ALGÈBRE GÉNÉRALE

par David Blottière, le 13 septembre 2023 à 14h16

CHAPITRE 1

« […] la méthode axiomatique permet, lorsqu'on a affaire à des êtres mathématiques complexes, d'en dissocier les propriétés et de les regrouper autour d'un petit nombre de notions, c'est-à-dire, pour employer un mot qui sera défini plus loin avec précision, de les classer suivant les *structures* auxquelles elles appartiennent […] »

Théorie des ensembles, Nicolas Bourbaki

SOMMAIRE

§ 1. RAPPELS SUR LES GROUPES

DÉFINITION 1 (GROUPE). — *Soit G un ensemble et soit une loi de composition interne notée $*$:*

$$* \left| \begin{array}{ccc} G\times G & \longrightarrow & G \\ (x,y) & \longmapsto & x*y\,. \end{array} \right.$$

On dit que $(G,*)$ est un groupe si les trois propriétés suivantes sont satisfaites.

(A1) *la loi $*$ est associative, i.e. :*

$$\forall (x,y,z)\in G^3,\quad (x*y)*z = x*(y*z)\,;$$

(A2) *la loi $*$ possède un élément neutre, i.e. :*

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

(A3) *tout élément de G admet un symétrique pour la loi $*$, i.e. :*

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

Remarque 2 (conséquence de la définition de groupe). — Soit $(G,*)$ un groupe.

1. La loi $*$ étant associative, on pourra omettre les parenthèses dans des calcul. Par exemple, si x,y,z désignent trois éléments de G, l'élément de G noté $(x*y)*z$ qui égale $x*(y*z)$ sera noté plus simplement $x*y*z$.
2. Il n'existe qu'un seul élément e de G vérifiant tel que, pour tout $x\in G$, $x*e = x = x*e$. L'élément e est appelé le neutre du groupe.
3. Si x est un élément de G il existe un seul élément y de G tel que $x*y = e = y*x$. On le nomme le symétrique de x et on le note x^{-1}.
4. L'inverse de e est e, i.e. $e^{-1} = e$.
5. Si x et y sont deux éléments de G, alors $\left(x*y\right)^{-1} = y^{-1}*x^{-1}$.
6. Si x est un élément de G, alors $\left(x^{-1}\right)^{-1} = x$.

■

Remarque 3 (terminologie pour un groupe dont la loi est notée $\times$)). — Si la loi d'un groupe est notée $\times$, le neutre est plutôt noté 1. Quant au symétrique d'un élément x de G, il est alors appelé inverse de x et encore noté x^{-1}. ■

DÉFINITION 4 (GROUPE COMMUTATIF OU ABÉLIEN). — *Soit $(G,*)$ un groupe. Si la loi $*$ vérifie la propriété additionnelle suivante :*

$$\forall (x,y)\in G^2,\quad x*y = y*x$$

alors on dit que le groupe $(G,*)$ est commutatif ou abélien, ou que la loi $*$ est commutative.

Remarque 5 (notations et terminologie pour un groupe abélien). — Lorsque le groupe G est abélien, sa loi est souvent notée $+$. Dans ce cas, le neutre est parfois noté 0. Quant au symétrique d'un élément x de G, il est alors appelé opposé de x et est noté $-x$ (et non x^{-1}). ■

Exemple 6 (groupes). —

1. Les ensembles de nombres livrent les groupes commutatifs suivants.

$$(\mathbf{Z},+)\qquad (\mathbb{Q},+)\qquad (\mathbf{R},+)\qquad (\mathbf{C},+)\qquad (\{-1,1\},\times)\qquad \left(\mathbb{Q}^*,\times\right)\qquad \left(\mathbf{R}^*,\times\right)\qquad \left(\mathbf{C}^*,\times\right)$$

2. L'ensemble $\mathbf{R}[X]$ des polynômes à coefficients dans $\mathbf{R}$ muni de l'addition usuelle $+$ est un groupe.
3. Soit $(p,n)\in \mathbf{N}^*\times\mathbf{N}^*$. L'ensemble $\mathscr{M}_{n,p}(\mathbf{C})$ des matrices à n lignes, p colonnes et à coefficients dans $\mathbf{C}$ muni de l'addition usuelle est un groupe.
4. Si E est un ensemble non vide, alors l'ensemble $S(E)$ des bijections de E dans E muni de la loi $\circ$ est un groupe, appelé groupe des permutations de E. En particulier, pour tout $n\in\mathbf{N}^*$, l'ensemble S_n des bijections de $[\![1,n]\!]$ dans lui-même muni de la loi $\circ$ est un groupe.
5. Soit un entier $n\geqslant 2$. L'ensemble $\mathrm{GL}_n(\mathbf{R})$ des matrices de format (n,n) à coefficients dans $\mathbf{R}$ qui sont inversibles muni de la multiplication usuelle est un groupe non abélien. En effet, les matrices de transvections :

