6
Structures algébriques usuelles

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 ✍ *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 ✍ *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 ✍ *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 ➔ **Unicité du neutre**
Un groupe possède un seul élément neutre.
2.2 ➔ **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 ➔ **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 ✍ *On pose $x^0=e$ et, pour tout entier $n\geqslant 1$,*

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

3.2

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

3.3 ➔ **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.

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

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. ✍ *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 ➔ **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 ➔ **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 $(\mathbb{Z},+)$. →**[22.4]**
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 $n \geqslant 1$, l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité sont des groupes multiplicatifs.
Pour tout entier $n \geqslant 1$, l'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices inversibles de taille n est un groupe multiplicatif.
L'ensemble $\mathrm{SL}_n(\mathbb{R}) = [\det M = 1]$, l'ensemble $O_n(\mathbb{R})$ des matrices orthogonales, l'ensemble $\mathrm{SO}_n(\mathbb{R})$ des matrices de rotation sont des sous-groupes de $\mathrm{GL}_n(\mathbb{R})$.
8.4 Pour tout entier $n \geqslant 1$, 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 $\varnothing$. 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**.

I.2 Morphismes de groupes

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

$$\varphi : G \to H$$

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

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

10. Si φ est un morphisme de groupes de $(G,\star)$ 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. **Exemples de morphismes**
11.1 Les fonctions

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

sont des morphismes de groupes.
11.2 L'application $[\boldsymbol{u} \mapsto T_{\boldsymbol{u}}]$ qui, à un vecteur $\boldsymbol{u} \in \mathbb{R}^2$, associe la translation $T_{\boldsymbol{u}}$ de vecteur $\boldsymbol{u}$ est un morphisme de $(\mathbb{R}^2,+)$ dans le groupe des translations de $\mathbb{R}^2$.
11.3 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 $(\mathrm{SO}_2(\mathbb{R}),\times)$. C'est aussi un morphisme de $(\mathbb{Z},+)$ ou de $(2\pi\mathbb{Z},+)$ dans $(\mathrm{SO}_2(\mathbb{R}),\times)$.
11.4 La **signature** ε est un morphisme de $\mathfrak{S}_n$ dans $(\{\pm1\},\times)$.
11.5 Le **déterminant** est un morphisme de $\mathrm{GL}_n(\mathbb{R})$ dans $\mathbb{R}^*$.
11.6 **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.

12. ➔ *Soit φ, un morphisme de groupes de $(G,\star)$ dans $(H,\otimes)$.*
12.1 *L'image par φ d'un sous-groupe de $(G,\star)$ est un sous-groupe de $(H,\otimes)$.*
12.2 *L'image réciproque par φ d'un sous-groupe de $(H,\otimes)$ est un sous-groupe de $(G,\star)$.*

13. **Surjectivité d'un morphisme**
Soit φ, un morphisme de groupes de $(G,\star)$ dans $(H,\otimes)$.
13.1 ✍ *L'**image** d'un morphisme de groupes $\varphi : G \to H$ est définie par*

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

13.2 L'image d'un morphisme $\varphi : G \to H$ est un sous-groupe de $(H,\otimes)$.
13.3 ➔ *Le morphisme $\varphi : G \to H$ est surjectif si, et seulement si, son image est égale au groupe d'arrivée :* $\mathrm{Im}\,\varphi = H$.

14. **Injectivité d'un morphisme**
Soit φ, un morphisme de groupes de $(G,\star)$ dans $(H,\otimes)$.
14.1 ✍ *Le **noyau** d'un morphisme de groupes $\varphi : G \to H$ est défini par*

$$\mathrm{Ker}\,\varphi = \big\{x \in G : \varphi(x) = e_H\big\}.$$

14.2 Le noyau d'un morphisme $\varphi : G \to H$ est un sous-groupe de $(G,\star)$.
14.3 ➔ *Le morphisme $\varphi : G \to H$ est injectif si, et seulement si, son noyau est réduit à l'élément neutre :*

$$\mathrm{Ker}\,\varphi = \{e_G\}.$$

15. **Morphismes bijectifs**
Soient $(G,\star)$ et $(H,\otimes)$, deux groupes.
15.1 ✍ *Un morphisme de groupes $\varphi : G \to H$ est un **isomorphisme (de groupes)** lorsqu'il est bijectif.*
15.2 ✍ *Un **automorphisme (de groupes)** est un isomorphisme de G sur G.*
15.3 ➔ *Si $\varphi : G \to H$ est un isomorphisme de groupes, alors sa bijection réciproque $\varphi^{-1} : H \to G$ est un isomorphisme de groupes.*

