I

Ordre des éléments d'un groupe

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

Action d'un groupe sur lui-même

2. ✍ *Soient* $(G,\star)$, *un groupe et* E, *un ensemble. Une* **action*** *(ou une* **opération***) de* G *sur* E *est une loi de composition externe*

$$\begin{array}{ccc} G\times E & \longrightarrow & E \\ (x,u) & \longmapsto & x\cdot u \end{array}$$

telle que

$$\forall\, u\in E,\qquad e\cdot u = u$$

et que

$$\forall\, x,x'\in G,\ \forall\, u\in E,\quad x'\cdot(x\cdot u) = (x'\star x)\cdot u.$$

3. Translation à gauche
Pour tout $a\in G$, l'application

$$\gamma_a = [x\mapsto a\star x]$$

est une bijection de G sur G.
3.1 L'application $\gamma = [a\mapsto\gamma_a]$ est un morphisme de groupes injectif de $(G,\star)$ dans $(\mathfrak{S}(G),\circ)$.
3.2 ✍ *Étant donné un sous-groupe* H *de* $(G,\star)$, *les* **classes à gauche selon un sous-groupe*** H *sont les ensembles*

$$xH = \{x\star h,\ h\in H\}$$

lorsque x *parcourt* G.
L'ensemble des classes à gauche selon H *est l'***ensemble quotient*** *de* G *par* H, *noté* ${}^{G}/_{H}$.
3.3 Les classes à gauche xH et yH sont égales si, et seulement si, $y^{-1}\star x\in H$.
3.4 La relation binaire définie par

$$\forall\, x,y\in G,\quad x\sim_H y \iff xH = yH$$

est une relation d'équivalence, dont les classes d'équivalence sont les classes à gauche selon H.
3.5 * *Les classes à gauche selon* H *sont toutes équipotentes à* H *et si* G *est fini, alors*

$$\#({}^{G}/_{H}) = \frac{\#(G)}{\#(H)}.$$

4. Conjugaison
Pour tout $a\in G$, l'application

$$\sigma_a = \left[x\mapsto a\star x\star a^{-1}\right]$$

est un automorphisme du groupe $(G,\star)$.
4.1 L'application $\sigma = [a\mapsto\sigma_a]$ est un morphisme de groupes de $(G,\star)$ dans $(\mathfrak{S}(G),\circ)$.
4.2 ✍ *L'***orbite***, *ou* **classe de conjugaison***, de* $x\in G$ *est l'ensemble*

$$\Omega_x = \{a\star x\star a^{-1},\ a\in G\}.$$

4.3 La relation binaire définie par

$$\forall\, x,y\in G,\quad x\equiv y \iff \Omega_x = \Omega_y$$

est une relation d'équivalence, dont les classes d'équivalence sont les orbites.

4.4 Si G est fini, alors il existe des éléments $x_1,\ldots,x_N$ de G tels que la famille des orbites

$$\left(\Omega_{x_k}\right)_{1\leqslant k\leqslant N}$$

soit une partition de G. En particulier,

$$\#(G) = \sum_{k=1}^{N}\#(\Omega_{x_k}).$$

4.5 ✍ *Le* **stabilisateur*** *de* $x\in G$ *est l'ensemble* G_x *des éléments qui commutent à* x *:*

$$\forall\, a\in G,\quad a\in G_x \iff a\star x\star a^{-1} = x.$$

4.6 * *Le stabilisateur de* $x\in G$ *est un sous-groupe de* $(G,\star)$.
4.7 Pour tout $b\in\Omega_a$, il existe $x\in G$ tel que $b = x\star a\star x^{-1}$ et l'application

$$u\mapsto x\star u\star x^{-1}$$

est un isomorphisme de G_a sur G_b.
4.8 Équation aux classes
Soit $a\in G$.

1. La relation binaire définie sur G par

$$\forall\, x,y\in G,\quad x\sim_a y \iff x\star a\star x^{-1} = y\star a\star y^{-1}$$

est une relation d'équivalence, dont les classes d'équivalence sont les classes à gauche selon le stabilisateur G_a :

$$\forall\, x,y\in G,\quad x\sim_a y \iff y\in xG_a.$$

2. Si G est fini, alors l'orbite de a est une partie finie :

$$\Omega_a = \left\{\sigma_{u_1}(a),\ldots,\sigma_{u_r}(a)\right\}$$

et la famille des classes à gauche $(u_kG_a)_{1\leqslant k\leqslant r}$ est une partitition de G. En particulier,

$$\forall\, a\in G,\qquad \#(G) = \#(\Omega_a)\times\#(G_a).$$

5. Translation à droite
5.1 Pour tout $a\in G$, l'application $\delta_a = [x\mapsto x\star a]$ est une bijection de G sur G et l'application $\delta = [a\mapsto\delta_a]$ vérifie

$$\forall\, a,b\in G,\quad \delta_{a\star b} = \delta_b\circ\delta_a.$$

5.2 ✍ *Les* **classes à droite selon un sous-groupe*** H *sont les ensembles*

$$Hx = \{h\star x,\ h\in H\}$$

lorsque x *parcourt* H.
5.3 Pour tout $x\in G$, les classes à gauche xH et à droite Hx sont équipotentes.

I.1 Sous-groupe engendré par une partie

6. ⇀ 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 $(G,*)$.

7. Parties génératrices d'un groupe
On considère un groupe $(G,\star)$ et une partie S de G.
7.1 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.
7.2 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.
7.3 ✍ *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 $S \subset H$.*

Exemples

8. 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 $\star = +$,

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

9.1 Le groupe $(\mathbb{Z},+)$ est engendré par 1.
9.2 Le groupe $(\mathbb{U}_n,\times)$ des racines n-ièmes de l'unité est engendré par $\exp(2i\pi/n)$.
9.3 Le groupe $(\mathrm{GL}_n(\mathbb{R}),\times)$ est engendré par les matrices de transvection et les matrices de dilatation.
9.4 Le groupe $\mathrm{SL}_2(\mathbb{Z})$ est engendré par les matrices

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

Il est aussi engendré par T_+ et

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

9.5 Aucune partie finie de $\mathbb{Q}$ n'engendre le groupe $(\mathbb{Q},+)$.
10. Groupe symétrique
Si $\sigma \in \mathfrak{S}_n$ est un cycle de longueur $2 \leqslant r \leqslant n$, alors il existe $x_0 \in [\![1,n]\!]$ tel que

$$\sigma = (x_0, x_1, \dots, x_{r-1}) = \big(x_0, \sigma(x_0), \dots, \sigma^{r-1}(x_0)\big)$$

avec $\sigma(x_{r-1}) = x_0$.
10.1 Étant donnés une permutation quelconque τ et un cycle de longueur r

$$\sigma = (x_0, x_1, \dots, x_{r-1})$$

la permutation conjuguée $\tau \circ \sigma \circ \tau^{-1}$ est encore un cycle de longueur r :

$$\tau \circ \sigma \circ \tau^{-1} = \big(\tau(x_0), \tau(x_1), \dots, \tau(x_{r-1})\big).$$

10.2 Toute permutation de $\mathfrak{S}_n$ se décompose en produit de cycles de supports deux à deux disjoints.
10.3 Le groupe symétrique $(\mathfrak{S}_n,\circ)$ est engendré par les transpositions $\tau_{i,j}$, $1 \leqslant i < j \leqslant n$.
10.4 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 $(1,2,3,\dots,n)$.
10.5 Le sous-groupe alterné $\mathfrak{A}_n$ est engendré par l'ensemble des cycles de longueur 3 :

$$(a,b,c) = \tau_{a,b} \circ \tau_{b,c}$$
$$\tau_{a,b} \circ \tau_{c,d} = \tau_{a,b} \circ \tau_{b,c} \circ \tau_{b,c} \circ \tau_{c,d} = (a,b,c) \circ (b,c,d)$$

mais aussi par la famille des cycles $(1,2,k)$ pour $3 \leqslant k \leqslant n$.

I.2 Groupes monogènes

11. ➙ *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,

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

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

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

12.2 Un groupe monogène est commutatif.
12.3 Le groupe $(\mathbb{Z},+)$ est monogène.
12.4 Pour tout entier $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z}$ est un sous-groupe monogène de $(\mathbb{Z},+)$.
12.5 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.
12.6 ➙ **Sous-groupes additifs de $\mathbb{Z}$**
Tout sous-groupe H de $(\mathbb{Z},+)$ est monogène et il existe un, et un seul, entier $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

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

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

Morphismes

15. ➙ *Soient $(G,\star)$, un groupe monogène ; $g \in G$, un générateur de G et $(H,\otimes)$, un groupe.*
Pour tout $h \in H$, il existe au plus un morphisme de groupes f de $(G,\star)$ dans $(H,\otimes)$ tel que $f(g) = h$.

