (commutatif). Il existe un espace vectoriel sur \mathbb{K} , noté $\mathbb{K}[X]$, qui admet une base dénombrable, notée $(X^n)_{n \in \mathbb{N}}$.

48.2 \Leftrightarrow Les vecteurs de $\mathbb{K}[X]$ sont les **polynômes** à coefficients dans \mathbb{K} en l'indéterminée X .

48.3 Pour tout polynôme $P \in \mathbb{K}[X]$, il existe une, et une seule, famille $(a_n)_{n \in \mathbb{N}}$ presque nulle de scalaires telle que

$$P = \sum_{n \in \mathbb{N}} a_n X^n = a_0 + a_1 X + a_2 X^2 + \dots$$

48.4 \Leftrightarrow Quels que soient les polynômes

$$P = \sum_{n \in \mathbb{N}} a_n X^n \quad \text{et} \quad Q = \sum_{n \in \mathbb{N}} b_n X^n$$

à coefficients dans \mathbb{K} , le **produit** PQ est le polynôme

$$PQ = \sum_{n \in \mathbb{N}} c_n X^n$$

où on a posé

$$\forall n \in \mathbb{N}, \quad c_n = \sum_{k=0}^n a_k b_{n-k}.$$

48.5 \rightarrow Muni de l'addition naturelle [48.1] et de la multiplication interne [48.4], l'ensemble $\mathbb{K}[X]$ est un anneau commutatif tel que

$$\forall n, p \in \mathbb{N}, \quad X^n X^p = X^{n+p}.$$

49. Dans l'expression d'un *polynôme*, la lettre X est un pur symbole de calcul, qui ne désigne aucun type d'objet mathématique particulier. Ce n'est ni un nombre, ni une matrice, ni un endomorphisme... Ce n'est donc pas une *variable* (qui appartiendrait à l'ensemble de départ d'une fonction), mais bien une **indéterminée**.

50. Si $P = a_0 + a_1 X + a_2 X^2 + \dots$ est un polynôme non nul, alors l'ensemble

$$\sigma(P) = \{k \in \mathbb{N} : a_k \neq 0\}$$

est une partie finie non vide de \mathbb{N} .

50.1 \Leftrightarrow Le **degré** d'un polynôme $P \neq 0$ est l'entier noté $\deg P$, égal à $\max \sigma(P)$.

Le degré du polynôme nul est, par convention, égal à $-\infty$.

50.2 \Leftrightarrow La **valuation*** d'un polynôme $P \neq 0$ est l'entier $\min \sigma(P)$.

La valuation du polynôme nul est, par convention, égale à $+\infty$.

50.3 \rightarrow Degré d'une somme

Soient P et Q , deux polynômes de $\mathbb{K}[X]$.

— Si $\deg P \neq \deg Q$, alors

$$\deg(P + Q) = \max\{\deg P, \deg Q\}.$$

— Si $\deg P = \deg Q$, alors

$$\deg(P + Q) \leq \deg P.$$

50.4 \rightarrow Degré d'un produit

$$\forall P, Q \in \mathbb{K}[X], \quad \deg(PQ) = \deg P + \deg Q$$

51. \rightarrow Division euclidienne dans $\mathbb{K}[X]$

Soient A et B , deux polynômes de $\mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple (Q, R) de polynômes de $\mathbb{K}[X]$ tels que

$$A = QB + R \quad \text{avec} \quad \deg R < \deg B.$$

Les polynômes Q et R sont appelés respectivement le **quotient** et le **reste** de la division euclidienne de A par B .

52. Soit $P \in \mathbb{K}[X]$.

52.1 \Leftrightarrow Un scalaire $\alpha \in \mathbb{K}$ est une **racine** de P lorsque le polynôme $(X - \alpha)$ divise P .

52.2 \Leftrightarrow La **multiplicité** de $\alpha \in \mathbb{K}$ en tant que racine de P est le plus grand entier m tel que le polynôme $(X - \alpha)^m$ divise P .

52.3 Le scalaire α est une racine de P si, et seulement si, sa multiplicité est supérieure à 1.

52.4 La multiplicité de α est supérieure à m si, et seulement si, $(X - \alpha)^m$ divise P .

52.5 Soit $(\alpha_k)_{k \in I}$, l'ensemble (éventuellement vide) des racines d'un polynôme $P \in \mathbb{K}[X]$ dans le corps \mathbb{K} . Pour tout $k \in I$, on note m_k , la multiplicité de α_k en tant que racine de P .

Le nombre de racines de P est le cardinal de l'ensemble I .

Le nombre de racines de P comptées avec multiplicité est égal à la somme des multiplicités m_k . Cette somme est supérieure au nombre de racines.

52.6 \rightarrow Soit $P \in \mathbb{K}[X]$, un polynôme non nul. Le nombre des racines de P , comptées avec multiplicité, est inférieur au degré de P .

53. Soit $\Omega \subset \mathbb{K}$.

53.1 \Leftrightarrow Une application $f : \Omega \rightarrow \mathbb{K}$ est une **application polynomiale** lorsqu'il existe une famille presque nulle de scalaires $(a_k)_{k \in \mathbb{N}}$ telle que

$$\forall x \in \Omega, \quad f(x) = \sum_{k \in \mathbb{N}} a_k x^k.$$

53.2 Tout $x \in \Omega$ tel que $f(x) = 0$ est une racine du polynôme défini par \rightarrow [82]

$$P = a_0 + a_1 X + a_2 X^2 + \dots$$

Si l'application f s'annule sur une partie infinie de \mathbb{K} , alors tous les scalaires a_k sont nuls.

53.3 \rightarrow Soit $f : \Omega \rightarrow \mathbb{K}$, une application polynomiale. Si Ω est une partie infinie de \mathbb{K} , alors il existe un unique polynôme $P \in \mathbb{K}[X]$ tel que

$$\forall x \in \Omega, \quad f(x) = P(x).$$

53.4 → Si la fonction polynomiale f définie par

$$f(x) = a_0 + a_1x + \dots + a_dx^d$$

est identiquement nulle sur une partie infinie Ω , alors les coefficients a_0, a_1, \dots, a_d sont tous nuls.