I.3 Produits de groupes

16. 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.
17. Soient $(G,\star)$ et $(H,\otimes)$, deux groupes. Sur le produit

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

on définit l'opération $\bullet$ par

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

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

18. Morphismes

18.1 ✍ *Les **projections canoniques** sont les applications définies par*

$$\begin{array}{rcl} \pi_G : G\times H & \to & G \\ (g,h) & \mapsto & g \end{array} \quad et \quad \begin{array}{rcl} \pi_H : G\times H & \to & H \\ (g,h) & \mapsto & h \end{array}.$$

18.2 ✍ *Les **injections canoniques** sont les applications définies par*

$$\begin{array}{rcl} i_G : G & \to & G\times H \\ g & \mapsto & (g,e_H) \end{array} \quad et \quad \begin{array}{rcl} i_H : H & \to & G\times H \\ h & \mapsto & (e_G,h) \end{array}.$$

18.3 Les projections canoniques π_G et π_H sont des morphismes de groupes surjectifs.

18.4 Les injections canoniques i_G et i_H sont des morphismes de groupes injectifs.

18.5 ➔ *Une application*

$$\begin{array}{rcl} \theta : L & \to & G\times H \\ x & \mapsto & \big(\varphi(x),\psi(x)\big) \end{array}$$

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

I.4 Sous-groupe engendré par un élément

19. Parties génératrices d'un groupe

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

19.1 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.

19.2 L'ensemble G_2 des $x\in G$ tels que

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

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

19.3 ✍ *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 $S\subset H$.*

20. Exemples

20.1 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,

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

ou, dans le cas où $\star=+$,

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

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

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

20.4 Le groupe symétrique $(\mathfrak{S}_n,\circ)$ est engendré par les transpositions $\tau_{i,j}$, $1\leqslant i<j\leqslant n$.
Il est aussi engendré par les transpositions $\tau_{1,i}$, $1\leqslant i\leqslant n$, ainsi que par la transposition $\tau_{1,2}$ et le cycle $(1\quad 2\quad 3\quad\cdots\quad n)$.
Il est enfin engendré par la famille des cycles.

20.5 Le groupe $\big(\mathrm{GL}_n(\mathbb{R}),\times\big)$ est engendré par les matrices de transvection et les matrices de dilatation.

21. ➔ *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,

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

22. Groupes monogènes

22.1 ✍ *Un groupe $(G,\star)$ est **monogène** lorsqu'il est engendré par un élément de G :*

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

22.2 Un groupe monogène est commutatif.

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

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

23. Groupes cycliques

23.1 ✍ *Un groupe $(G,\star)$ est **cyclique** lorsqu'il est monogène et fini.*

23.2 ✍ *L'**ordre d'un groupe** $(G,\star)$ est le cardinal de l'ensemble G.*

23.3 Le groupe $(\mathbb{U}_n,\times)$ est cyclique.

24. 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.

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

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

24.3 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 $n\geqslant 1$, le sous-groupe $\langle a\rangle$ est constitué de n éléments :

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

et $a^n=e_G$.

24.4 ➔ *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

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

25.2 ➔ *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,

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

25.3 ➔ *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,

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

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

26. Théorème de Lagrange

26.1 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 $a^n=e_G$.

26.2 ➔ *Si $(G,\star)$ est un groupe fini, alors l'ordre de tout élément a de G divise l'ordre de G.*

26.3 Le théorème **[26.2]** est vrai également pour les groupes non commutatifs. →**[95]**

Entraînement

27. 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 $\varnothing$ 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. L'application

$$\left[M \mapsto {}^tMM\right]$$

est un morphisme de groupes de $\mathrm{GL}_n(\mathbb{R})$ dans lui-même. Relier les groupes $O_n(\mathbb{R})$ et $\mathrm{SO}_n(\mathbb{R})$ à ce morphisme.
10. Soit $\varphi : G \to H$, un morphisme de groupes.
10.a Si le groupe G est commutatif, alors $\operatorname{Im}\varphi$ est un sous-groupe commutatif de H.
10.b Le noyau de φ est un **sous-groupe distingué** de G :

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

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

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

est un morphisme de groupe pour tout entier $n \in \mathbb{Z}$.
12. Pour tout $a \in G$, l'application $\left[x \mapsto a^{-1} \star x \star a\right]$ est un automorphisme de G. Les points fixes de cet automorphisme sont les éléments de G qui commutent à a.
13. L'ensemble des automorphismes d'un groupe $(G, \star)$ est un groupe pour $\circ$.
14. *Suite de* **[18]** –

$$\operatorname{Im} i_G = \operatorname{Ker}\pi_H \qquad \operatorname{Im} i_H = \operatorname{Ker}\pi_G$$
$$\pi_G \circ i_G = \mathrm{I}_G \qquad \pi_H \circ i_H = \mathrm{I}_H$$

Étudier les morphismes $i_G \circ \pi_G$ et $i_H \circ \pi_H$.
15. 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 ?
16. Pour $n \geqslant 3$, le groupe symétrique $(\mathfrak{S}_n, \circ)$ n'est pas cyclique.