16. 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.
16.1 L'application φ_a est un morphisme de groupes de $(\mathbb{Z},+)$ dans $(G,\star)$.
16.2 L'image de φ_a est le sous-groupe $\langle a\rangle$.
16.3 Si φ_a est injectif, alors l'ordre du groupe $\langle a\rangle$ est infini.
16.4 Si φ_a n'est pas injectif, alors il existe un, et un seul, entier $n \geqslant 1$ tel que le noyau de φ_a soit égal à $n\mathbb{Z}$. Le sous-groupe $\langle a\rangle$ est alors un groupe cyclique d'ordre n :

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

et $a^n = e_G$.

17. Soit $\langle a\rangle$, un groupe cyclique d'ordre $n \in \mathbb{N}^*$.
17.1 Pour tout morphisme de groupes $f : \langle a\rangle \to H$, l'ordre de $f(a)$ est un diviseur de n.
17.2 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 l'unique morphisme de groupes de $\langle a\rangle$ dans H tel que $f(a) = y_0$. →**[52]**

L'image de ce morphisme est le sous-groupe $\langle y_0\rangle$.
Si l'ordre de y_0 est égal à n, alors ce morphisme est injectif.

18. ➙ *Soient $\langle a\rangle$, un groupe cyclique d'ordre $n \in \mathbb{N}^*$ et y_0, un élément du groupe $(H,\otimes)$.*
18.1 *Il existe un morphisme de groupes $f : \langle a\rangle \to H$ tel que $f(a) = y_0$ si, et seulement si, le sous-groupe $\langle y_0\rangle$ est un groupe cyclique dont l'ordre divise n.*
18.2 *Ce morphisme induit un isomorphisme de $\langle a\rangle$ sur $\langle y_0\rangle$ si, et seulement si, l'ordre de $\langle y_0\rangle$ est égal à n.*

19. ➙ **Classification des groupes monogènes**
Un groupe monogène infini est isomorphe à $(\mathbb{Z},+)$.
Un groupe cyclique d'ordre $n \in \mathbb{N}$ est isomorphe à $(\mathbb{U}_n,\times)$. →**[52.7]**

20. 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.

I.3 Ordre d'un élément

21.1 ✍ *L'***ordre d'un élément** *$a \in G$ est l'ordre du sous-groupe $\langle a \rangle$.*
21.2 ➙ *Si $a \in G$ est un élément d'ordre d, alors*

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

Si G est un groupe additif,

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

21.3 ➙ *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,

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

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

23. Si $(G, \star)$ est un groupe cyclique d'ordre n, alors l'ordre de chaque élément de G est un diviseur de n. →**[24.2]**

24. Théorème de Lagrange
24.1 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 $a^n = e_G$.
24.2 ➙ *Si $(G, \star)$ est un groupe fini, alors l'ordre de tout élément a de G divise l'ordre de G.*
24.3 Le théorème **[24.2]** est vrai également pour les groupes non commutatifs. →**[115]**

Entraînement

25. Questions pour réfléchir
1. Le groupe $(\mathbb{U}, \times)$ est-il monogène ?
2. Pour $n \geqslant 3$, le groupe symétrique $(\mathfrak{S}_n, \circ)$ n'est pas cyclique.
3. L'ensemble des nombres décimaux est un sous-groupe de $(\mathbb{Q}, +)$ qui n'est pas monogène.
4. 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 $n \in \mathbb{Z}$.

26. On considère un ensemble E (non vide) et un sous-groupe G du groupe $(\mathfrak{S}(E), \circ)$ des applications bijectives de E dans E. La relation binaire $\sim$ définie par

$$\forall\, x, y \in E, \quad x \sim y \iff \exists\, g \in G, \quad y = g(x)$$

est une relation d'équivalence.

27. Soient H et K, deux sous-groupes de $(G, \star)$.
1. Si les deux ensembles

$$HK = \{u \star v,\, (u, v) \in H \times K\}$$

et

$$KH = \{v \star u,\, (u, v) \in H \times K\}$$

sont égaux, alors HK est le sous-groupe de $(G, \star)$ engendré par $H \cup K$.
2. Si HK est un sous-groupe de $(G, \star)$, alors $HK = KH$.

28. Groupe d'ordre premier
Soit p, un nombre premier.
Tout groupe $(G, \star)$ d'ordre p est cyclique (en particulier commutatif) et chaque élément distinct du neutre engendre G.

29. Sous-groupes d'un groupe monogène [16]
On considère un groupe monogène $(G, \star)$ engendré par a.
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 $(\mathbb{Z}, +)$.
2. Un sous-groupe d'un groupe monogène est monogène.

30.
1. L'ensemble des morphismes de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Q}, +)$ est isomorphe au groupe $(\mathbb{Q}, +)$.
2. Il existe un, et un seul, morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

31. Groupe de Klein
L'ensemble $G = \{\pm 1\} \times \{\pm 1\}$ muni de la loi de composition définie par

$$(g_1, g_2) \star (h_1, h_2) = (g_1 g_2,\, h_1 h_2)$$

est un groupe commutatif d'ordre 4. Ce groupe est engendré par les éléments $(1, -1)$ et $(-1, 1)$, mais il n'est pas cyclique. Il est isomorphe au sous-groupe de $\mathfrak{S}_4$ constitué de I et des permutations

$$\tau_{1,2} \circ \tau_{3,4}, \quad \tau_{1,3} \circ \tau_{2,4}, \quad \tau_{1,4} \circ \tau_{2,3}.$$

32. Soit $(G, \star)$, un groupe.
1. Un élément a de G est d'ordre 2 si, et seulement si,

$$a = a^{-1}.$$

2. L'ordre de G est pair si, et seulement si, G admet au moins un élément d'ordre 2.

33. Soit $(G, *)$, un groupe fini d'élément neutre e. On suppose que

$$\forall\, x \in G, \qquad x^2 = e.$$

1. Le groupe $(G, *)$ est abélien.
2. Soient H, un sous-groupe strict de G et $a \in G \setminus H$. On pose

$$aH = \{a * x,\, x \in H\}.$$

Les ensembles H et aH ont même cardinal, sont disjoints et l'ensemble $H \cup aH$ est un sous-groupe de G.
3. Le cardinal de G est une puissance de 2.

34. Soit σ, un cycle de longueur ℓ dans $\mathfrak{S}_n$.

$$\sigma = (a_1, \ldots, a_\ell)$$

1. L'ordre de σ est égal à ℓ.
2. On suppose que $\sigma^k(a_1) = a_1$. Que dire de σ^k ?
3. Pour $k \in \mathbb{N}$, la permutation σ^k est-elle un cycle ? Que dire de l'ordre de σ^k ?

35. Soit n, un entier supérieur à 2.
1. Pour toute transposition $\tau \in \mathfrak{S}_n$, il existe une permutation σ telle que $\sigma \circ \tau \circ \sigma$ soit la transposition $\tau_{1,2} = (1, 2)$.
2. Il existe exactement deux morphismes de groupes de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

36. 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.

37. On suppose qu'un groupe fini G contient un élément x d'ordre 3 et un élément y d'ordre 5.
1. L'ordre de G est divisible par 15.
2. Si $x \star y = y \star x$, alors G contient un élément d'ordre 15.

38. Soit H, un sous-groupe strict d'un groupe fini $(G,\star)$. Pour tout $g \in G$, on pose

$$gHg^{-1} = \{g \star h \star g^{-1},\, h \in H\}.$$

1. Pour tout $g \in G$, l'ensemble gHg^{-1} est un sous-groupe de $(G,\star)$ isomorphe à H.
2. Quels que soient g_1 et g_2 dans G, l'intersection

$$g_1Hg_1^{-1} \cap g_2Hg_2^{-1}$$

contient au moins l'élément neutre e et si $g_2 \in g_1H$, alors $g_1Hg_1^{-1} = g_2Hg_2^{-1}$.
3. Comme

$$\bigcup_{g\in G} gHg^{-1} \subsetneq G,$$

il existe $x \in G$ tel que $H \cap \{g \star x \star g^{-1},\, g \in G\} = \varnothing$.