53.5 L'application polynomiale définie par

$$f(x) = x(x-1)(x-2) = 2x - 3x^2 + x^3$$

est identiquement nulle sur $\Omega = \{0, 1, 2\}$ alors que ses coefficients ne sont pas tous nuls.

II.4 Morphismes d'anneaux

54. Un morphisme d'anneaux est une application d'un ensemble A dans un ensemble B , compatible avec les structures d'anneaux définies sur A et B .

55. ↯ Soient $(A, +, \star)$ et (B, \oplus, \otimes) , deux anneaux. Une application $\varphi : A \rightarrow B$ est un **morphisme d'anneaux** lorsque

- (1) $\forall (x, y) \in A \star A, \quad \varphi(x + y) = \varphi(x) \oplus \varphi(y)$
- (2) $\forall (x, y) \in A \star A, \quad \varphi(x \star y) = \varphi(x) \otimes \varphi(y)$
- (3) $\varphi(1_A) = 1_B.$

56. Soit $\varphi : (A, +, \star) \rightarrow (B, \oplus, \otimes)$, un morphisme d'anneaux.

56.1 L'image $\varphi_*(A)$ du morphisme d'anneaux φ est un sous-anneau de (B, \oplus, \otimes) .

56.2 Si $(A, +, \star)$ est un anneau commutatif, alors l'image de φ est un sous-anneau commutatif de (B, \oplus, \otimes) .

56.3 Pour tout $x \in A$ et tout $n \in \mathbb{Z}$,

$$\varphi(n \cdot x) = n \cdot \varphi(x)$$

et en particulier, $\varphi(0_A) = 0_B$.

56.4 $\forall x \in A, \forall n \in \mathbb{N}, \quad \varphi(x^{*n}) = [\varphi(x)]^{\otimes n}$

56.5 Si x est un élément inversible de A , alors $\varphi(x)$ est un élément inversible de B et

$$[\varphi(x)]^{-1} = \varphi(x^{-1}).$$

56.6 Si $x \in A$ est nilpotent, alors $\varphi(x)$ est nilpotent et son indice de nilpotence est inférieur à celui de x .

57. **Noyau d'un morphisme d'anneaux**

57.1 ↯ Soit $\varphi : (A, +, \star) \rightarrow (B, \oplus, \otimes)$, un morphisme d'anneaux. Le **noyau** de φ est défini par

$$\text{Ker } \varphi = \{x \in A : \varphi(x) = 0_B\}.$$

57.2 Un morphisme est injectif si, et seulement si, son noyau est réduit à $\{0_A\}$.

57.3 Le noyau d'un morphisme d'anneaux $\varphi : A \rightarrow B$ n'est pas un sous-anneau de A .

58.1 ↯ Un **isomorphisme d'anneaux** de $(A, +, \star)$ sur (B, \oplus, \otimes) est une application bijective $\varphi : A \rightarrow B$ qui est un morphisme d'anneaux de $(A, +, \star)$ dans (B, \oplus, \otimes) .

58.2 Si le morphisme d'anneaux φ est une bijection de A sur B , alors sa bijection réciproque est un morphisme d'anneaux de (B, \oplus, \otimes) dans $(A, +, \star)$.

58.3 Si $\varphi : A \rightarrow B$ est un isomorphisme d'anneaux, alors $x \in A$ est inversible si, et seulement si, $\varphi(x) \in B$ est inversible.

II.5 Produit d'anneaux

59. Soient $(A_1, +, \star)$ et $(A_2, +, \otimes)$, deux anneaux. Sur le produit

$$A = A_1 \times A_2$$

on définit les opérations \oplus et \bullet par

$$\begin{aligned} (x_1, x_2) \oplus (y_1, y_2) &= (x_1 + y_1, x_2 + y_2) \\ (x_1, x_2) \bullet (y_1, y_2) &= (x_1 \star y_1, x_2 \otimes y_2). \end{aligned}$$

59.1 L'ensemble $A_1 \times A_2$ muni des opérations \oplus et \bullet est un anneau.

59.2 ↯ L'anneau $(A_1 \times A_2, \oplus, \bullet)$ est l'**anneau produit** de $(A_1, +, \star)$ par $(A_2, +, \otimes)$.

59.3 L'élément nul de l'anneau produit est $(0_{A_1}, 0_{A_2})$; l'élément unité est $(1_{A_1}, 1_{A_2})$.

59.4 L'élément (x_1, x_2) est inversible si, et seulement si, x_1 et x_2 sont inversibles. Dans ce cas,

$$(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1}).$$

59.5 L'anneau produit $(A_1 \times A_2, +, \bullet)$ est commutatif si, et seulement si, les deux anneaux $(A_1, +, \star)$ et $(A_2, +, \otimes)$ sont commutatifs.

59.6 L'anneau produit $(A_1 \times A_2, +, \bullet)$ n'est pas intègre :

$$(0, 1) \bullet (1, 0) = (0, 0)$$

même si les anneaux A_1 et A_2 sont intègres.

60. Morphismes

60.1 ↯ Les **projections canoniques** sont les applications définies par

$$\begin{aligned} \pi_1 : A_1 \times A_2 &\rightarrow A_1 & \pi_2 : A_1 \times A_2 &\rightarrow A_2 \\ (x_1, x_2) &\mapsto x_1 & (x_1, x_2) &\mapsto x_2. \end{aligned}$$

60.2 Les projections canoniques sont des morphismes d'anneaux surjectifs.

60.3 → Une application

$$\begin{aligned} \theta : L &\rightarrow A_1 \times A_2 \\ x &\mapsto (\varphi(x), \psi(x)) \end{aligned}$$

est un morphisme d'anneaux de $(L, +, \top)$ dans $(A_1 \times A_2, +, \bullet)$ si, et seulement si, les applications $\varphi : L \rightarrow A_1$ et $\psi : L \rightarrow A_2$ sont des morphismes d'anneaux.

60.4 Les injections définies par

$$\begin{aligned} i_1 : A_1 &\rightarrow A_1 \times A_2 & i_2 : A_2 &\rightarrow A_1 \times A_2 \\ x_1 &\mapsto (x_1, 0_{A_2}) & x_2 &\mapsto (0_{A_1}, x_2) \end{aligned}$$

ne sont pas des morphismes d'anneaux.