28. Sous-groupes d'un groupe monogène [24]
28.1 L'image réciproque d'un sous-groupe H de $(G, \star)$ par le morphisme $\varphi_a : \mathbb{Z} \to G$ est un sous-groupe de $(\mathbb{Z}, +)$.
28.2 Un sous-groupe d'un groupe monogène est monogène.

29. Groupes cycliques et morphismes
Soit $\langle a \rangle$, un groupe cyclique d'ordre $n \in \mathbb{N}^*$.
29.1 Soient f et g, deux morphismes de groupes de $\langle a \rangle$ dans H. Si $f(a) = g(a)$, alors $f = g$.
29.2 Pour tout morphisme de groupes $f : \langle a \rangle \to H$, l'ordre de $f(a)$ est un diviseur de n.
29.3 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 $\langle y_0 \rangle$.

29.4 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 $[x \mapsto \overline{x}]$.
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.

30. 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

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

32. ✍ 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.*
32.1 Règles pour l'addition
Le couple $(A, +)$ est un groupe commutatif. L'élément neutre pour $+$ est noté 0_A (ou 0).
32.2 Règles pour la multiplication
*La multiplication $\star$ est une loi interne associative et il existe un élément neutre pour $\star$ (structure d'**anneau unitaire**).*
32.3 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** :*

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

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

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

34. ➔ *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**.*

35. Sous-anneaux
Soit $(A, +, \star)$, un anneau.
35.1 ✍ *Une partie B de l'anneau A est un **sous-anneau** lorsque $(B, +, \star)$ est un anneau qui admet 1_A pour élément unité.*
35.2 ➔ *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 :

$$\forall\, x, y \in B, \quad x - y \in B \quad \textit{et} \quad x \star y \in B.$$

36. Exemples et contre-exemples
On identifie un anneau $(A,+,\star)$ à l'ensemble A lorsque les opérations sont usuelles.
36.1 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.
36.2 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 $n\geqslant 1$, l'ensemble $\mathbb{R}_n[X]$ des polynômes dont le degré est inférieur à n n'est pas un anneau.
36.3 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 $\mathrm{GL}_n(\mathbb{C})$ des matrices inversibles n'est pas un anneau, pas plus que l'ensemble $O_n(\mathbb{R})$ des matrices orthogonales.
36.4 Anneau des endomorphismes
L'ensemble $\mathrm{L}(E)$ des endomorphismes de E est un anneau. La loi multiplicative est $\circ$, l'élément unité est I_E.
36.5 Anneau booléen
Pour tout ensemble E, le triplet $(\mathfrak{P}(E),\Delta,\cap)$ est un anneau commutatif.
36.6 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

37. Soit $(A,+,\star)$, un anneau.
37.1 ✍ *Pour tout $x\in A$, on convient de*

$$x^0 = 1_A$$

et on définit par récurrence :

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

On peut noter x^n au lieu de $x^{\star n}$ lorsqu'il n'y a pas d'ambiguïté sur la multiplication utilisée.
37.2 ➔

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

37.3 ➔

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

37.4 ➔ *L'élément nul est **absorbant** pour la multiplication.*

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

37.5 ➔ **Règle des signes**

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

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

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

38.1

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

38.2

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

38.3 ➔ **Formule du binôme**
Si x et y sont deux éléments qui commutent, alors

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

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

$$(x-y)\star\Big(\sum_{k=0}^{n}x^k\star y^{n-k}\Big) = \Big(\sum_{k=0}^{n}x^k\star y^{n-k}\Big)\star(x-y)$$
$$= x^{n+1}-y^{n+1}.$$

Éléments remarquables d'un anneau

39. Éléments inversibles
39.1 ✍ *Soit $(A,+,\star)$, un anneau. Un élément x de A est **inversible** lorsqu'il existe $y\in A$ tel que*

$$x\star y = y\star x = 1_A.$$

39.2 Si x est inversible dans l'anneau $(A,+,\star)$, alors il existe un, et un seul, élément y de A tel que $x\star y = y\star x = 1_A$.
39.3 Si x et y sont deux éléments inversibles de $(A,+,\star)$, alors $x\star y$ est inversible et