$$T_{1,2}(1) := I_n + E_{1,2}\in \mathrm{GL}_n(\mathbf{R})\qquad \text{et}\qquad T_{2,1}(1) := I_n + E_{2,1}\in \mathrm{GL}_n(\mathbf{R})$$

vérifient :

$$T_{1,2}(1)\times T_{2,1}(1) = I_n + E_{1,2} + E_{2,1} + E_{1,1} \neq I_n + E_{1,2} + E_{2,1} + E_{2,2} = T_{2,1}(1)\times T_{1,2}(1).$$

■

EXERCICE 7. — Justifier que ni $(\mathbf{N},+)$, ni $(\mathbf{Z},\times)$ ne sont des groupes. □

EXERCICE 8. — Soit $(E,\circ)$ un ensemble non vide. Déterminer une condition nécessaire et suffisante pour que le groupe $(S(E),\circ)$ soit abélien. □

§ 2. RAPPELS SUR LES SOUS-GROUPES

DÉFINITION 9 (SOUS-GROUPE D'UN GROUPE). — *Soit $(G,*)$ un groupe, dont le neutre est noté e. Soit H une partie de G. On dit que H est un sous-groupe de $(G,*)$ si :*

(A1) *H contient l'élément neutre, i.e. : $e \in H$.*

(A2) *H est stable pour la loi $*$, i.e. :*

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

(A3) *H est stable pour le passage au symétrique, i.e. :*

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

Exemple 10 (sous-groupes triviaux d'un groupe). — Si $(G,*)$ est un groupe, dont le neutre est noté e, alors $\{e\}$ et G sont des sous-groupes de G. ■

Remarque 11 (structure de groupe d'un sous-groupe). — Soit $(G,*)$ un groupe. Soit $H \subset G$ un sous-groupe de $(G,*)$. Alors la restriction de la loi $*$ à H (notée abusivement également $*$) définit une loi de composition interne sur H et $(H,*)$ est un groupe. ■

PROPOSITION 12 (CARACTÉRISATION DES SOUS-GROUPES). — *Soit $(G,*)$ un groupe. Soit H une partie de G. Alors H est un sous-groupe de $(G,*)$ si et seulement si les deux propriétés suivantes sont vérifiées.*

(P1) *H est non vide, i.e. : $H \neq \emptyset$.*

(P2) *H est stable par produit tordu, i.e. :*

$$\forall (x,y) \in H^2, \quad x * y^{-1} \in H .$$

Remarque 13 (caractérisation des sous-groupes d'un groupe abélien). — Soit $(G,+)$ un groupe abélien. En écrivant la proposition précédente lorsque la loi du groupe est noté additivement, il vient qu'une partie H de G est un sous-groupe de $(G,+)$ si et seulement si les deux propriétés suivantes sont vérifiées.

(P1) H est non vide, i.e. : $H \neq \emptyset$.

(P2) H est stable par somme tordue :

$$\forall (x,y) \in H^2, \quad x - y \in H .$$

■

Exemple 14 (sous-groupes de groupes). —

1. L'ensemble :
$$\mathbb{U} := \{z \in \mathbf{C} : |z| = 1\} = \left\{e^{i\theta} : \theta \in \mathbf{R}\right\} \qquad \text{[cercle unité]}$$
est un sous-groupe de $\left(\mathbf{C}^*, \times\right)$.
2. Soit $n \in \mathbf{N}^*$. L'ensemble :
$$\mathbb{U}_n := \left\{z \in \mathbf{C} : z^n = 1\right\} = \left\{e^{i\frac{2k\pi}{n}} : k \in [\![0, n-1]\!]\right\} \qquad \text{[ensemble des racines } n\text{-ièmes de l'unité]}$$
est un sous-groupe de $(\mathbb{U}, \times)$.
3. Soit un entier $n \geqslant 2$. Démontrer que :
$$A_n := \{\sigma \in S_n : \varepsilon(\sigma) = 1\} \qquad \text{[groupe alterné d'indice } n\text{]}$$
est un sous-groupe de $(S_n, \circ)$.
4. Si E est un $\mathbf{K}$-espace vectoriel, alors l'ensemble :
$$\mathrm{GL}(E) := \left\{f \in \mathscr{L}(E) : f \text{ est bijective}\right\} \qquad \text{[groupe des automorphismes de } E\text{]}$$
est un sous-groupe de $(S(E), \circ)$.
5. Soit $n \in \mathbf{N}^*$. L'ensemble :
$$\mathrm{SL}_n(\mathbf{R}) := \{M \in \mathscr{M}_n(\mathbf{R}) : \det(M) = 1\} \qquad \text{[groupe spécial linéaire]}$$
est un sous-groupe de $(\mathrm{GL}_n(\mathbf{R}), \times)$.