II.6 Idéaux d'un anneau commutatif

61. ↯ Soit $(A, +, \star)$, un anneau commutatif. Une partie I de A est un **idéal** de A lorsque

1. I est un sous-groupe de $(A, +)$
2. qui est **absorbant** pour \star :

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

62. → Le noyau d'un morphisme d'anneaux $\varphi : A \rightarrow B$ est un idéal de A .

63.1 Les idéaux d'un corps commutatif \mathbb{K} sont $\{0\}$ et \mathbb{K} .

63.2 Un morphisme d'anneaux d'un corps commutatif \mathbb{K} dans un corps commutatif \mathbb{L} est injectif. L'existence d'un tel morphisme permet de voir \mathbb{K} comme un sous-corps de \mathbb{L} .

64. **Idéal engendré par un élément**

64.1 Pour tout $x \in A$, l'ensemble

$$xA = \{x \star y, y \in A\}$$

est un idéal de A .

64.2 \Leftrightarrow Pour tout $x \in A$, l'idéal xA est appelé **idéal engendré par x** .

64.3 Soit I , un idéal de A . Alors :

$$x \in I \iff xA \subset I$$

et en particulier

$$I = A \iff 1_A \in I.$$

65. Opération sur les idéaux

65.1 Si I et J sont deux idéaux de A , alors $I \cap J$ est un idéal de A et tout idéal H contenu dans I et dans J est aussi contenu dans $I \cap J$.

65.2 Si I et J sont deux idéaux de A , alors $I + J$ est un idéal de A et tout idéal H qui contient I et J contient aussi $I + J$.

65.3 \triangleright L'idéal $xA + yA$ est le plus petit idéal de A contenant à la fois x et y .

Divisibilité et idéaux d'un anneau intègre

66. Anneaux intègres [42.4]

66.1 Un corps est un anneau intègre.

Les anneaux \mathbb{Z} et $\mathbb{K}[X]$, qui ne sont pas des corps, sont intègres. Les anneaux $\mathfrak{M}_3(\mathbb{R})$ et $\mathbb{Z}/6\mathbb{Z}$ ne sont pas intègres.

66.2 \rightarrow Simplification dans un anneau intègre

Soit A , un anneau intègre et $z \neq 0_A$. Si $x * z = y * z$, alors $x = y$.

67.1 \Leftrightarrow Dans un anneau intègre $(A, +, *)$, on dit que $x \in A$ **divise** $y \in A$ (ou que y est un **multiple** de x) lorsque

$$\exists q \in A, \quad y = q * x.$$

On note alors $x \mid y$.

67.2 \rightarrow

$$x \mid y \iff yA \subset xA$$

68. Éléments inversibles

68.1 Un élément x de A est inversible si, et seulement si, il divise 1_A .

68.2 \rightarrow Un élément x de A est inversible si, et seulement si, l'idéal xA est égal à A .

$$x \in A^* \iff xA = A$$

68.3 S'il existe $n \in \mathbb{N}^*$ tel que x^n soit inversible, alors x est inversible.

68.4 Exemples fondamentaux

1. Les éléments inversibles de \mathbb{Z} sont 1 et -1 .
2. Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls, c'est-à-dire les polynômes dont le degré est nul.

69. Éléments associés

69.1 \Leftrightarrow Deux éléments x et y d'un anneau intègre A sont **associés** lorsqu'ils engendrent le même idéal : $xA = yA$.

69.2 \rightarrow Deux éléments x et y de A sont associés si, et seulement si, il existe un élément inversible $u \in A^\times$ tel que $y = u * x$.

69.3 \triangleright Les éléments inversibles de A sont les éléments associés à 1_A .

70. Éléments irréductibles

Soit A , un anneau intègre.

70.1 \Leftrightarrow Un élément non nul de A qui peut s'écrire comme le produit de deux éléments non inversibles de A est dit **composé**.

70.2 Un entier $x \in \mathbb{N}$ est composé si, et seulement si, il existe deux entiers $y \geq 2$ et $z \geq 2$ tels que $x = yz$.

70.3 Un polynôme $P \in \mathbb{K}[X]$ est composé si, et seulement si, il existe deux polynômes Q_1 et Q_2 tels que $P = Q_1 Q_2$ avec $\deg Q_1 \geq 1$ et $\deg Q_2 \geq 1$.

70.4 Si x est le produit de deux éléments y et z non inversibles, alors

$$xA \subsetneq yA \subsetneq A \quad \text{et} \quad xA \subsetneq zA \subsetneq A.$$

70.5 \Leftrightarrow Un élément non nul de A est **irréductible** lorsqu'il n'est ni inversible, ni composé.

70.6 Si un élément irréductible x est factorisé sous la forme $x = y * z$ avec z non inversible, alors y est inversible. Autrement dit :

$$(xA \subsetneq yA) \implies (yA = A).$$

Idéaux des anneaux euclidiens

71. Les seuls anneaux intègres intéressants que nous rencontrerons sont l'anneau \mathbb{Z} des entiers relatifs et l'anneau $\mathbb{K}[X]$ des polynômes sur un corps $\mathbb{K} \subset \mathbb{C}$. Il se trouve que ces deux anneaux sont munis d'une division euclidienne, ce qui simplifie considérablement la structure de leurs idéaux : tous les idéaux sont engendrés par un élément. \rightarrow [64]

72. \rightarrow Idéaux de \mathbb{Z} [23.6]

Pour tout idéal I de \mathbb{Z} , il existe un, et un seul, entier $n \in \mathbb{N}$ tel que

$$I = n\mathbb{Z}.$$

73. Idéaux de $\mathbb{K}[X]$

Soit I , un idéal de $\mathbb{K}[X]$, non réduit à $\{0\}$.

73.1 Si P et Q sont deux polynômes appartenant à I , alors le reste de la division euclidienne de P par Q appartient à I .

73.2 L'idéal I est engendré par tout polynôme $P_0 \in I$ tel que

$$\deg P_0 = \min\{\deg P, P \in I \setminus \{0\}\}.$$

73.3 \rightarrow Pour tout idéal $I \subset \mathbb{K}[X]$ non réduit à $\{0\}$, il existe un, et un seul, polynôme unitaire $P_0 \in \mathbb{K}[X]$ tel que I soit engendré par P_0 .