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

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

40. Éléments nilpotents
Soit $(A,+,\star)$, un anneau.
40.1 ✍ *Un élément x de A est dit **nilpotent** lorsqu'il existe $n\in\mathbb{N}$ tel que $x^n = 0_A$.*
40.2 Un élément nilpotent n'est pas inversible.
40.3 ✍ *L'**indice de nilpotence** de x est le plus petit élément de*

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

40.4 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 $x^{n-1}\neq 0_A$.
40.5 Si $x^n = 0_A$, alors $(1_A - x)$ est inversible et

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

41. Diviseurs de zéro
41.1 ✍ *Soit $(A,+,\star)$, 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 $x\star y = 0_A$ (resp. $y\star x = 0_A$).*
41.2 Un diviseur de zéro n'est pas inversible.
41.3 Tout élément nilpotent non nul est un diviseur de zéro.
41.4 ✍ *Un **anneau intègre** est un anneau commutatif sans diviseur de zéro.*

II.2 Structure de corps

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

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

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

45. Exemples et contre-exemples
45.1 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.
45.2 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.
45.3 Les anneaux $\mathfrak{M}_n(\mathbb{R})$ et $\mathrm{L}(E)$ ne sont en général pas des corps.

46. Sous-corps
Soit $(\mathbb{L}, +, \star)$, un corps.
46.1 ✍ *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 $\mathbb{K}$.*
46.2 ➔ *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 :

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

46.3 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.
46.4 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

47.1 ➔ *Soit $\mathbb{K}$, un corps (commutatif). Il existe un espace vectoriel sur $\mathbb{K}$, noté $\mathbb{K}[X]$, qui admet une base dénombrable, notée $(X^n)_{n\in\mathbb{N}}$.*
47.2 ✍ *Les vecteurs de $\mathbb{K}[X]$ sont les* ***polynômes*** *à coefficients dans $\mathbb{K}$ en l'indéterminée X.*
47.3 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

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

47.4 ✍ *Quels que soient les polynômes*

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

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

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

47.5 ➔ *Muni de l'addition naturelle* **[47.1]** *et de la multiplication interne* **[47.4]**, *l'ensemble $\mathbb{K}[X]$ est un anneau commutatif tel que*

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

48. 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**.

49. Si $P = a_0 + a_1 X + a_2 X^2 + \cdots$ 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 $\mathbb{N}$.
49.1 ✍ *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 $-\infty$.

49.2 ✍ *La* ***valuation**** *d'un polynôme $P \neq 0$ est l'entier $\min \sigma(P)$.*
La valuation du polynôme nul est, par convention, égale à $+\infty$.
49.3 ➔ **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*

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

49.4 ➔ **Degré d'un produit**

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

50. ➔ **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

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

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

51. Soit $P \in \mathbb{K}[X]$.
51.1 ✍ *Un scalaire $\alpha \in \mathbb{K}$ est une* ***racine*** *de P lorsque le polynôme $(X - \alpha)$ divise P.*
51.2 ✍ *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.*
51.3 Le scalaire α est une racine de P si, et seulement si, sa multiplicité est supérieure à 1.
51.4 La multiplicité de α est supérieure à m si, et seulement si, $(X - \alpha)^m$ divise P.
51.5 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.
51.6 ➔ *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.*

52. Soit $\Omega \subset \mathbb{K}$.
52.1 ✍ *Une application $f : \Omega \to \mathbb{K}$ est une* ***application polynomiale*** *lorsqu'il existe existe une famille presque nulle de scalaires $(a_k)_{k\in\mathbb{N}}$ telle que*

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

52.2 Tout $x \in \Omega$ tel que $f(x) = 0$ est une racine du polynôme défini par →**[81]**

$$P = a_0 + a_1 X + a_2 X^2 + \cdots.$$

Si l'application f s'annule sur une partie infinie de $\mathbb{K}$, alors tous les scalaires a_k sont nuls.
52.3 ➔ *Soit $f : \Omega \to \mathbb{K}$, 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*

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

52.4 ➔ *Si la fonction polynomiale f définie par*

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d$$

est identiquement nulle sur une partie infinie Ω, alors les coefficients $a_0, a_1, \ldots, a_d$ sont tous nuls.
52.5 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

53. 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.

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

$$\text{(1)} \qquad \forall\,(x,y)\in A\star A,\quad \varphi(x+y)=\varphi(x)\oplus\varphi(y)$$

$$\text{(2)} \qquad \forall\,(x,y)\in A\star A,\quad \varphi(x\star y)=\varphi(x)\otimes\varphi(y)$$

$$\text{(3)} \qquad \varphi(1_A)=1_B.$$

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

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

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

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

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

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

55.4

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

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

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

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

56. Noyau d'un morphisme d'anneaux

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

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

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

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

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

57.2 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 $(A,+,\star)$.