■

EXERCICE 15 (GROUPE ORTHOGONAL D'INDICE n). — Démontrer que :

$$\mathrm{O}_n(\mathbf{R}) := \left\{M \in \mathscr{M}_n(\mathbf{R}) : M \times M^\top = I_n\right\} \qquad \text{[groupe orthogonal d'indice } n\text{]}$$

est un sous-groupe de $(\mathrm{GL}_n(\mathbf{R}), \times)$. □

EXERCICE 16 (GROUPE ORTHOGONAL D'UN ESPACE EUCLIDIEN). — Soit $(E, \langle\cdot,\cdot\rangle)$ un espace euclidien. On note $||\cdot||$ la norme associée au produit scalaire $\langle\cdot,\cdot\rangle$. Démontrer que :

$$\mathrm{O}(E) := \left\{f \in \mathscr{L}(E) : \forall x \in E, \quad \left|\left|f(x)\right|\right| = ||x||\right\} \qquad \text{[groupe orthogonal de } E\text{]}$$

est un sous-groupe de $(\mathrm{GL}(E), \circ)$. □

§ 3. RAPPELS SUR LES MORPHISMES DE GROUPES

DÉFINITION 17 (MORPHISME DE GROUPES). — *Soient $(G,*)$ et $(H,\cdot)$ deux groupes. Une application $f : G \longrightarrow H$ est un morphisme de groupes si :*

$$\forall (x,y) \in G^2, \quad f(x*y) = f(x)\cdot g(y).$$

PROPOSITION 18 (PROPRIÉTÉS D'UN MORPHISME DE GROUPES). — *Soient $(G,*)$ et $(H,\cdot)$ deux groupes, Soit $f : G \longrightarrow H$ un morphisme de groupes. Notons respectivement e_G et e_H les éléments neutres de G et H.*

1. *L'application f respecte les neutres, i.e. :*
$$f\left(e_G\right) = e_H\,.$$
2. *L'application f respecte les symétriques, i.e. :*
$$\forall x \in G, \quad f\left(x^{-1}\right) = f(x)^{-1}\,.$$

Exemple 19 (morphismes de groupes). —

1. Si $a \in \mathbf{Z}$, l'application :
$$\varphi_a \left| \begin{array}{ccc} (\mathbf{Z},+) & \longrightarrow & (\mathbf{Z},+) \\ n & \longmapsto & an \end{array} \right.$$
est un morphisme de groupes.
2. L'application
$$\ln \left| \begin{array}{ccc} (\mathbf{R}_{>0},\times) & \longrightarrow & (\mathbf{R},+) \\ x & \longmapsto & \ln(x) \end{array} \right.$$
est un morphisme de groupes.
3. Soit $n \in \mathbf{N}^*$. Pour tout $\sigma \in S_n$, on pose :
$$I(\sigma) := \mathrm{Card}\left(\left\{(i,j) \in [\![1,n]\!]^2 \,:\, i<j \text{ et } \sigma(i) > \sigma(j)\right\}\right) \qquad \text{[nombre d'inversions de } \sigma\text{]}\,.$$
La signature :
$$\varepsilon \left| \begin{array}{ccc} (S_n,\circ) & \longrightarrow & (\{-1,1\},\times) \\ \sigma & \longmapsto & \varepsilon(\sigma) = (-1)^{I(\sigma)} \end{array} \right.$$
est un morphisme de groupes.
4. Soit n^*. L'application :
$$\left| \begin{array}{ccc} (\mathrm{GL}_n(\mathbf{C}),\times) & \longrightarrow & \left(\mathbf{C}^*,\times\right) \\ M & \longmapsto & \det(M) = \displaystyle\sum_{\sigma\in S_n} \varepsilon(\sigma)\cdot \prod_{k=1}^{n} [M]_{k,\sigma(k)} \end{array} \right.$$
est un morphisme de groupes.