74. Éléments normalisés

La notion d'**élément normalisé** a pour seul but de donner une représentation unique des idéaux de l'anneau A . \rightarrow [74.4]

74.1 \Leftrightarrow Un élément x de \mathbb{Z} est **normalisé** lorsqu'il appartient à \mathbb{N}^* (entier positif).

74.2 \Leftrightarrow Un élément P de $\mathbb{K}[X]$ est **normalisé** lorsque son coefficient dominant est égal à 1 (polynôme unitaire).

74.3 Pour tout $x \in A$ non nul, il existe un, et un seul, élément normalisé $x_0 \in A$ associé à x .

74.4 \rightarrow Pour tout idéal I de $A = \mathbb{Z}$ ou de $A = \mathbb{K}[X]$ distinct de $\{0_A\}$, il existe un, et un seul, élément normalisé $x_0 \in A$ tel que $I = \langle x_0 \rangle$.

Entraînement

75. Questions pour réfléchir

1. Un sous-anneau d'un anneau commutatif est commutatif.
 2. Soient x et y , deux éléments d'un anneau A .
 - 2.a Si $xy = 1_A$, l'élément x est-il inversible ?
 - 2.b Si x est inversible et si $xy = 1_A$, alors $yx = 1_A$.
 3. Soit B , un sous-anneau de A . Un élément $x \in B$ peut être inversible en tant qu'élément de A sans être inversible en tant qu'élément de B .
 4. L'indice de nilpotence peut-il être nul ? égal à 1 ?
 5. L'indice de nilpotence de x est inférieur à n si, et seulement si, $x^n = 0$.
 6. Un produit d'éléments nilpotents est-il encore un élément nilpotent ?
 7. Dans quels cas particuliers les anneaux $\mathfrak{M}_n(\mathbb{R})$ et $L(E)$ sont-ils des corps ?
 8. Suite de [56] –
 - 8.a Est-il possible que $\varphi(x)$ soit inversible sans que x soit inversible ?
 - 8.b Si x est un diviseur de zéro, $\varphi(x)$ est-il encore un diviseur de zéro ?
 9. Quels sont les éléments nilpotents d'un anneau produit ?
 10. On suppose que les seuls idéaux de l'anneau commutatif A sont $\{0\}$ et A .
 - 10.a Si $x \neq 0$, alors l'élément unité 1_A appartient à l'idéal xA engendré par x .
 - 10.b L'anneau A est en fait un corps.
 11. Suite de [67.1] – Si un élément x non nul divise y , alors il existe un, et un seul, élément $q \in A$ tel que $y = q * x$.
 12. Pourquoi la notion de divisibilité est-elle sans intérêt dans un corps ?

III

Algèbres et polynômes

III.1 Structure d'algèbre

76. Algèbres associatives unitaires

Soit \mathbb{K} , un corps.

76.1 \Leftarrow Une algèbre associative unitaire sur \mathbb{K} est un ensemble A muni d'une structure d'espace vectoriel sur \mathbb{K} pour $(+, \cdot)$ et d'une structure d'anneau pour $(+, \cdot)$ telles que

$$\forall (\lambda, x, y) \in \mathbb{K} \times A^2, \quad (\lambda \cdot x) * y = \lambda \cdot (x * y) = x * (\lambda \cdot y).$$

76.2 Dans une algèbre associative unitaire A , si

$$a = \sum_{k=0}^m \alpha_k \cdot x_k \quad \text{et} \quad b = \sum_{\ell=0}^n \beta_\ell \cdot y_\ell,$$

alors

$$a * b = \sum_{k=0}^m \sum_{\ell=0}^n (\alpha_k \beta_\ell) \cdot (x_k * y_\ell).$$

76.3 \Leftarrow La dimension d'une algèbre $(A, +, *, \cdot)$ est la dimension (finie ou non) de l'espace vectoriel $(A, +, \cdot)$.

76.4 \Leftarrow L'élément unité d'une algèbre est l'élément neutre pour la multiplication interne.

76.5 \Leftarrow Les éléments inversibles d'une algèbre sont ceux qui ont un symétrique dans cette algèbre pour la multiplication interne.

76.6 L'ensemble des éléments inversibles d'une algèbre est muni d'une structure de groupe pour $*$.

77. Sous-algèbres

77.1 \Leftarrow Une sous-algèbre de $(A, +, *, \cdot)$ est une partie de A munie d'une structure d'algèbre associative unitaire pour les lois $+$, $*$ et \cdot .

77.2 Les sous-algèbres d'une algèbre sur le corps \mathbb{K} sont aussi des algèbres sur le corps \mathbb{K} .

78. Méthodes

78.1 $(A, +, *, \cdot)$ est une algèbre associative unitaire si, et seulement si, $(A, +, \cdot)$ est un espace vectoriel et si $*$ est une loi de composition interne, associative, admettant un élément neutre et bilinéaire de $A \times A$ dans A .

78.2 \rightarrow Une partie B de l'algèbre $(A, +, *, \cdot)$ est une sous-algèbre si, et seulement si, B est un sous-espace vectoriel de $(A, +, \cdot)$ qui contient l'élément unité et stable par $*$.

79. Morphismes d'algèbres

79.1 \Leftarrow Une application φ d'une algèbre $(A, +, *, \cdot)$ dans une algèbre $(B, +, \otimes, \cdot)$ est un morphisme d'algèbres lorsque φ est à la fois une application linéaire et un morphisme d'anneaux.

$$\begin{aligned} \forall (\lambda, x, y) \in \mathbb{K} \times A^2, \quad & f(\lambda x + y) = \lambda f(x) + f(y), \\ \forall (x, y) \in A^2, \quad & f(x * y) = f(x) \otimes f(y), \\ & f(1_A) = 1_B. \end{aligned}$$

79.2 En particulier, un morphisme d'algèbres possède toutes les propriétés d'un morphisme d'anneaux. \rightarrow [56]

79.3 \triangleright Si $f : A \rightarrow B$ est un morphisme d'algèbres bijectif, alors sa bijection réciproque est un morphisme d'algèbres.