57.3 Si $\varphi : A\to B$ 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

58. 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

$$(x_1,x_2)\oplus(y_1,y_2)=(x_1+y_1,x_2+y_2)$$
$$(x_1,x_2)\bullet(y_1,y_2)=(x_1\star y_1,\ x_2\otimes y_2).$$

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

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

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

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

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

58.5 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.

58.6 Si l'anneau produit $(A_1\times A_2,+,\bullet)$ est intègre, alors les deux anneaux $(A_1,+,\star)$ et $(A_2,+,\otimes)$ sont intègres.

Cependant, l'anneau produit $(\mathbb{Z}^2,+,\times)$ n'est pas intègre :

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

alors que l'anneau $(\mathbb{Z},+,\times)$ est intègre.

59. Morphismes

59.1 ✍ *Les* ***projections canoniques*** *sont les applications définies par*

$$\pi_1 : \begin{array}{ccc} A_1\times A_2 & \to & A_1\\ (x_1,x_2) & \mapsto & x_1\end{array} \quad \textit{et} \quad \pi_2 : \begin{array}{ccc} A_1\times A_2 & \to & A_2\\ (x_1,x_2) & \mapsto & x_2\end{array}.$$

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

59.3 ➔ *Une application*

$$\theta : \begin{array}{ccc} L & \to & A_1\times A_2\\ x & \mapsto & \big(\varphi(x),\psi(x)\big)\end{array}$$

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

59.4 Les injections définies par

$$i_1 : \begin{array}{ccc} A_1 & \to & A_1\times A_2\\ x_1 & \mapsto & (x_1,0_{A_2})\end{array} \quad \text{et} \quad i_2 : \begin{array}{ccc} A_2 & \to & A_1\times A_2\\ x_2 & \mapsto & (0_{A_2},x_2)\end{array}$$

ne sont pas des morphismes d'anneaux.

II.6 Idéaux d'un anneau commutatif

60. ✍ *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 $\star$:*

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

61. ➔ *Le noyau d'un morphisme d'anneaux $\varphi : A\to B$ est un idéal de A.*

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

62.2 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 $\mathbb{L}$.

63. Idéal engendré par un élément

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

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

est un idéal de A.

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

63.3 Soit I, un idéal de A. Alors :

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

et en particulier

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

64. Opération sur les idéaux

64.1 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 $I\cap J$.

64.2 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 $I+J$.

64.3 ▷ *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

65. Anneaux intègres [41.4]
65.1 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.
65.2 ➔ **Simplification dans un anneau intègre**
Soit A, un anneau intègre et $z \neq 0_A$. Si $x \star z = y \star z$, alors $x = y$.

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

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

On note alors $x \mid y$.
66.2 ➔

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

67. Éléments inversibles
67.1 Un élément x de A est inversible si, et seulement si, il divise 1_A.
67.2 ➔ *Un élément x de A est inversible si, et seulement si, l'idéal xA est égal à A.*

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

67.3 S'il existe $n \in \mathbb{N}^*$ tel que x^n soit inversible, alors x est inversible.
67.4 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.

68. Éléments associés
68.1 ✍ *Deux éléments x et y d'un anneau intègre A sont **associés** lorsqu'ils engendrent le même idéal : $xA = yA$.*
68.2 ➔ *Deux éléments x et y de A sont associés si, et seulement si, il existe un élément inversible $u \in A^\times$ tel que $y = u \star x$.*
68.3 ▷ *Les éléments inversibles de A sont les éléments associés à 1_A.*

69. Éléments irréductibles
Soit A, un anneau intègre.
69.1 ✍ *Un élément non nul de A qui peut s'écrire comme le produit de deux éléments non inversibles de A est dit **composé**.*
69.2 Un entier $x \in \mathbb{N}$ est composé si, et seulement si, il existe deux entiers $y \geqslant 2$ et $z \geqslant 2$ tels que $x = yz$.
69.3 Un polynôme $P \in \mathbb{K}[X]$ est composé si, et seulement si, il existe deux polynômes Q_1 et Q_2 tels que $P = Q_1Q_2$ avec $\deg Q_1 \geqslant 1$ et $\deg Q_2 \geqslant 1$.
69.4 Si x est le produit de deux éléments y et z non inversibles, alors

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

69.5 ✍ *Un élément non nul de A est **irréductible** lorsqu'il n'est ni inversible, ni composé.*
69.6 Si un élément irréductible x est factorisé sous la forme $x = yz$ avec z non inversible, alors y est inversible. Autrement dit :

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

Idéaux des anneaux euclidiens

70. 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. →**[63]**

71. ➔ Idéaux de $\mathbb{Z}$ [22.4]
Pour tout idéal I de $\mathbb{Z}$, il existe un, et un seul, entier $n \in \mathbb{N}$ tel que