■

EXERCICE 20. — Soit un entier $n \geqslant 2$. L'application :

$$f \left| \begin{array}{ccc} (\mathrm{GL}_n(\mathbf{C}),\times) & \longrightarrow & (\mathrm{GL}_n(\mathbf{C}),\times)) \\ M & \longmapsto & M^{\top} \end{array} \right.$$

est-elle un morphisme de groupes? □

EXERCICE 21. — Soit f un morphisme de groupes de $(\mathbf{Z},+)$ dans lui-même. Démontrer que :

$$\exists a \in \mathbf{Z}, \quad \forall n \in \mathbf{Z}, \quad f(n) = a\cdot n.$$

□

PROPOSITION 22 (IMAGE ET IMAGE RÉCIPROQUE D'UN SOUS-GROUPE PAR UN MORPHISME DE GROUPES). — *Soient $(G,*)$, $(H,\cdot)$ deux groupes et $f : G \longrightarrow H$ un morphisme de groupes.*

1. *Soit K un sous-groupe de $(G,*)$. Alors :*
$$f(K) := \left\{f(k) \,:\, k \in K\right\}$$
est un sous-groupe de $(H,\cdot)$.
2. *Soit L un sous-groupe de $(H,\cdot)$. Alors :*
$$f^{-1}(L) := \left\{g \in G \,:\, f\left(g\right) \in L\right\}$$
est un sous-groupe de $(G,*)$.

DÉFINITION 23 (NOYAU ET IMAGE D'UN MORPHISME DE GROUPES). — *Soient $(G,*)$, $(H,\cdot)$ deux groupes et $f : G \longrightarrow H$ un morphisme de groupes.*

1. *L'ensemble*
$$\mathrm{Ker}(f) := \{x \in G \,:\, f(x) = e_H\} = f^{-1}(\{e_H\})$$
est appelé noyau du morphisme f.
2. *L'ensemble*
$$\mathrm{Im}(f) := \{f(x) \,:\, x \in G\} = f(G)$$
est appelé image du morphisme f.

PROPOSITION 24 (STRUCTURES DU NOYAU ET DE L'IMAGE D'UN MORPHISME DE GROUPES). — *Soient $(G,*)$, $(H,\cdot)$ deux groupes et $f : G \longrightarrow H$ un morphisme de groupes.*

1. $\mathrm{Ker}(f)$ *est un sous-groupe de G.*
2. $\mathrm{Im}(f)$ *est un sous-groupe de H.*

Remarque 25 (critère d'injectivité et de surjectivité pour un morphisme de groupes). — Soient $(G,*)$, $(H,\cdot)$ deux groupes et $f : G \longrightarrow H$ un morphisme de groupes.

1. L'application f est injective si et seulement si $\mathrm{Ker}(f) = \{e_G\}$, où e_G désigne le neutre de $(G,*)$.
2. L'application f est surjective si et seulement si $\mathrm{Im}(f) = H$.

■

Exemple 26 (groupe spécial orthogonal). — Soit un entier $n \geqslant 2$. L'application :
$$\left|\begin{array}{ccc} (\mathrm{O}_n(\mathbf{R}),\times) & \longrightarrow & (\mathbf{R}^*,\times) \\ M & \longmapsto & \det(M) \end{array}\right.$$
est un morphisme de groupes. Son noyau est noté $\mathrm{SO}_n(\mathbf{R})$, i.e. :
$$\mathrm{SO}_n(\mathbf{R}) := \{M \in \mathrm{O}_n(\mathbf{R}) \,:\, \det(M) = 1\} \qquad \text{[groupe spécial orthogonal d'indice } n\text{]}.$$

■

EXERCICE 27 (MESURE D'ANGLE D'UNE ROTATION PLANE). — On considère l'application :
$$\rho \left|\begin{array}{ccc} (\mathbf{R},+) & \longrightarrow & (\mathrm{SO}_2(\mathbf{R}),\times) \\ \theta & \longmapsto & \rho(\theta) := \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \end{array}\right..$$

1. Démontrer que l'application ρ est bien définie et surjective.
2. Démontrer que l'application ρ est un morphisme de groupes et préciser son noyau.