79.4 \triangleright L'image d'un morphisme d'algèbres $f : A \rightarrow B$ est une sous-algèbre de B .

Exemples d'algèbres et de sous-algèbres

80.1 Le corps \mathbb{K} est une algèbre sur \mathbb{K} où la multiplication interne et la multiplication externe coïncident.

80.2 L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans \mathbb{K} est une algèbre sur \mathbb{K} .

80.3 L'ensemble $\mathbb{K}[X^2]$ des polynômes pairs est une sous-algèbre de $\mathbb{K}[X]$.

80.4 L'ensemble $\mathfrak{M}_n(\mathbb{K})$ des matrices carrées est une algèbre.

80.5 Les ensembles $D_n(\mathbb{K})$ des matrices diagonales; $U_n(\mathbb{K})$ des matrices triangulaires supérieures et $L_n(\mathbb{K})$ des matrices triangulaires inférieures sont des sous-algèbres de $\mathfrak{M}_n(\mathbb{K})$.

80.6 L'ensemble $L(E)$ des endomorphismes de E est une algèbre, qui a \circ pour multiplication interne.

80.7 L'ensemble $\mathcal{A}(\Omega, A)$ des applications d'un ensemble Ω dans une algèbre $(A, +, *, \cdot)$ est une algèbre dont la multiplication interne \otimes est définie par

$$\forall f, g, \quad (f \otimes g) = [x \mapsto f(x) * g(x)].$$

80.8 Lorsque $\Omega \subset \mathbb{K}$, l'ensemble des applications polynomiales de Ω dans \mathbb{K} est une sous-algèbre de $\mathcal{A}(\Omega, \mathbb{K})$.

81. Commutant

Soit $(A, +, *, \cdot)$, une algèbre.

81.1 \Leftarrow Le commutant* d'un élément $a \in A$ est la partie de A définie par

$$\{b \in A : a * b = b * a\}.$$

81.2 Le commutant de a est une sous-algèbre de A (pas nécessairement commutative).

III.2 Action des polynômes sur une algèbre

82. Les règles de calcul de la structure d'algèbre ont pour but de former des expressions polynomiales.

82.1 \Leftarrow Pour tout polynôme

$$P = \alpha_0 + \alpha_1 X + \dots + \alpha_d X^d \in \mathbb{K}[X]$$

et tout élément a d'une algèbre A sur le corps \mathbb{K} , l'évaluation en a du polynôme P est l'élément de l'algèbre A défini par

$$P(a) = \alpha_0 \cdot 1_A + \alpha_1 \cdot a + \dots + \alpha_d \cdot a^d.$$

82.2 On obtient $P(a)$ par substitution de $a \in A$ à l'indéterminée X . Il serait absurde de prendre $X = a$ dans l'expression de P : cela reviendrait en effet à déterminer le type de X .

82.3 Soit a , un élément de l'algèbre $(A, +, *, \cdot)$.

1.

$$(1)(a) = 1_A$$

2. Quels que soient P, Q dans $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$,

$$(\lambda P + Q)(a) = \lambda P(a) + Q(a).$$

3. Quels que soient P, Q dans $\mathbb{K}[X]$,

$$(PQ)(a) = P(a) * Q(a)$$

4. Si $P_1 = QP_0 + R$, alors

$$P_1(a) = Q(a) * P_0(a) + R(a).$$

82.4 \rightarrow Morphisme d'évaluation

Pour tout $a \in A$, l'application $\mathcal{E}_a : \mathbb{K}[X] \rightarrow A$ définie par

$$\forall P \in \mathbb{K}[X], \quad \mathcal{E}_a(P) = P(a)$$

est un morphisme d'algèbres.

82.5 Si $f : A \rightarrow B$ est un morphisme d'algèbres, alors

$$\forall P \in \mathbb{K}[X], \forall a \in A, \quad P(f(a)) = f(P(a)).$$

82.6 \rightarrow Soit $a \in A$. Si $b \in A$ est inversible, alors

$$P(b^{-1} * a * b) = b^{-1} * P(a) * b$$

pour tout polynôme $P \in \mathbb{K}[X]$.

83. Sous-algèbre engendrée par un élément

83.1 \Leftarrow La sous-algèbre des polynômes en $a \in A$ est l'image du morphisme \mathcal{E}_a . Elle est notée $\mathbb{K}[a]$.

$$\mathbb{K}[a] = \{P(a), P \in \mathbb{K}[X]\}$$

83.2 Minimalité de $\mathbb{K}[a]$

Si une sous-algèbre B de A contient l'élément a , alors $\mathbb{K}[a] \subset B$.

83.3 → La sous-algèbre $\mathbb{K}[a]$ est commutative et

$$\forall P \in \mathbb{K}[X], \quad P(a) * a = a * P(a).$$

84. Idéal annulateur

84.1 ⇔ Les polynômes annulateurs de $a \in A$ sont les polynômes P tels que $P(a) = 0_A$.

84.2 Un élément $a \in A$ est nilpotent si, et seulement si, il existe $d \in \mathbb{N}$ tel que X^d soit un polynôme annulateur de a .

84.3 → À tout polynôme annulateur non nul de a :

$$\alpha_0 + \alpha_1 X + \cdots + \alpha_d X^d$$

correspond une relation de liaison non triviale dans l'algèbre A :

$$\alpha_0 \cdot 1_A + \alpha_1 \cdot a + \cdots + \alpha_d \cdot a^d = 0_A.$$

84.4 ⇔ L'ensemble des polynômes annulateurs de $a \in A$ est le noyau du morphisme d'algèbres

$$\mathcal{E}_a = [P \mapsto P(a)] : \mathbb{K}[X] \rightarrow A.$$

On l'appelle **idéal annulateur** de a .

84.5 ⇔ Si l'idéal annulateur de a n'est pas réduit à $\{0\}$, alors l'unique polynôme unitaire qui engendre cet idéal est appelé **polynôme minimal** de a . → [73.3]

84.6 Si $\varphi : A \rightarrow B$ est un isomorphisme d'algèbres, alors $a \in A$ et $\varphi(a) \in B$ ont même polynôme minimal (s'ils en ont un).