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

72. Idéaux de $\mathbb{K}[X]$
Soit I, un idéal de $\mathbb{K}[X]$, non réduit à $\{0\}$.
72.1 Si P et Q sont deux polynômes appartenant à I, alors le reste de la division euclidienne de P par Q appartient à I.
72.2 L'idéal I est engendré par tout polynôme $P_0 \in I$ tel que

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

72.3 ➔ *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.*

73. Éléments normalisés
La notion d'**élément normalisé** a pour seul but de donner une représentation unique des idéaux de l'anneau A. →**[73.4]**
73.1 ✍ *Un élément x de $\mathbb{Z}$ est **normalisé** lorsqu'il appartient à $\mathbb{N}^*$* (entier positif).
73.2 ✍ *Un élément P de $\mathbb{K}[X]$ est **normalisé** lorsque son coefficient dominant est égal à 1* (polynôme unitaire).
73.3 Pour tout $x \in A$ *non nul*, il existe un, et un seul, élément normalisé $x_0 \in A$ associé à x.
73.4 ➔ *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

74. 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 $\mathrm{L}(E)$ sont-ils des corps ?
8. *Suite de* **[55]** –
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. On suppose que les seuls idéaux de l'anneau commutatif A sont $\{0\}$ et A.
9.a Si $x \neq 0$, alors l'élément unité 1_A appartient à l'idéal xA engendré par x.
9.b L'anneau A est en fait un corps.
10. *Suite de* **[66.1]** – Si un élément x non nul divise y, alors il existe un, et un seul, élément $q \in A$ tel que $y = q \star x$.
11. Pourquoi la notion de divisibilité est-elle sans intérêt dans un corps ?

III

Algèbres et polynômes

III.1 Structure d'algèbre

75. Algèbres associatives unitaires
Soit $\mathbb{K}$, un corps.
75.1 ✍ *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 $(+, *)$ telles que*

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

75.2 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

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

75.3 ✍ *La **dimension** d'une algèbre $(A,+,*,\cdot)$ est la dimension (finie ou non) de l'espace vectoriel $(A,+,\cdot)$.*
75.4 ✍ *L'**élément unité** d'une algèbre est l'élément neutre pour la multiplication interne.*
75.5 ✍ *Les **éléments inversibles** d'une algèbre sont ceux qui ont un symétrique* dans cette algèbre *pour la multiplication interne.*
75.6 L'ensemble des éléments inversibles d'une algèbre est muni d'une structure de groupe pour $*$.

76. Sous-algèbres
76.1 ✍ *Une **sous-algèbre** de $(A,+,*,\cdot)$ est une partie de A munie d'une structure d'algèbre associative unitaire pour les lois $+$, $*$ et $\cdot$.*
76.2 Les sous-algèbres d'une algèbre sur le corps $\mathbb{K}$ sont aussi des algèbres sur le corps $\mathbb{K}$.

77. Méthodes
77.1 $(A,+,*,\cdot)$ 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.
77.2 ➔ *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 $*$.*

78. Morphismes d'algèbres
78.1 ✍ *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.*

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

78.2 En particulier, un morphisme d'algèbres possède toutes les propriétés d'un morphisme d'anneaux. →**[55]**
78.3 ▷ *Si $f:A\to B$ est un morphisme d'algèbres bijectif, alors sa bijection réciproque est un morphisme d'algèbres.*
78.4 ▷ *L'image d'un morphisme d'algèbres $f:A\to B$ est une sous-algèbre de B.*

Exemples d'algèbres et de sous-algèbres

79.1 Le corps $\mathbb{K}$ est une algèbre sur $\mathbb{K}$ où la multiplication interne et la multiplication externe coïncident.
79.2 L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est une algèbre sur $\mathbb{K}$.
79.3 L'ensemble $\mathbb{K}[X^2]$ des polynômes pairs est une sous-algèbre de $\mathbb{K}[X]$.
79.4 L'ensemble $\mathfrak{M}_n(\mathbb{K})$ des matrices carrées est une algèbre.
79.5 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 $\mathfrak{M}_n(\mathbb{K})$.
79.6 L'ensemble $\mathrm{L}(E)$ des endomorphismes de E est une algèbre, qui a $\circ$ pour multiplication interne.
79.7 L'ensemble $\mathscr{A}(\Omega,A)$ des applications d'un ensemble Ω dans une algèbre $(A,+,*,\cdot)$ est une algèbre dont la multiplication interne $\otimes$ est définie par

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

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

80. Commutant
Soit $(A,+,*,\cdot)$, une algèbre.
80.1 ✍ *Le **commutant*** d'un élément $a\in A$ est la partie de A définie par*