39. Groupes abéliens d'ordre pq
Soit $(G,\star)$, un groupe commutatif d'ordre pq où p et q sont deux nombres premiers distincts.
1. L'ordre d'un élément x de G est égal à 1, à p, à q ou à pq.
2. S'il existe un élément a d'ordre p et un élément b d'ordre q, alors l'ordre de $a \star b$ est nécessairement égal à pq.
3. On suppose qu'il existe un élément a d'ordre p et qu'il existe un élément $b \in G \setminus \langle a\rangle$ d'ordre p.
Alors $\langle a\rangle \cap \langle b\rangle = \{e\}$ et

$$\langle a,b\rangle = \{a^i \star b^j,\, 0 \leqslant i,j < p\}$$

est un sous-groupe d'ordre p^2.
4. Le groupe $(G,\star)$ est cyclique.

40. Sous-groupes additifs de $\mathbb{R}$
Contrairement à $(\mathbb{Z},+)$, le groupe $(\mathbb{R},+)$ contient des sous-groupes qui ne sont pas monogènes.
40.1 Soit G, un sous-groupe monogène de $(\mathbb{R},+)$, qui n'est pas réduit au singleton $\{0\}$. Il existe un plus petit élément $g > 0$ dans G et $G = \langle g\rangle = g\mathbb{Z}$.
40.2 Soient a et b, deux réels strictement positifs. Si le sous-groupe

$$\langle a,b\rangle = \langle a\rangle + \langle b\rangle$$

est monogène, alors le quotient a/b est rationnel.
40.3 Un sous-groupe G de $(\mathbb{R},+)$ qui n'est pas monogène est dense dans $\mathbb{R}$.

41. Soient H_1 et H_2, deux sous-groupes de $(G,+)$.
41.1 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.
41.2 En revanche, l'union $H_1 \cup H_2$ est un sous-groupe de G si, et seulement si,

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

42. Soit $(G,\star)$, un groupe qui n'admet qu'un nombre fini de sous-groupes.
Comme tout élément de G est d'ordre fini et que

$$G = \bigcup_{x\in G} \langle x\rangle,$$

alors G est un ensemble fini.

43. Soient $(G,\star)$, un groupe d'ordre n et $a \in G$.
1. Si l'ordre de a est égal à p, alors la translation à gauche $\gamma_a = [x \mapsto a \star x]$ est une permutation de G et les orbites de cette permutation sont toutes de cardinal p.
Il existe un entier q tel que $n = pq$ et la signature de la permutation γ_a est égale à $(-1)^{n-q}$.
2. S'il existe un entier impair $m \geqslant 3$ tel que $n = 2^\alpha m$ et s'il existe un élément $a \in G$ d'ordre 2^α, alors l'ensemble

$$\{x \in G \,:\, \varepsilon(\gamma_x) = 1\}$$

est un sous-groupe de $(G,\star)$ distinct de G et de $\{e\}$.

44. Soit $(G,\star)$, un groupe commutatif fini. Pour tout $a \in G$, on note $\omega(a)$, l'ordre de a.
1. Si $\omega(a)$ et $\omega(b)$ sont premiers entre eux, alors

$$\langle a\rangle \cap \langle b\rangle = \{e\} \quad \text{et} \quad \omega(a\star b) = \omega(a)\omega(b).$$

Si les entiers $\omega(a_i)$ sont deux à deux premiers entre eux pour $1 \leqslant i \leqslant m$, alors l'ordre du produit $b = a_1 \star \cdots \star a_m$ est égal au produit $\omega(a_1)\cdots\omega(a_m)$.
2. En général, l'ordre de $a \star b$ divise le ppcm de $\omega(a)$ et de $\omega(b)$. Que dire du cas $b = a^{-1}$?
3. On suppose qu'aucun nombre premier ne figure avec le même exposant dans les décompositions en facteurs premiers de $\omega(a)$ et de $\omega(b)$: on a donc

$$\omega(a) = \prod_{i=1}^{r} p_i^{\alpha_i} \quad \text{et} \quad \omega(b) = \prod_{i=1}^{r} p_i^{\beta_i}$$

avec $\alpha_i \neq \beta_i$ pour tout $1 \leqslant i \leqslant r$.
Pour tout entier $q \in \mathbb{N}$ tel que $(ab)^q = e$, on note m, le plus petit commun multiple de q et de $\omega(a)$ et n, celui de q et de $\omega(b)$. Alors $\omega(a)$ divise n et $\omega(b)$ divise m. On en déduit que q est un multiple du ppcm de $\omega(a)$ et de $\omega(b)$.

45. Dans $\mathfrak{S}_3$, toute transposition est d'ordre 2 et l'ordre du cycle $\sigma = (1,2,3)$ est égal à 3.
Cependant, l'ordre du produit $\tau_{1,2} \circ \tau_{2,3}$ est égal à 3 et l'ordre du produit $\sigma \circ \tau_{1,2}$ est égal à 2. Comparer avec **[44]**.

46. Structure du groupe $\mathfrak{S}_3$
1. On considère le cycle $\sigma = (1,2,3)$ et la transposition $\tau = (1,2)$ de $\mathfrak{S}_3$. Alors

$$\tau\circ\sigma = \sigma^2\circ\tau \quad \text{et} \quad \mathfrak{S}_3 = \{\mathrm{I},\sigma,\sigma^2,\tau,\sigma\circ\tau,\sigma^2\circ\tau\}.$$

2. On considère un groupe $(G,\star)$ d'élément neutre e. On suppose que G contient deux éléments s et t, d'ordres respectifs 3 et 2, tels que

$$t \star s = s^2 \star t.$$

Alors

$$G_0 = \{e,s,s^2,t,s\star t,s^2\star t\}$$

est un sous-groupe d'ordre 6 de $(G,\star)$.
3. Il existe un, et un seul, morphisme de groupes

$$f \,:\, (\mathfrak{S}_3,\circ) \to (G_0,\star)$$

tel que $f(\sigma) = s$ et $f(\tau) = t$ et c'est un isomorphisme.

47. Le Théorème de Lagrange permet de classer les petits groupes.
1. Pour $n = 2$, 3, 5 et 7, tout sous-groupe d'ordre n est isomorphe à $\mathbb{U}_n$.
2. Un groupe d'ordre $n = 4$ qui n'est pas isomorphe à $\mathbb{U}_4$ est isomorphe au groupe de Klein **[31]**.
3. Considérons un groupe $(G,\star)$ d'ordre $n = 6$.
3.a Un tel groupe contient au moins un élément s d'ordre 3 **[33]** ainsi qu'un élément $t \notin \langle s\rangle$ d'ordre 2 **[32]**.
3.b Si s et t commutent, alors $G = \langle st\rangle$; sinon **[46]**, le groupe $(G,\star)$ est isomorphe au groupe symétrique $\mathfrak{S}_3$.

48. Sous-groupes normaux
Soit $(G,\star)$, un groupe.
48.1 ✍ *Un sous-groupe H de $(G,\star)$ est* **normal*** *(ou* **distingué****) lorsqu'il est stable par conjugaison :*

$$\forall\, h \in H,\ \forall\, x \in G, \quad x \star h \star x^{-1} \in H.$$

On note alors $H \lhd G$.

48.2 Un sous-groupe H est normal si, et seulement si, ses classes à gauche et à droite coïncident :

$$H \lhd G \iff \forall\, x \in G, \quad xH = Hx.$$

48.3 Si $f : G \to G'$ est un morphisme de groupes, alors $\operatorname{Ker} f$ est un sous-groupe normal de $(G, \star)$.

48.4 Structure de groupe quotient
Si H est un sous-groupe normal de $(G, \star)$, alors l'ensemble quotient **[3.2]** ${}^{G}/_{H}$ est muni d'une structure de groupe avec

$$\forall\, x, y \in G, \quad (xH) \otimes (yH) = (x \star y)H$$

et la ***projection canonique*** $\pi : G \to {}^{G}/_{H}$ définie par

$$\forall\, x \in G, \quad \pi(x) = xH$$

est un morphisme de groupes dont le noyau est égal au sous-groupe H.

49. Centre d'un p-groupe [4]
Soit $(G, \star)$, un groupe.
49.1 ✍ *Le* **centre** *du groupe $(G, \star)$ est l'ensemble des éléments qui commutent à tous les autres.*

$$Z(G) = \{x \in G : \forall\, y \in G, \quad x \star y = y \star x\}.$$

49.2 Le centre de $(G, \star)$ est un sous-groupe de $(G, \star)$.
49.3 Un élément x de G appartient au centre si, et seulement si, sa classe de conjugaison Ω_x est un singleton.
49.4 ✍ *Soit p, un nombre premier. Un groupe $(G, \star)$ est un* **p-groupe*** *lorsque l'ordre de G est une puissance de p.*
49.5 Un p-groupe contient au moins un élément d'ordre p.
49.6 On suppose que $(G, \star)$ est un p-groupe.