84.7 → Soit A , une algèbre de dimension finie. Tout élément de a admet un polynôme minimal et le degré du polynôme minimal est inférieur à la dimension de A .

84.8 Toute matrice de $\mathcal{M}_n(\mathbb{K})$ admet un polynôme minimal.

84.9 Si E est un espace vectoriel de dimension finie, alors tout endomorphisme de E admet un polynôme minimal.

Entraînement**85. Questions pour réfléchir**

1. Le noyau d'un morphisme d'algèbres $f : A \rightarrow B$ est-il une sous-algèbre de A ?

2. Le sous-espace $\mathbb{K}_n[X]$ est-il une sous-algèbre de $\mathbb{K}[X]$?

3.a L'ensemble $GL_n(\mathbb{K})$ des matrices inversibles est-il une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$?

3.b Et l'ensemble $\mathcal{O}_n(\mathbb{R})$ des matrices orthogonales ?

3.c Et l'ensemble $\mathcal{S}_n(\mathbb{R})$ des matrices symétriques ?

3.d Et l'ensemble $U_n^0(\mathbb{K})$ des matrices triangulaires supérieures strictes (dont les coefficients diagonaux sont tous nuls) ?

3.e Et l'ensemble des matrices triangulaires ?

4. Condition pour que l'algèbre $\mathcal{A}(\Omega, E)$ soit une algèbre commutative ?

5. Suite de [81] – Comparer la sous-algèbre $\mathbb{K}[a]$ et le commutant de a pour $A = \mathcal{M}_n(\mathbb{K})$ et $a = I_n$.

6. Quels sont les polynômes annulateurs d'un élément nilpotent ?

7. L'élément a d'une algèbre admet un polynôme annulateur non nul si, et seulement si, la famille $(a^k)_{k \in \mathbb{N}}$ est liée.

8. Si $f \in L(E)$ et $\dim E \geq 2$, l'application $[P \mapsto P(f)]$ n'est pas surjective.

86. Soient A et B , deux algèbres. L'ensemble $\text{Hom}(A, B)$ des morphismes d'algèbres de A dans B est une sous-algèbre de l'algèbre $\mathcal{A}(A, B)$ des applications de A dans B .

87. Morphisme d'évaluation [82]**87.1 Sous-algèbre des applications polynomiales**

On considère $A = \mathcal{A}(\Omega, \mathbb{K})$ avec $\Omega \subset \mathbb{K}$.

1. La sous-algèbre $\mathcal{A}_0(\Omega, \mathbb{K})$ des applications polynomiales de Ω dans \mathbb{K} est l'image de \mathcal{E}_a avec $a = [x \mapsto x]$.

2. Le morphisme \mathcal{E}_a est injectif si, et seulement si, Ω est une partie infinie de \mathbb{K} .

87.2 Nombres algébriques, nombres transcendants

On suppose que $\mathbb{K} = \mathbb{Q}$ et $A = \mathbb{C}$. Le nombre a est dit **transcendant** lorsque \mathcal{E}_a est injective et **algébrique** dans le cas contraire.

1. La famille $(x_1, \dots, x_N) \in \mathbb{C}^N$ est liée si, et seulement si, il existe une famille (m_1, \dots, m_N) d'entiers relatifs non tous nuls tels que

$$m_1 x_1 + \cdots + m_N x_N = 0.$$

2. Un nombre a est algébrique si, et seulement si, il existe un polynôme $P \in \mathbb{Z}[X]$, non nul, tel que $P(a) = 0$.

3. On admet que π est transcendant. Quelle est la dimension de \mathbb{C} en tant qu'espace vectoriel sur \mathbb{Q} ?

4. Soit \mathfrak{P} , l'ensemble des nombres premiers. La famille $(\ell n p)_{p \in \mathfrak{P}}$ est une famille libre de \mathbb{C} . Comparer avec [3].

5. Existe-t-il $a \in \mathbb{C}$ tel que l'application \mathcal{E}_a soit surjective ?

6. Soit $a \in \mathbb{C}$, un nombre algébrique. Le **polynôme minimal** de a est l'unique générateur unitaire P_0 de l'idéal annulateur $\text{Ker } \mathcal{E}_a \subset \mathbb{Q}[X]$.

6.a En tant qu'élément de $\mathbb{Q}[X]$, le polynôme P_0 est irréductible.

6.b Si $a \neq 0$, alors le terme constant de P_0 n'est pas nul et il existe un polynôme $P_1 \in \mathbb{Q}[X]$ tel que $a^{-1} = P_1(a)$.

6.c L'algèbre $\mathbb{Q}[a]$ est un sous-corps de \mathbb{C} . En tant que \mathbb{Q} -espace vectoriel, elle admet

$$(1, a, \dots, a^{d-1})$$

pour base, où $d = \deg P_0$.

88.

1. L'application $[u \mapsto \mathcal{M}_{\mathcal{B}}(u)]$ est un isomorphisme d'algèbres de $L(E)$ sur $\mathcal{M}_n(\mathbb{K})$, pour toute base \mathcal{B} de E .

2. L'application $[M \mapsto Q^{-1}MQ]$ est un automorphisme d'algèbre de $\mathcal{M}_n(\mathbb{K})$ pour toute matrice $Q \in GL_n(\mathbb{K})$.

2.a L'application $[M \mapsto {}^t M]$ est-elle un isomorphisme d'algèbre de $\mathcal{M}_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$?

89. Inversibilité d'un polynôme en u

Soit $v \in \mathbb{K}[u]$.

1. Comparer $\mathbb{K}[v]$ et $\mathbb{K}[u]$.

2. On suppose que la dimension de $\mathbb{K}[u]$ est finie. Si v est inversible dans A , alors $v^{-1} \in \mathbb{K}[u]$.