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

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

III.2 Action des polynômes sur une algèbre

81. Les règles de calcul de la structure d'**algèbre** ont pour but de former des expressions polynomiales.
81.1 ✍ *Pour tout polynôme*

$$P=\alpha_0+\alpha_1X+\cdots+\alpha_dX^d\in\mathbb{K}[X]$$

*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*

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

81.2 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.
81.3 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
$$P_1(a)=Q(a)*P_0(a)+R(a).$$

81.4 ➔ **Morphisme d'évaluation**
Pour tout $a\in A$, l'application $\mathcal{E}_a:\mathbb{K}[X]\to A$ définie par

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

est un morphisme d'algèbres.
81.5 Si $f:A\to B$ est un morphisme d'algèbres, alors

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

81.6 ➔ *Soit $a\in A$. Si $b\in A$ est inversible, alors*

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

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

82. Sous-algèbre engendrée par un élément
82.1 ✍ *La **sous-algèbre des polynômes en** $a\in A$ est l'image du morphisme $\mathcal{E}_a$. Elle est notée $\mathbb{K}[a]$.*

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

82.2 **Minimalité de $\mathbb{K}[a]$**
Si une sous-algèbre B de A contient l'élément a, alors $\mathbb{K}[a]\subset B$.
82.3 ➔ *La sous-algèbre $\mathbb{K}[a]$ est commutative et*

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

83. Idéal annulateur
83.1 ✍ *Les **polynômes annulateurs de** $a\in A$ sont les polynômes P tels que $P(a)=0_A$.*
83.2 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.
83.3 ➔ *À tout polynôme annulateur* non nul *de a :*

$$\alpha_0+\alpha_1X+\cdots+\alpha_dX^d$$

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

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

83.4 ✍ *L'ensemble des polynômes annulateurs de $a \in A$ est le noyau du morphisme d'algèbres*

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

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

83.5 ✍ *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.* →**[72.3]**

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

83.7 ➔ *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.*

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

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

Entraînement

84. Questions pour réfléchir

1. Le noyau d'un morphisme d'algèbres $f : A \to B$ 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 $\mathrm{GL}_n(\mathbb{K})$ des matrices inversibles est-il une sous-algèbre de $\mathfrak{M}_n(\mathbb{K})$?
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 $\mathscr{A}(\Omega, E)$ soit une algèbre commutative ?
5. *Suite de* **[80]** – Comparer la sous-algèbre $\mathbb{K}[a]$ et le commutant de a pour $A = \mathfrak{M}_n(\mathbb{K})$ 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 $f \in \mathrm{L}(E)$ et $\dim E \geqslant 2$, l'application $[P \mapsto P(f)]$ n'est pas surjective.

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

86. Morphisme d'évaluation [81]

86.1 Sous-algèbre des applications polynomiales

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

1. La sous-algèbre $\mathscr{A}_0(\Omega, \mathbb{K})$ 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 $\mathbb{K}$.

86.2 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 $(x_1, \ldots, x_N) \in \mathbb{C}^N$ est liée si, et seulement si, il existe une famille $(m_1, \ldots, m_N)$ 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 $(\ell\mathrm{n}\, p)_{p\in\mathfrak{P}}$ 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 $\mathrm{Ker}\, \mathcal{E}_a \subset \mathbb{Q}[X]$.

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

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

pour base, où $d = \deg P_0$.

87.

1. L'application $[u \mapsto \mathfrak{Mat}_{\mathscr{B}}(u)]$ est un isomorphisme d'algèbres de $\mathrm{L}(E)$ sur $\mathfrak{M}_n(\mathbb{K})$, pour toute base $\mathscr{B}$ de E.
2. L'application $[M \mapsto Q^{-1}MQ]$ est un automorphisme d'algèbre de $\mathfrak{M}_n(\mathbb{K})$ pour toute matrice $Q \in \mathrm{GL}_n(\mathbb{K})$.

2.a L'application $[M \mapsto {}^tM]$ est-elle un isomorphisme d'algèbre de $\mathfrak{M}_n(\mathbb{K})$ sur $\mathfrak{M}_n(\mathbb{K})$?

88. 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 $v^{-1} \in \mathbb{K}[u]$.

Questions, exercices & problèmes

Perfectionnement

89. 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 $\mathbb{K}[X^n]$?

90. 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 **[93]**.
4. Comment calculer le polynôme minimal **[83.5]** d'une matrice $A \in \mathfrak{M}_3(\mathbb{K})$?