1. Pour tout élément a de G, le stabilisateur de a est aussi un p-groupe et la cardinal de la classe de conjugaison est une puissance de p.
2. Le cardinal du centre de $(G, \star)$ est divisible par p, donc le centre $Z(G)$ n'est pas réduit à $\{e\}$.

50. Exposant d'un groupe abélien fini
Soit $(G, \star)$, un groupe abélien fini.

1. Soit m, le plus petit commun multiple des ordres des éléments de G. On considère sa décomposition en produit de facteurs premiers :

$$m = \prod_{i=1}^{r} p_i^{\alpha_i}$$

Pour tout $1 \leqslant i \leqslant r$, il existe un élément $X_i \in G$ dont l'ordre est égal à $p_i^{\alpha_i} q_i$, où $p_i \wedge q_i = 1$.
Pour tout $1 \leqslant i \leqslant r$, l'ordre de $x_i = X_i^{q_i}$ est égal à $p_i^{\alpha_i}$ et **[44]** l'ordre de $a = x_1 \cdots x_r$ est égal à m.
L'entier m est donc l'ordre maximal pour les éléments de G.

2. Soient $(\mathbb{K}, +, \times)$, un corps commutatif et G, un sous-groupe fini de $\mathbb{K}^\times$. En notant m, le plus petit commun multiple des ordres des éléments de G, on a

$$G \subset \{x \in \mathbb{K} : x^m = 1_{\mathbb{K}}\}.$$

L'ordre de G est donc inférieur à m et, d'après la première question, le groupe $(G, \times)$ est cyclique.

51. Un groupe indécomposable
Soit p, un nombre premier. Pour tout $\alpha \in \mathbb{N}$, on pose

$$\zeta_\alpha = \exp\frac{2i\pi}{p^\alpha} \quad \text{et} \quad G_\alpha = \langle \zeta_\alpha \rangle.$$

1. La famille $(G_\alpha)_{\alpha \in \mathbb{N}}$ est une suite croissante de sous-groupes de $(\mathbb{C}^*, \times)$ et leur union

$$U_p = \bigcup_{\alpha \in \mathbb{N}} G_\alpha$$

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

2. Si G est un sous-groupe de $(G_\alpha, \times)$, alors **[24.2]** il existe $\beta \in [\![0, \alpha]\!]$ tel que $\#(G) = p^\beta$ et de ce fait $G = G_\beta$.
Les sous-groupes de $(U_p, \times)$ contenus dans un G_α sont donc les G_β pour $0 \leqslant \beta \leqslant \alpha$.
3. Soit G, un sous-groupe de $(U_p, \times)$ tel que

$$\forall\, \alpha \in \mathbb{N}, \qquad G \cap G_\alpha^c \neq \varnothing.$$

Pour $x \in G \cap G_\alpha^c$, on pose

$$n = \min\{k \in \mathbb{N} \; x \in G_k\} > \alpha.$$

Il existe alors $k \in \mathbb{Z}$ tel que $x = \zeta_n^k$ et comme $x \notin G_{n-1}$, alors k et p^n sont premiers entre eux et

$$G_\alpha \subset G_n \subset G.$$

Ainsi, $G = U_p$.
4. S'il existait deux groupes H et K ainsi qu'un isomorphisme φ de U_p sur le groupe produit $H \times K$, alors $\varphi_*(\{1\} \times K)$ et $\varphi_*(H \times \{1\})$ seraient deux sous-groupes de U_p dont l'intersection serait réduit à $\{1\}$.
Donc H ou K est réduit à son élément neutre.

52. Quotient d'un groupe commutatif
Soient $(G, \star)$, un groupe commutatif ; $(H, \bullet)$, un groupe et f, un morphisme de groupes de G dans H.
52.1 ✍ *Pour tout $x \in G$, la* **classe de x modulo** $\operatorname{Ker} f$ *est définie par*

$$\mathscr{C}(x) = \{x \star h,\ h \in \operatorname{Ker} f\}.$$

L'ensemble des classes modulo $\operatorname{Ker} f$

$$G/\operatorname{Ker} f = \{\mathscr{C}(x),\ x \in G\}$$

est appelé le **quotient de G par** $\operatorname{Ker} f$.
52.2 La relation binaire $\sim$ définie par

$$\forall\, x, y \in G, \qquad x \sim y \iff \exists\, h \in \operatorname{Ker} f, \quad y = x \star h$$

est une relation d'équivalence sur G et les classes modulo $\operatorname{Ker} f$ sont les classes d'équivalence de cette relation d'équivalence.
52.3 ✍ *Quels que soient x et y dans G, on pose*

$$\mathscr{C}(x) \otimes \mathscr{C}(y) = \mathscr{C}(x \star y).$$

52.4 Si $\mathscr{C}(x_1) = \mathscr{C}(x_2)$ et $\mathscr{C}(y_1) = \mathscr{C}(y_2)$, alors

$$\mathscr{C}(x_1 \star y_1) = \mathscr{C}(x_2 \star y_2).$$

Par conséquent, l'opération $\otimes$ est une loi de composition interne, associative et commutative sur le quotient $G/\operatorname{Ker} f$.
52.5 L'opération $\otimes$ définit une structure de groupe sur $G/\operatorname{Ker} f$, dont l'élément neutre est $\mathscr{C}(e_G)$.
L'application $\mathscr{C}$ est alors un morphisme de groupes de G sur $G/\operatorname{Ker} f$. Ce morphisme de groupes est surjectif ; son noyau est égal à $\operatorname{Ker} f$.
52.6 Pour tout élément $C \in G/\operatorname{Ker} f$, il existe $x \in G$ tel que $C = \mathscr{C}(x)$ et on pose alors

$$\varphi(C) = f(x).$$

1. L'application $\varphi : G/\operatorname{Ker} f \to H$ est bien définie.
2. L'application φ est un morphisme de groupes injectif.
3. Si le morphisme f est surjectif, alors φ réalise un isomorphisme de $G/\operatorname{Ker} f$ sur H.

52.7 Soient $n \geqslant 2$, un entier et $\zeta = \exp(2i\pi/n)$. L'application

$$f = \left[k \mapsto \zeta^k\right]$$

est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{U}_n, \cdot)$ qui induit un isomorphisme du groupe additif $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ sur le groupe multiplicatif $(\mathbb{U}_n, \cdot)$. →**[19]**

53. Le groupe symétrique $\mathfrak{S}_n$ peut être engendré par une famille de $(n-1)$ transpositions. Si $1 \leqslant r < n-1$, alors une famille de r transpositions ne peut engendrer $\mathfrak{S}_n$.

54. Un groupe fini $(G, \star)$ d'ordre n est cyclique si, et seulement si, pour tout entier $d \in \mathbb{N}^*$ divisant n, il existe au plus un sous-groupe d'ordre d de $(G, \star)$.

II

Anneaux et corps

55. Exemples et contre-exemples
On identifie un anneau $(A,+,\star)$ à l'ensemble A lorsque les opérations sont usuelles.

55.1 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.

55.2 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.

55.3 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.

55.4 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.

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

55.6 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.

Éléments remarquables d'un anneau

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

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

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

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

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

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

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

57.4 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 $x^{n-1}\neq 0_A$.

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

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

58. Diviseurs de zéro
58.1 ✍ *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. $y\star x = 0_A$).*
58.2 Un diviseur de zéro n'est pas inversible.
58.3 Tout élément nilpotent non nul est un diviseur de zéro.
58.4 ✍ *Un* **anneau intègre** *est un anneau commutatif sans diviseur de zéro.*

Morphismes d'anneaux

59. 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.

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

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

61. Soit $\varphi : A\to B$, un morphisme d'anneaux.
61.1 Pour tout $x\in A$ et tout $n\in\mathbb{Z}$,

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

et en particulier, $\varphi(0_A) = 0_B$.
61.2

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

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

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

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

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

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

63. ✍ *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 $(B,\oplus,\otimes)$.*

64. Soit $\varphi : A\to B$, un isomorphisme d'anneaux.
64.1 La bijection réciproque φ^{-1} est un morphisme d'anneaux de $(B,\oplus,\otimes)$ dans $(A,+,\star)$.
64.2 ➙ *Un élément $x\in A$ est inversible si, et seulement si, son image $\varphi(x)\in B$ est inversible.*
64.3 Si $x\in A$ est nilpotent d'indice n, alors $\varphi(x)$ est aussi nilpotent d'indice n.
64.4 Si $x\in A$ est un diviseur de zéro, alors $\varphi(x)$ est aussi un diviseur de zéro.