90. Les matrices suivantes ont un polynôme minimal de degré 2.

$$\begin{pmatrix} 3 & 4 & -4 \\ -4 & -5 & 4 \\ -2 & -2 & 1 \end{pmatrix} \quad \begin{pmatrix} -4 & -6 & 6 \\ 6 & 8 & -6 \\ 3 & 3 & -1 \end{pmatrix}$$

$$\begin{pmatrix} -2 & 0 & 0 \\ -4 & 6 & -6 \\ -6 & 12 & -11 \end{pmatrix} \quad \begin{pmatrix} 5 & 4 & -4 \\ -4 & -3 & 4 \\ -2 & -2 & 3 \end{pmatrix}$$

91. Les matrices suivantes ont un polynôme minimal de degré 3.

$$\begin{pmatrix} 0 & -2 & 2 \\ -7 & -11 & 10 \\ -8 & -14 & 13 \end{pmatrix} \quad \begin{pmatrix} -7 & -8 & 8 \\ 2 & -1 & 0 \\ -2 & -6 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 7 & 10 & -8 \\ 8 & 12 & -9 \end{pmatrix}$$

Questions, exercices & problèmes

Perfectionnement

92. Exemples et contre-exemples

1. Les matrices

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

sont des éléments nilpotents de l'anneau $\mathfrak{M}_2(\mathbb{K})$, mais les produits AB et BA ne sont pas nilpotents.

2. Exemples de groupes cycliques; de groupes non cycliques.

3. Exemples d'algèbres commutatives? non commutatives?

4. Exemples d'algèbres de dimension finie? de dimension infinie?

5. Existe-t-il une sous-algèbre de $\mathbb{K}[X]$ qui ne soit pas de la forme $\mathbb{K}[X^n]$?

93. Méthodes

1. Comment déterminer l'ordre d'un élément?

2. Comment vérifier si un groupe est cyclique?

3. Construire un algorithme qui calcule la table [96].

4. Comment calculer le polynôme minimal [84.5] d'une matrice $A \in \mathfrak{M}_3(\mathbb{K})$?

94. Questions pour réfléchir

1. Quels algorithmes reposent-ils sur les factorisations du groupe symétrique [21.4]? du groupe linéaire [21.5]?

2. Un groupe d'ordre n contient-il un élément d'ordre n ?

3. On suppose qu'un groupe fini G contient un élément x d'ordre 3 et un élément y d'ordre 5.

3.a L'ordre de G est divisible par 15.

3.b Si $x * y = y * x$, alors G contient un élément d'ordre 15.

4. Pourquoi le groupe \mathfrak{S}_3 n'est-il pas cyclique?

5. Un diviseur de zéro est-il toujours nilpotent?

6. Suite de [50.2] –

6.a La valuation de la somme $P + Q$ est supérieure à la valuation de P et à la valuation de Q .

6.b La valuation du produit PQ est la somme des valuations de P et de Q .

7. Suite de [53.4] – Si $\Omega \subset \mathbb{K}$ est une partie finie, condition pour que les coefficients a_0, a_1, \dots, a_d soient tous nuls?

8. Tout sous-anneau d'un corps est intègre. Réciproquement, tout anneau intègre est en quelque sorte contenu dans un corps (**corps des fractions**).

9. Suite de [89] – Étudier le cas où la dimension de $\mathbb{K}[u]$ est infinie.

Approfondissement

95. Quaternions

On considère les quatre matrices complexes $I = I_2$,

$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad L = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

et on note \mathbb{H} , l'espace vectoriel réel engendré par ces matrices.

$$\mathbb{H} = \{aI + bJ + cK + dL, (a, b, c, d) \in \mathbb{R}^4\} \subset \mathfrak{M}_2(\mathbb{C})$$

L'ensemble \mathbb{H} des **quaternions** est une algèbre de dimension 4 sur \mathbb{R} ainsi qu'un corps non commutatif dont un sous-corps est isomorphe à \mathbb{C} .

96. Groupe diédral d'ordre 8

Le **groupe diédral** est le sous-groupe G de $GL_2(\mathbb{R})$ engendré par les deux matrices

$$S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

1. L'ensemble G est un sous-groupe de $O_2(\mathbb{R})$.

2. Comme $TS = ST^3$, alors

$$G = \{I_2, S, T, ST, T^2, ST^2, T^3, ST^3\}$$

et la table de multiplication de G est

	I_2	S	T	ST	T^2	ST^2	T^3	ST^3
$I_2 \times$	I_2	S	T	ST	T^2	ST^2	T^3	ST^3
$S \times$	S	I_2	ST	T	ST^2	T^2	ST^3	T^3
$T \times$	T	ST^3	T^2	S	T^3	ST	I_2	ST^2
$ST \times$	ST	T^3	ST^2	I_2	ST^3	T	S	T^2
$T^2 \times$	T^2	ST^2	T^3	ST^3	I_2	S	T	ST
$ST^2 \times$	ST^2	T^2	ST^3	T^3	S	I_2	ST	T
$T^3 \times$	T^3	ST	I_2	ST^2	T	ST^3	T^2	S
$ST^3 \times$	ST^3	T	S	T^2	ST	T^3	ST^2	I_2

3. Le groupe (G, \times) n'est pas isomorphe à (\mathbb{U}_8, \times) , ni à $(\mathbb{U}_2 \times \mathbb{U}_4, \times)$, ni à $(\mathbb{U}_2 \times \mathbb{U}_2 \times \mathbb{U}_2, \times)$.

4. L'ensemble des automorphismes de \mathbb{R}^2 qui laissent le carré unité globalement invariant est isomorphe au groupe G .

À chaque polygone régulier d'ordre $2n$ (carré, hexagone, octogone...) correspond un sous-groupe de $SO_2(\mathbb{R})$ qui est l'ensemble des automorphismes de \mathbb{R}^2 qui laissent ce polygone globalement invariant.

97. Exemples de parties génératrices

97.1 Le sous-groupe alterné \mathfrak{A}_n , constitué des permutations $\sigma \in \mathfrak{S}_n$ dont la signature est égale à 1, est engendré par les cycles de longueur 3.

97.2 Algorithme du pivot

1. Le sous-groupe $SL_n(\mathbb{R})$ des matrices dont le déterminant est égal à 1 est engendré par les matrices de transvection.

2. L'ensemble $SL_2(\mathbb{Z})$ des matrices de $\mathfrak{M}_2(\mathbb{Z})$ dont le déterminant est égal à 1 est un groupe pour \times . Il est engendré par les matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

97.3 Le groupe produit additif $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est engendré par $(\mathcal{E}_2(1), \mathcal{E}_3(1))$.