91. Questions pour réfléchir

1. Quels algorithmes reposent-ils sur les factorisations du groupe symétrique **[20.4]** ? du groupe linéaire **[20.5]** ?
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 $x \star y = y \star x$, 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* **[49.2]** –

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* **[52.4]** – Si $\Omega \subset \mathbb{K}$ est une partie finie, condition pour que les coefficients $a_0, a_1, \ldots, a_d$ 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* **[88]** – Étudier le cas où la dimension de $\mathbb{K}[u]$ est infinie.

Approfondissement

92. 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 $\mathbb{C}$.

93. Groupe diédral d'ordre 8
Le **groupe diédral** est le sous-groupe G de $\mathrm{GL}_2(\mathbb{R})$ 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 $\mathrm{SO}_2(\mathbb{R})$ qui est l'ensemble des automorphismes de $\mathbb{R}^2$ qui laissent ce polygone globalement invariant.

94. Exemples de parties génératrices
94.1 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.
94.2 Algorithme du pivot
1. Le sous-groupe $\mathrm{SL}_n(\mathbb{R})$ des matrices dont le déterminant est égal à 1 est engendré par les matrices de transvection.
2. L'ensemble $\mathrm{SL}_2(\mathbb{Z})$ 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

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

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

Pour aller plus loin

95. Démonstration du théorème de Lagrange [26.2]
On pose H, un sous-groupe de G et, pour tout $x \in G$,

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

1. Quel que soit $x \in G$, l'ensemble xH est l'image de H par la translation $[y \mapsto x \star y]$, donc le cardinal de xH est égal au cardinal de H et
$$xH = H \iff x \in H.$$
2. La relation $\mathscr{R}$ définie par
$$x \mathscr{R} y \iff xH = yH$$
est une relation d'équivalence sur G.
3. Si $x_1H \cap x_2H \neq \varnothing$, alors $x_1H = x_2H$.
4. Il existe $x_1, \ldots, x_q$ dans G tels que
$$G = \bigsqcup_{1\leqslant k\leqslant q} x_kH$$
donc le cardinal de H divise l'ordre de G.

96. Applications polynomiales
Nous parlerons ici de *polynômes* alors qu'il s'agit en fait de *fonctions polynomiales*.
96.1 ✍ *Un* ***monôme en*** d ***variables*** *est une application de* $\mathbb{K}^d$ *dans* $\mathbb{K}$ *de la forme*

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

où $(k_1, \ldots, k_d) \in \mathbb{N}^d$.
96.2 ✍ *L'espace des* ***polynômes en*** d ***variables****, noté* $\mathbb{K}[x_1, \ldots, x_d]$*, est le sous-espace de* $\mathscr{A}(\mathbb{K}^d, \mathbb{K})$ *engendré par les monômes.*
96.3 ➔ *L'ensemble* $\mathbb{K}[x_1, \ldots, x_d]$ *des polynômes en d variables est une algèbre associative unitaire.*
96.4 Notation courte
Pour tout vecteur $x = (x_1, \ldots, x_d) \in \mathbb{K}^d$ et tout **multi-indice**

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

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 $x_1, \ldots, x_d$ est nulle.
96.5 ➔ *Étant donnés deux multi-indices* k *et* ℓ *dans* $\mathbb{N}^d$,

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

96.6 Base canonique de $\mathbb{K}[x_1, \ldots, x_d]$
1. Si la fonction polynomiale
$$\left[x \mapsto \sum_{k\in\mathbb{N}} a_k x^k\right]$$
de $\mathbb{K}$ dans $\mathbb{K}$ est identiquement nulle sur $\mathbb{K}$, alors tous les coefficients a_k sont nuls.
2. Si $d \geqslant 2$, un polynôme de $\mathbb{K}[x_1, \ldots, x_d]$ peut être considéré comme une fonction polynomiale en une variable x_d à coefficients dans $\mathbb{K}[x_1, \ldots, x_{d-1}]$.
3. Pour tout $d \geqslant 1$ et tout polynôme $P \in \mathbb{K}[x_1, \ldots, x_d]$, il existe une, et une seule, famille presque nulle $(a_k)_{k\in\mathbb{N}^d}$ telle que
$$\forall\, x \in \mathbb{K}^d, \quad P(x) = \sum_{k\in\mathbb{N}^d} a_k x^k.$$
4. On suppose que l'application polynomiale définie par
$$\forall\, x \in \mathbb{K}^d, \quad P(x) = \sum_{k\in\mathbb{N}^d} a_k x^k$$
est identiquement nulle sur une partie Ω de $\mathbb{K}^d$.
4.a Si $\Omega = \mathbb{K}^d$, alors tous les coefficients a_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 ?

96.7 ✍ **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*

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

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

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

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

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

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

96.10 ✍ *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 ?