II.1 Produit fini d'anneaux

65. 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

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

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

65.2 ✍ *L'anneau $(A_1 \times A_2, \oplus, \bullet)$ est l'***anneau produit** *de l'anneau $(A_1, +, \star)$ par l'anneau $(A_2, +, \otimes)$.*
65.3 L'élément nul de l'anneau produit est $(0_{A_1}, 0_{A_2})$; l'élément unité est $(1_{A_1}, 1_{A_2})$.
65.4 L'élément (x_1, x_2) est inversible si, et seulement si, x_1 et x_2 sont inversibles. Dans ce cas,

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

65.5 L'anneau produit $(A_1 \times A_2, \oplus, \bullet)$ est commutatif si, et seulement si, les deux anneaux $(A_1, +, \star)$ et $(A_2, +, \otimes)$ sont commutatifs.
65.6 L'anneau produit $(A_1 \times A_2, \oplus, \bullet)$ n'est pas intègre :

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

même si les anneaux A_1 et A_2 sont intègres.

66. Morphismes
66.1 ✍ *Les* **projections canoniques** *sont les applications définies par*

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

66.2 Les projections canoniques sont des morphismes d'anneaux surjectifs.
66.3 ➙ *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.
66.4 Les injections définies par

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

ne sont pas des morphismes d'anneaux.

II.2 Idéaux d'un anneau commutatif

67. ✍ *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 $\star$:*

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

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

69.1 Si un idéal I de A contient au moins un élément inversible, alors $I = A$.
69.2 Les idéaux d'un corps commutatif $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$.
69.3 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 $\mathbb{L}$.

70. Idéal engendré par un élément
70.1 Pour tout $x \in A$, l'ensemble

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

est un idéal de A.
70.2 ✍ *Pour tout $x \in A$, l'idéal xA, aussi noté $\langle x \rangle$, est appelé* **idéal engendré par** *x.*
70.3 Soit I, un idéal de A. Alors :

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

et en particulier

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

71. Opération sur les idéaux
71.1 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 $I \cap J$.
71.2 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 $I + J$.
71.3 ➙ *L'idéal $xA + yA$ est le plus petit idéal de A contenant à la fois x et y.*

II.3 Divisibilité dans un anneau intègre

72. Anneaux intègres [58.4]
72.1 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.
72.2 ➙ **Simplification dans un anneau intègre**
Soit A, un anneau intègre et $z \neq 0_A$. Si $x \star z = y \star z$, alors $x = y$.

73.1 ✍ *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 $x \mid y$.
73.2 ➙

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

74. Éléments inversibles
74.1 Un élément x de A est inversible si, et seulement si, il divise 1_A.
74.2 ➙ *Un élément x de A est inversible si, et seulement si, l'idéal xA est égal à A.*

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

74.3 S'il existe $n \in \mathbb{N}^*$ tel que x^n soit inversible, alors x est inversible.
74.4 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.

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

76. Éléments irréductibles
Soit A, un anneau intègre.
76.1 ✍ *Un élément non nul de A qui peut s'écrire comme le produit de deux éléments non inversibles de A est dit* **composé**.
76.2 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 $x = yz$.
76.3 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 $\deg Q_1 \geqslant 1$ et $\deg Q_2 \geqslant 1$.
76.4 Si x est le produit de deux éléments y et z non inversibles, alors

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

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

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

77. Polynômes irréductibles et extensions de corps
Soient $\mathbb{K}$ et $\mathbb{L}$, deux corps tels que $\mathbb{K} \subset \mathbb{L}$: on dit que $\mathbb{L}$ est une ***extension*** du corps $\mathbb{K}$.
77.1 Tout polynôme $P \in \mathbb{K}[X]$ peut aussi être considéré comme un élément de $\mathbb{L}[X]$.

77.2 Un même polynôme $P \in \mathbb{K}[X]$ peut donc être irréductible en tant qu'élément de $\mathbb{K}[X]$ (on dit alors ***irréductible sur*** $\mathbb{K}$) sans être irréductible en tant qu'élément de $\mathbb{L}[X]$.
En revanche, si un polynôme est irréductible sur $\mathbb{L}$, alors il est nécessairement irréductible sur $\mathbb{K}$.
77.3 Par exemple, X^2+1 est irréductible sur $\mathbb{R}$ (c'est-à-dire en tant qu'élément de l'anneau $\mathbb{R}[X]$), mais pas sur $\mathbb{C}$.
De même, X^3-2 est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$.

Anneaux euclidiens

78. 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. →**[70]**

79. ➙ **Idéaux de $\mathbb{Z}$ [12.6]**
Pour tout idéal I de $\mathbb{Z}$, il existe un, et un seul, entier $n \in \mathbb{N}$ tel que

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

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

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

80.3 ➙ *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.*

Entraînement

81. **Questions pour réfléchir**
1. Soient x et y, deux éléments d'un anneau A.
1.a Si $xy = 1_A$, l'élément x est-il inversible ?
1.b Si x est inversible et si $xy = 1_A$, alors $yx = 1_A$.
2. 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.
3. L'indice de nilpotence peut-il être nul ? égal à 1 ?
4. L'indice de nilpotence de x est inférieur à n si, et seulement si, $x^n = 0$.
5. Un produit d'éléments nilpotents est-il encore un élément nilpotent ?
6. *Suite de* **[61]** –
6.a Est-il possible que $\varphi(x)$ soit inversible sans que x soit inversible ?
6.b Si x est un diviseur de zéro, $\varphi(x)$ est-il encore un diviseur de zéro ?
7. Quels sont les éléments nilpotents d'un anneau produit ?
8. On suppose que les seuls idéaux de l'anneau commutatif A sont $\{0\}$ et A.
8.a Si $x \neq 0$, alors l'élément unité 1_A appartient à l'idéal xA engendré par x.
8.b L'anneau A est en fait un corps.
9. *Suite de* **[73.1]** – Si un élément x non nul divise y, alors il existe un, et un seul, élément $q \in A$ tel que $y = q \star x$.
10. Pourquoi la notion de divisibilité est-elle sans intérêt dans un corps ?

82. Soient A et B, deux anneaux commutatifs et $f : A \to B$, un morphisme d'anneaux.
1. Si J est un idéal de B, alors son image réciproque $f^*(J)$ est un idéal de A.
2. Si I est un idéal de A et si f est surjectif, alors l'image directe $f_*(I)$ est un idéal de B.

83. **Radical d'un idéal**
Soit I, un idéal d'un anneau commutatif $(A, +, \star)$. Le ***radical*** de l'idéal I est l'ensemble $R(I)$ défini par

$$\forall\, x \in A, \quad x \in R(I) \iff \exists\, p \in \mathbb{N}, \quad x^p \in I.$$

1. Le radical $R(I)$ est un idéal de l'anneau A.
2. Si $I = n\mathbb{Z}$ où l'entier n admet pour décomposition en produit de facteurs premiers

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

alors $R(I) = m\mathbb{Z}$ avec $m = p_1 \cdots p_r$.

84. On pose

$$\mathbb{K} = \mathrm{Vect}_{\mathbb{Q}}(1, \sqrt{2}) \quad \text{et} \quad \mathbb{L} = \mathrm{Vect}_{\mathbb{K}}(1, \sqrt{3}).$$

1. L'ensemble $\mathbb{K}$ est à la fois un sous-corps de $\mathbb{R}$ et un espace vectoriel de dimension 2 sur $\mathbb{Q}$.
2. L'ensemble $\mathbb{L}$ est à la fois un sous-corps de $\mathbb{R}$, un espace vectoriel de dimension 2 sur $\mathbb{K}$ et un espace vectoriel de dimension 4 sur $\mathbb{Q}$.
3. Soient a, b et c, trois entiers relatifs tels que

$$a + b\sqrt{2} + c\sqrt{3} = 0.$$

Alors $a = b = c = 0$.
4. On note $A = (\sqrt{2}, \sqrt{3})$.
4.a Un cercle de centre A et de rayon $r \in \mathbb{R}_+$ contient au plus un point de $\mathbb{Z}^2$.
4.b Pour tout entier $n \in \mathbb{N}$, il existe au moins un réel r tel que le disque de centre A et de rayon r contienne exactement n points de $\mathbb{Z}^2$.