Pour aller plus loin

98. Soient H_1 et H_2 , deux sous-groupes de $(G, +)$.

98.1 La somme

$$H_1 + H_2 = \{x + y, (x, y) \in H_1 \times H_2\}$$

est un sous-groupe de G qui contient H_1 et H_2 .

98.2 En revanche, l'union $H_1 \cup H_2$ est un sous-groupe de G si, et seulement si,

$$H_1 \subset H_2 \quad \text{ou} \quad H_2 \subset H_1.$$

99. Soient A , un anneau intègre et I , un idéal de A . L'ensemble

$$J = \{x \in A : \exists n \in \mathbb{N}, x^n \in I\}$$

est un idéal de A .

100. Démonstration du théorème de Lagrange [27.2]

On pose H , un sous-groupe de G et, pour tout $x \in G$,

$$xH = \{x * y, y \in H\}.$$

1. Quel que soit $x \in G$, l'ensemble xH est l'image de H par la translation $[y \mapsto x * y]$, donc le cardinal de xH est égal au cardinal de H et

$$xH = H \iff x \in H.$$

2. La relation \mathcal{R} définie par

$$x \mathcal{R} y \iff xH = yH$$

est une relation d'équivalence sur G .

3. Si $x_1H \cap x_2H \neq \emptyset$, alors $x_1H = x_2H$.
4. Il existe x_1, \dots, x_q dans G tels que

$$G = \bigsqcup_{1 \leq k \leq q} x_k H$$

donc le cardinal de H divise l'ordre de G .

101. Applications polynomiales

Nous parlerons ici de *polynômes* alors qu'il s'agit en fait de *fonctions polynomiales*.

101.1 Un *monôme en d variables* est une application de \mathbb{K}^d dans \mathbb{K} de la forme

$$[x = (x_1, \dots, x_d) \mapsto x_1^{k_1} \cdots x_d^{k_d}]$$

où $(k_1, \dots, k_d) \in \mathbb{N}^d$.

101.2 L'espace des *polynômes en d variables*, noté $\mathbb{K}[x_1, \dots, x_d]$, est le sous-espace de $\mathcal{A}(\mathbb{K}^d, \mathbb{K})$ engendré par les monômes.

101.3 L'ensemble $\mathbb{K}[x_1, \dots, x_d]$ des polynômes en d variables est une algèbre associative unitaire.

101.4 Notation courte

Pour tout vecteur $x = (x_1, \dots, x_d) \in \mathbb{K}^d$ et tout **multi-indice**

$$k = (k_1, \dots, k_d) \in \mathbb{N}^d,$$

le produit

$$x_1^{k_1} \cdots x_d^{k_d} \in \mathbb{K}$$

sera noté simplement x^k .

Le produit x^k est nul si, et seulement si, l'une des coordonnées x_1, \dots, x_d est nulle.

101.5 Étant donnés deux multi-indices k et ℓ dans \mathbb{N}^d ,

$$\forall x \in \mathbb{K}^d, \quad x^{k+\ell} = x^k x^\ell.$$

101.6 Base canonique de $\mathbb{K}[x_1, \dots, x_d]$

1. Si la fonction polynomiale

$$[x \mapsto \sum_{k \in \mathbb{N}^d} \alpha_k x^k]$$

de \mathbb{K} dans \mathbb{K} est identiquement nulle sur \mathbb{K} , alors tous les coefficients α_k sont nuls.

2. Si $d \geq 2$, un polynôme de $\mathbb{K}[x_1, \dots, x_d]$ peut être considéré comme une fonction polynomiale en une variable x_d à coefficients dans $\mathbb{K}[x_1, \dots, x_{d-1}]$.

3. Pour tout $d \geq 1$ et tout polynôme $P \in \mathbb{K}[x_1, \dots, x_d]$, il existe une, et une seule, famille presque nulle $(\alpha_k)_{k \in \mathbb{N}^d}$ telle que

$$\forall x \in \mathbb{K}^d, \quad P(x) = \sum_{k \in \mathbb{N}^d} \alpha_k x^k.$$

4. On suppose que l'application polynomiale définie par

$$\forall x \in \mathbb{K}^d, \quad P(x) = \sum_{k \in \mathbb{N}^d} \alpha_k x^k$$

est identiquement nulle sur une partie Ω de \mathbb{K}^d .

4.a Si $\Omega = \mathbb{K}^d$, alors tous les coefficients α_k sont nuls.

4.b Il existe une partie infinie $\Omega_0 \subset \mathbb{R}^2$ telle que l'application polynomiale définie sur \mathbb{R}^2 par

$$P_0(x, y) = x^2 + y^2 - 1$$

soit identiquement nulle sur Ω alors que ses coefficients ne sont pas tous nuls.

4.c Condition suffisante sur $\Omega \subset \mathbb{K}^d$ pour que les coefficients de P soient tous nuls?

101.7 Degré d'un polynôme en d variables

Si $k = (k_1, \dots, k_d) \in \mathbb{N}^d$, le *degré du monôme* $[x \mapsto x^k]$ est

$$|k| = \sum_{i=1}^d k_i.$$

101.8 À tout polynôme $[x \mapsto \sum_{k \in \mathbb{N}^d} \alpha_k x^k]$ de $\mathbb{K}[x_1, \dots, x_d]$, on associe les ensembles

$$K = \{k \in \mathbb{N}^d : \alpha_k \neq 0\} \subset \mathbb{N}^d \quad \text{et} \quad |K| = \{|k|, k \in K\} \subset \mathbb{N}.$$

5. Les ensembles K et $|K|$ sont finis.

6. Un polynôme est un monôme si, et seulement si, K est un singleton.

101.9 Un polynôme est *homogène* lorsque l'ensemble $|K|$ est un singleton.

101.10 Le *degré d'un polynôme* est $\max(|K|)$. Sa *valuation* est $\min(|K|)$.

7. Que dire du degré de la somme de deux polynômes?

8. Écrire la formule donnant le produit de deux applications polynomiales. Que dire du degré du produit de deux polynômes?