85. **Anneau des entiers de Gauss**
L'ensemble des ***entiers de Gauss*** est défini par

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

Pour tout $x \in \mathbb{Z}[i]$, on pose $f(x) = x\overline{x}$.
1. L'ensemble $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
2. Un entier de Gauss x est inversible si, et seulement si, $f(x) = 1$. Le groupe des éléments inversibles de $\mathbb{Z}[i]$ est donc le groupe cyclique $\mathbb{U}_4$.
3. Si $f(x)$ est premier, alors x est irréductible dans $\mathbb{Z}[i]$.
4.a Si $x \in \mathbb{Z}[i]$ et $y \in \mathbb{Z}[i] \setminus \{0\}$, alors il existe $q \in \mathbb{Z}[i]$ tel que

$$f(x/y - q) < 1.$$

4.b Déterminer un tel $q \in \mathbb{Z}[i]$ pour $x = 5 + 6i$ et $y = 2 + i$.
5. Pour tout idéal I de $\mathbb{Z}[i]$, il existe $a \in \mathbb{Z}[i]$ tel que

$$f(a) = \min\{f(x),\ x \in I\}$$

et $I = \langle a \rangle = \{au,\ u \in \mathbb{Z}[i]\}$.

86. Soient s et p, deux entiers relatifs tels que le polynôme

$$P_0 = X^2 - sX + p$$

n'ait pas de racine dans $\mathbb{Q}$.
1. Les racines complexes α et β de P_0 sont distinctes.
2. L'ensemble

$$\mathbb{Z}[\alpha] = \{x + \alpha y,\ (x,y) \in \mathbb{Z}^2\}$$

est un sous-anneau intègre de $(\mathbb{C}, +, \times)$.
3. Pour tout $z = x + \alpha y \in \mathbb{Z}[\alpha]$, on peut définir

$$\overline{z} = x + \beta y \in \mathbb{Z}[\alpha].$$

4.

$$\forall\, (z_1, z_2) \in \mathbb{Z}[\alpha], \quad \overline{z_1 + z_2} = \overline{z} + \overline{z_2}, \quad \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}.$$

5. On pose :

$$\forall\, z \in \mathbb{Z}[\alpha], \quad N(z) = |z\,\overline{z}| \in \mathbb{N}.$$

Un élément z de $\mathbb{Z}[\alpha]$ est inversible si, et seulement si, $N(z) = 1$.

6. L'ensemble

$$\mathbb{Q}[\alpha] = \left\{x + \alpha y,\ (x,y) \in \mathbb{Q}^2\right\}$$

est le plus petit sous-corps de $(\mathbb{C}, +, \times)$ qui contienne $\mathbb{Z}[\alpha]$.

87. Caractéristique d'un corps

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

1. Il existe un, et un seul, morphisme d'anneaux $f : \mathbb{Z} \to \mathbb{K}$.
2. Si ce morphisme f est injectif, le corps $\mathbb{K}$ est dit ***de caractéristique nulle*** et il contient un sous-corps isomorphe à $(\mathbb{Q}, +, \times)$.
3. Sinon, il existe un, et un seul, entier naturel $p \geqslant 1$ tel que $\operatorname{Ker} f = p\mathbb{Z}$. Cet entier p est un nombre premier et le corps $\mathbb{K}$ est dit ***de caractéristique*** p.

87.2 Morphisme de Frobenius

On suppose que $\mathbb{K}$ est un corps de caractéristique p.

4. Pour $1 \leqslant k < p$, le coefficient binomial $\binom{p}{k}$ est divisible par p. et, pour tout entier $n \in \mathbb{Z}$,

$$n^p \equiv n \pmod{p}.$$

5. L'application $[x \mapsto x^p]$ est un morphisme d'anneaux du corps $(\mathbb{K}, +, \star)$ dans lui-même.

88. Factorisation d'un morphisme d'anneaux [52]

Soient $(A, +, \star)$ et $(B, +, \bullet)$, deux anneaux commutatifs et f, un morphisme d'anneaux de A dans B. On définit les classes modulo $I = \operatorname{Ker} f$ par

$$\forall\, x \in A, \quad \mathscr{C}(x) = \left\{x + h,\ h \in \operatorname{Ker} f\right\}$$

et on note A/I, l'ensemble des classes.

88.1 Les classes modulo I forment une partition de A et

$$\forall\, x, y \in A, \qquad \mathscr{C}(x) = \mathscr{C}(y) \iff f(x) = f(y).$$

88.2 L'ensemble quotient A/I est muni d'une structure d'anneau commutatif définie par

$$\begin{aligned} \forall\, x, y \in A, \quad \mathscr{C}(x) \oplus \mathscr{C}(y) &= \mathscr{C}(x + y) \\ \mathscr{C}(x) \otimes \mathscr{C}(y) &= \mathscr{C}(x \star y) \end{aligned}$$

et l'application $\mathscr{C}$ est alors un morphisme d'anneaux surjectif de $(A, +, \star)$ dans $(A/I, \oplus, \otimes)$.

88.3 Il existe un, et un seul, morphisme d'anneaux

$$\varphi : A/I \to B$$

tel que

$$\forall\, x \in A, \quad f(x) = \varphi\big(\mathscr{C}(x)\big).$$

Ce morphisme φ est injectif et, si le morphisme f est surjectif, alors φ est un isomorphisme de A/I sur B.

III

Algèbres et polynômes

89. Soit $\mathbb{K}$, un corps.

89.1 ✍ *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*

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

89.2 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

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

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

89.4 ✍ *L'***élément unité** *d'une algèbre est l'élément neutre pour la multiplication interne.*

89.5 ✍ *Les* **éléments inversibles** *d'une algèbre sont ceux qui ont un symétrique* dans cette algèbre *pour la multiplication interne.*

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

III.1 Sous-algèbres

90. Sous-algèbres

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

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

91. Méthodes

91.1 $(A, +, *, \cdot)$ 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.

91.2 ➙ *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 $*$.*

Exemples d'algèbres et de sous-algèbres

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

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

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

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

92.5 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 $\mathfrak{M}_n(\mathbb{K})$.

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

92.7 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

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

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

93. Soit $(A, +, *, \cdot)$, une algèbre. Le ***commutant*** C_a d'un élément $a \in A$, défini par

$$C_a = \{b \in A : a * b = b * a\},$$

est une sous-algèbre de A (pas nécessairement commutative).

94. Morphismes d'algèbres

94.1 ✍ *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.*

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

94.2 En particulier, un morphisme d'algèbres possède toutes les propriétés d'un morphisme d'anneaux. →**[61]**

94.3 ▷ *Si $f : A\to B$ est un morphisme d'algèbres bijectif, alors sa bijection réciproque est un morphisme d'algèbres.*

94.4 ▷ *L'image d'un morphisme d'algèbres $f : A\to B$ est une sous-algèbre de B.*

94.5 ▷ *Le noyau d'un morphisme d'algèbres $f : \mathscr{A}\to B$ est à la fois un sous-espace vectoriel et un idéal de A.*

III.2 Action des polynômes sur une algèbre

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

95.1 ✍ *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*

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

95.2 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.

95.3 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
$$P_1(a)=Q(a)*P_0(a)+R(a).$$

95.4 ➙ **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.

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

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

95.6 ➙ *Soit $a\in A$. Si $b\in A$ est inversible, alors*

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

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

96. Sous-algèbre engendrée par un élément

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

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

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

96.3 ➙ *La sous-algèbre $\mathbb{K}[a]$ est commutative et*

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

97. Idéal annulateur

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

97.2 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.

97.3 ➙ *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 :*

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

97.4 ✍ *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.*

97.5 ✍ *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.* →**[80.3]**

97.6 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).

97.7 ➙ *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.*

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

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

Entraînement

98. Questions pour réfléchir

1. Le sous-espace $\mathbb{K}_n[X]$ est-il une sous-algèbre de $\mathbb{K}[X]$?
2.a L'ensemble $\mathrm{GL}_n(\mathbb{K})$ des matrices inversibles est-il une sous-algèbre de $\mathfrak{M}_n(\mathbb{K})$?
2.b Et l'ensemble $\mathcal{O}_n(\mathbb{R})$ des matrices orthogonales ?
2.c Et l'ensemble $\mathcal{S}_n(\mathbb{R})$ des matrices symétriques ?
2.d Et l'ensemble $\mathcal{U}_n^0(\mathbb{K})$ des matrices triangulaires supérieures strictes (dont les coefficients diagonaux sont tous nuls) ?
2.e Et l'ensemble des matrices triangulaires ?
3. Condition pour que l'algèbre $\mathscr{A}(\Omega,E)$ soit une algèbre commutative ?
4. *Suite de* [**93**] – Comparer la sous-algèbre $\mathbb{K}[a]$ et le commutant de a pour $A=\mathfrak{M}_n(\mathbb{K})$ et $a=I_n$.
5. Le noyau d'un morphisme d'algèbres $f : A\to B$ est-il une sous-algèbre de A ?
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.

99. 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.

100. Polynôme minimal d'un endomorphisme
Soit $u\in\mathrm{L}(E)$, un endomorphisme admettant un polynôme minimal μ.

1. Pour tout $x\in E$, l'ensemble
$$\mathcal{N}_x=\big\{P\in\mathbb{K}[X]\ :\ P(u)(x)=0_E\big\}$$
est un idéal de $\mathbb{K}[X]$, engendré par un diviseur de μ.
2. Si μ est scindé à racines simples, alors il existe un vecteur $x\in E$ tel que l'idéal $\mathcal{N}_x$ soit engendré par μ.

101. Morphisme d'évaluation [95]

101.1 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 $\mathbb{K}$.

101.2 Nombres algébriques, nombres transcendants

Le corps $A = \mathbb{C}$ est considéré comme un espace vectoriel sur le corps des scalaires $\mathbb{K} = \mathbb{Q}$. 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 $(\ell\mathrm{n}\, p)_{p\in\mathfrak{P}}$ 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 $\operatorname{Ker} \mathcal{E}_a \subset \mathbb{Q}[X]$.

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

6.b En tant qu'élément de $\mathbb{C}[X]$, le polynôme P_0 est scindé à racines simples.

6.c 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.d L'algèbre $\mathbb{Q}[a]$ est un sous-corps de $\mathbb{C}$. En tant que $\mathbb{Q}$-espace vectoriel, il admet
$$(1, a, \dots, a^{d-1})$$
pour base, où $d = \deg P_0$.

102.

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 $[M \mapsto M^\top]$ est-elle un isomorphisme d'algèbre de $\mathfrak{M}_n(\mathbb{K})$ sur $\mathfrak{M}_n(\mathbb{K})$?

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

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

$$\begin{pmatrix} 3 & 4 & -4 \\ -4 & -5 & 4 \\ -2 & -2 & 1 \end{pmatrix} \qquad \begin{pmatrix} -4 & -6 & 6 \\ 6 & 8 & -6 \\ 3 & 3 & -1 \end{pmatrix}$$
$$\begin{pmatrix} -2 & 0 & 0 \\ -4 & 6 & -6 \\ -6 & 12 & -11 \end{pmatrix} \qquad \begin{pmatrix} 5 & 4 & -4 \\ -4 & -3 & 4 \\ -2 & -2 & 3 \end{pmatrix}$$

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

$$\begin{pmatrix} 0 & -2 & 2 \\ -7 & -11 & 10 \\ -8 & -14 & 13 \end{pmatrix} \qquad \begin{pmatrix} -7 & -8 & 8 \\ 2 & -1 & 0 \\ -2 & -6 & 5 \end{pmatrix}$$
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 3 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 \\ 7 & 10 & -8 \\ 8 & 12 & -9 \end{pmatrix}$$

106. On considère le polynôme $P_0 = X^3 - 2 \in \mathbb{Q}[X]$ et on note α, une racine complexe de ce polynôme.

1. Le polynôme P_0 est irréductible sur $\mathbb{Q}$.
2. L'ensemble
$$A = \mathrm{Vect}_{\mathbb{Q}}(1, \alpha, \alpha^2)$$
est un espace vectoriel de dimension 3 sur $\mathbb{Q}$.
3. Pour tout élément non nul $u \in A$, l'application
$$f_u = [z \mapsto uz]$$
est un automorphisme de l'espace vectoriel A. L'ensemble A est donc un sous-corps de $\mathbb{C}$. →**[116]**

Questions, exercices & problèmes

Perfectionnement

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

108. 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 **[114]**.

4. Comment calculer le polynôme minimal **[97.5]** d'une matrice $A \in \mathfrak{M}_3(\mathbb{K})$?

109. Questions pour réfléchir

1. Quels algorithmes reposent-ils sur les factorisations du groupe symétrique **[10]** ? du groupe linéaire **[9.3]** ?

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

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

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

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

6. *Suite de* **[103]** – Étudier le cas où la dimension de $\mathbb{K}[u]$ est infinie.

Approfondissement

110. Il existe une infinité de points $(x, y) \in \mathbb{Q}^2$ tels que

$$x^2 + y^2 = 1.$$

111. Théorème de Gauss-Lucas

Soit $P \in \mathbb{C}[X]$, de degré supérieur à 2.

1. Les racines de P' appartiennent à l'enveloppe convexe des racines de P.

2. En particulier, si les parties réelles des racines de P sont toutes strictement négatives, alors les parties réelles des racines de P' sont toutes strictement négatives.

112. 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 $\mathbb{C}$.

113. Exemples de parties génératrices

113.1 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.

113.2 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

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

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

114. 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.

Pour aller plus loin

115. Démonstration du théorème de Lagrange [24.2]

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

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

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

116. Idéaux maximaux

Soient $(A, +, \star)$, un anneau commutatif et I, un idéal de A.

116.1 ✍ *L'idéal I est dit* **maximal** *lorsque $I \neq A$ et que le seul idéal qui contienne strictement I soit l'anneau A lui-même.*

116.2 Pour $A = \mathbb{Z}$, l'idéal $n\mathbb{Z}$ est maximal si, et seulement si, n est un nombre premier.

116.3 On note A, l'ensemble des suites rationnelles $u \in \mathbb{Q}^N$ qui vérifient le ***critère de Cauchy*** :

$$\forall\, \varepsilon > 0,\ \exists\, N \in \mathbb{N},\ \forall\, n, p \geqslant N, \quad |u_n - u_p| \leqslant \varepsilon.$$

L'ensemble Z des suites rationnelles de limite nulle est un idéal maximal de l'anneau A.

116.4 On considère un idéal maximal I.

1. La relation binaire $\sim$ définie par

$$\forall\, x, y \in A, \quad x \sim y \iff x - y \in I$$

est une relation d'équivalence sur A. La classe d'équivalence de l'élément x est notés $\mathscr{C}(x)$ et l'ensemble des classes d'équivalence est noté A/I.

2. L'ensemble quotient A/I, muni des deux opérations définies par

$$\begin{aligned} \forall\, x, y \in A, \quad \mathscr{C}(x) \oplus \mathscr{C}(y) &= \mathscr{C}(x+y) \\ \mathscr{C}(x) \otimes \mathscr{C}(y) &= \mathscr{C}(x \star y) \end{aligned}$$

est un anneau commutatif et l'application $\mathscr{C} : A \to {}^{A}\!/_{I}$ est un morphisme d'anneaux.

3. Si J est un idéal de l'anneau quotient ${}^{A}\!/_{I}$, alors son image réciproque $\mathscr{C}^*(J)$ est un idéal de A qui contient I et comme I est maximal, l'anneau quotient ${}^{A}\!/_{I}$ est un corps.

116.5 On considère l'anneau $A = \mathbb{K}[X]$ et I, l'idéal engendré par un polynôme $P_0 \in \mathbb{K}[X]$ non constant. Si l'anneau quotient ${}^{A}\!/_{I}$ est un corps, alors le polynôme P_0 est irréductible.

116.6 Pour les opérations usuelles, l'ensemble $A = \mathscr{C}^0(\mathbb{R}, \mathbb{R})$ des applications continues de $\mathbb{R}$ dans $\mathbb{R}$ est un anneau commutatif.

4. Pour toute partie non vide X de $\mathbb{R}$, l'ensemble $I(X)$ des applications de $\mathbb{R}$ dans $\mathbb{R}$ qui sont nulles sur X est un idéal de A.

5. Pour tout $x_0 \in \mathbb{R}$, l'ensemble $I(x_0)$ des applications de $\mathbb{R}$ dans $\mathbb{R}$ qui sont nulles en x_0 est un idéal.

6. Quels que soient les réels distincts x_1 et x_2,

$$\forall\, f \in A,\ \forall\, x \in \mathbb{R}, \quad f(x) = \frac{x - x_1}{x_2 - x_1} \cdot f(x) + \frac{x_2 - x}{x_2 - x_1} \cdot f(x).$$

Pour tout $x_0 \in \mathbb{R}$, l'idéal $I(x_0)$ est maximal et l'anneau quotient $A/I(x_0)$ est un corps isomorphe à $(\mathbb{R}, +, \times)$.

117. Anneaux euclidiens

Un anneau euclidien est un anneau intègre muni d'une opération qui généralise la division euclidienne.

117.1 ✍ *Soit $(A, +, \star)$, un anneau intègre. On note A^*, l'ensemble des éléments* non nuls *de l'ensemble A. Un* **stathme*** *sur A est une application $f : A^* \to \mathbb{N}$ telle que*

—
$$\forall\, (x, y) \in A \times A^*, \quad f(x \star y) \geqslant f(x)$$

— *quels que soient $a \in A$ et $b \in A^*$, il existe au moins un couple*

$$(q, r) \in A \times A$$

tel que

$$a = b \star q + r$$

avec $r = 0_A$ ou $f(r) < f(b)$.

117.2 ✍ *Un anneau intègre $(A, +, \star)$ muni d'un stathme est un* **anneau euclidien***.

117.3 Exemples d'anneaux euclidiens

— $A = \mathbb{Z}$ avec $f(x) = |x|$

— $A = \mathbb{K}[X]$ avec $f(x) = \deg x$

— $A = \mathbb{Z}[i]$ avec $f(x) = x\overline{x}$ →**[85]**

— $A = \mathbb{Z}[\sqrt{2}]$ avec $f(a + \sqrt{2}b) = |a^2 - 2b^2|$

117.4 Si $f : A^* \to \mathbb{N}$ est un stathme et si

$$\forall\, x \neq y, \qquad f(x - y) \leqslant \sup\{f(x), f(y)\},$$

alors le couple (q, r) est unique.

117.5 Soit I, un idéal d'un anneau euclidien.

1. Il existe un élément $a \in I$ tel que

$$f(a) = \min\{f(x),\ x \in I\}$$

et tout élément de I est divisible par a.

2. Il existe un élément $a \in I$ tel que I soit l'idéal de A engendré par a.

118. *Suite de* **[116.6]** – On considère l'anneau $A = \mathscr{C}^0([0,1], \mathbb{R})$ et I, un idéal maximal de A.

1. Pour toute fonction $f \in I$, l'ensemble

$$Z(f) = \{x \in [0,1] \,:\, f(x) = 0\}$$

est une partie compacte non vide de $[0,1]$.

2. Si l'ensemble

$$Z_\omega = \bigcap_{f \in I} Z(f)$$

est vide, alors il existe une famille finie $(f_k)_{1 \leqslant k \leqslant n}$ d'éléments de I telle que

$$\bigcap_{k=1}^{n} Z(f_k) = \varnothing.$$

3. Soient $(f_k)_{1 \leqslant k \leqslant n}$, une famille finie d'éléments de I. Comme la fonction $f_1^2 + \cdots + f_n^2$ appartient à I, il existe $x_0 \in [0,1]$ tel que

$$\forall\, 1 \leqslant k \leqslant n, \quad f_k(x_0) = 0.$$

4. Un idéal I de A est maximal si, et seulement si, il existe un réel $x_0 \in [0,1]$ tel que

$$\forall\, f \in A, \quad f \in I \iff f(x_0) = 0.$$

119. Applications polynomiales

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

119.1 ✍ *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 $(k_1, \ldots, k_d) \in \mathbb{N}^d$.

119.2 ✍ *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.

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

119.4 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.

119.5 ↣ *Étant donnés deux multi-indices k et ℓ dans $\mathbb{N}^d$,*

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

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

1. Si la fonction polynomiale

$$\Big[x \mapsto \sum_{k\in\mathbb{N}} a_k x^k\Big]$$

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 $\mathbb{K}[x_1,\dots,x_d]$ 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 $d \geqslant 1$ et tout polynôme $P \in \mathbb{K}[x_1,\dots,x_d]$, 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 ?

119.7✍ 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*

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

119.8 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.

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

120. Corps des nombres algébriques

Soit $a \in \mathbb{C}$, un nombre algébrique. On sait **[101.2]** que l'ensemble

$$\mathbb{Q}[a] = \big\{P(a),\, P \in \mathbb{Q}[X]\big\} = \mathrm{Vect}_{\mathbb{Q}}(a^n,\, n \in \mathbb{N})$$

est un sous-corps de $\mathbb{C}$ et un espace vectoriel de dimension finie sur $\mathbb{Q}$.

1. Soit b, un nombre algébrique. L'ensemble

$$\mathbb{Q}[a,b] = \big\{P(a,b),\, P \in \mathbb{Q}[X,Y]\big\} = \mathrm{Vect}_{\mathbb{Q}}(a^m b^n,\, (m,n) \in \mathbb{N}^2)$$

est une sous-algèbre de $(\mathbb{C},+,\times)$ de dimension finie sur le corps $\mathbb{K} = \mathbb{Q}[a]$ et donc de dimension finie sur $\mathbb{Q}$, avec

$$\dim_{\mathbb{Q}} \mathbb{Q}[a,b] = \dim_{\mathbb{Q}[a]} \mathbb{Q}[a,b] \cdot \dim_{\mathbb{Q}} \mathbb{Q}[a].$$

2. Comme

$$\mathbb{Q}[a-b] \subset \mathbb{Q}[a,b] \quad \text{et} \quad \mathbb{Q}[ab] \subset \mathbb{Q}[a,b],$$

les deux nombres $a-b$ et ab sont algébriques.

3. L'ensemble des nombres algébriques est un sous-corps dénombrable de $\mathbb{C}$.

121. Résultant de deux polynômes

On considère deux polynômes P et Q à coefficients dans un corps $\mathbb{K}$, avec $\deg P = n$ et $\deg Q = m$. On pose alors

$$\forall\,(U,V) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X], \quad \Phi(UX^n + V) = PU + QV.$$

121.1

1. L'application Φ est bien définie et c'est un endomorphisme de l'espace vectoriel $\mathbb{K}_{m+n-1}[X]$.

2. Tout polynôme de $\mathrm{Im}\,\Phi$ est divisible par $P \wedge Q$.

3. Si P et Q sont premiers entre eux, alors Φ est injectif.

121.2✍ *Le* **résultant*** *$R(P,Q)$ des polynômes P et Q est le déterminant de l'endomorphisme Φ.*

121.3 Le résultant $R(P,Q)$ est une expression polynomiale en les coefficients des polynômes P et Q.

121.4 ***** *Deux polynômes à coefficients dans $\mathbb{K}$ sont premiers entre eux si, et seulement si, leur résultant $R(P,Q)$ est non nul.*

121.5 *Suite de* **[101.2]** – Soient a et b, deux nombres algébriques, de polynômes minimaux respectifs $P_0 \in \mathbb{Q}[X]$ et $P_1 \in \mathbb{Q}[X]$.

4. On pose $s = a + b$. Les polynômes

$$P = P_0 \quad \text{et} \quad Q = P_1(s - X)$$

ont une racine commune dans $\mathbb{C}$. En tant que polynômes à coefficients dans le corps $\mathbb{K} = \mathbb{Q}(s)$, leur résultant est nul et de ce fait, s est un nombre algébrique.

5. On pose $p = ab$ (en supposant $a \neq 0$). Si $\deg P_1 = m$, alors les polynômes

$$P = P_0 \quad \text{et} \quad Q = X^m P_1(p/X)$$

ont une racine commune dans $\mathbb{C}$ et, de même, p est un nombre algébrique.

122. Approximation rationnelle

122.1 S'il existe une suite de rationnels $x_n = {}^{p_n}\!/_{q_n}$ qui converge vers un réel a, telle que

$$a - \frac{p_n}{q_n} \underset{n\to+\infty}{=} o\Big(\frac{1}{q_n}\Big),$$

alors le nombre a est irrationnel.

122.2 L'origine du principe de Dirichlet

Soit $a \in \mathbb{R}$, un nombre irrationnel.

1. Pour tout entier N, les $N+1$ réels x_k définis par

$$\forall\, 0 \leqslant k \leqslant N, \quad x_k = ka - \lfloor ka \rfloor$$

appartiennent à $[0,1[$.

2. Il existe donc deux entiers $p \in \mathbb{Z}$ et $0 < q \leqslant N$ tels que

$$\Big|a - \frac{p}{q}\Big| < \frac{1}{qN} \leqslant \frac{1}{q^2}.$$

3. Il existe une infinité de couples $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que

$$\Big|a - \frac{p}{q}\Big| \leqslant \frac{1}{q^2}.$$