□

THÉORÈME 28 (COMPOSITION DE MORPHISMES DE GROUPES). — *Soient $(G_1,*_1)$, $(G_2,*_2)$, $(G_3,*_3)$ trois groupes. Soient $f : (G_1,*_1) \longrightarrow (G_2,*_2)$ et $g : (G_2,*_2) \longrightarrow (G_3,*_3)$ deux morphismes de groupes. Alors :*
$$g \circ f \left|\begin{array}{ccc} (G_1,*_1) & \longrightarrow & (G_3,*_3) \\ x_1 & \longmapsto & g(f(x_1)) \end{array}\right.$$
est un morphisme de groupes.

DÉFINITION 29 (ISOMORPHISME DE GROUPES). — *Soient $(G_1,*_1)$, $(G_2,*_2)$ et $f : (G_1,*_1) \longrightarrow (G_2,*_2)$ une application. On dit que f est un isomorphisme de groupes si :*

1. *f est un morphisme de groupes ;*
2. *f est bijectif.*

Remarque 30 (groupes isomorphes). — Deux groupes sont dits isomorphes s'il existe un isomorphisme de groupes de l'un vers l'autre. ■

EXERCICE 31. — Déterminer tous les isomorphismes de groupes de $(\mathbf{Z},+)$ dans lui-même. □

EXERCICE 32. — Les groupes $(\mathbf{R}^*,\times)$ et $(\mathbf{R}_+^*,\times)$ sont-ils isomophes ? □

PROPOSITION 33 (INVERSE D'UN ISOMORPHISME DE GROUPES). — *Soit $f : (G_1,*_1) \longrightarrow (G_2,*_2)$ un isomorphisme de groupes. Sa bijection réciproque :*
$$f^{-1} \left|\begin{array}{ccc} (G_2,*_2) & \longrightarrow & (G_1,*_1) \\ g_2 & \longmapsto & \text{l'unique } g_1 \in G_1 \text{ tel que } f(g_1) = g_2 \end{array}\right.$$
est un morphisme de groupes.

§ 4. SOUS-GROUPES ADDITIFS DE Z

Rappel 34 (division euclidienne sur Z). — En utilisant la propriété du bon ordre dans $\mathbf{N}$ (toute partie non vide de $\mathbf{N}$ possède un plus petit élément), on démontre qu'il existe une division euclidienne sur $\mathbf{Z}$. Précisément, si $b \in \mathbf{N}^*$, alors pour tout $a \in \mathbf{Z}$, il existe un unique couple $(q,r) \in \mathbf{Z}^2$ tel que :

$$a = qb + r \quad \text{et} \quad 0 \leqslant r \leqslant b-1.$$

On nomme q (resp. r) le quotient (resp. le reste) de la division euclidienne de a par b. ■

PROPOSITION 35 (EXEMPLE FONDAMENTAL DE SOUS-GROUPE ADDITIF DE Z). — *Soit $a \in \mathbf{Z}$. Alors l'ensemble :*

$$a\mathbf{Z} := \{an : n \in \mathbf{Z}\} \qquad \left[\text{ensemble des multiples de } a\right]$$

est un sous-groupe de $(\mathbf{Z},+)$.

THÉORÈME 36 (DESCRIPTION DES SOUS-GROUPES ADDITIFS DE Z). — *Soit H un sous-groupe de $(\mathbf{Z},+)$. Il existe un unique $a \in \mathbf{N}$ tel que :*

$$H = a\mathbf{Z} := \{an : n \in \mathbf{Z}\}.$$

Remarque 37. — La proposition et le théorème qui précèdent nous livrent le résultat suivant. Les parties de $\mathbf{Z}$ de la forme $a\mathbf{Z}$ (avec $a \in \mathbf{Z}$) sont les seuls sous-groupes de $(\mathbf{Z},+)$. ■

EXERCICE 38 (SOUS-GROUPES ADDITIFS DE R). — Soit H un sous-groupe de $(\mathbf{R},+)$ distinct de $\{0_{\mathbf{R}}\}$.

1. Démontrer que $a := \inf\left(H \cap \mathbf{R}_+^*\right)$ est bien défini.
2. Démontrer que, si $a \in H$, alors $H = a\mathbf{Z}$.
3. Démontrer que, si $a \notin H$, alors H est dense dans $\mathbf{R}$.

□

§ 5. SOUS-GROUPE ENGENDRÉ PAR UNE PARTIE

PROPOSITION 39 (INTERSECTION DE SOUS-GROUPES). — *Soit $(G,*)$ un groupe. Soit $(H_i)_{i\in I}$ une famille de sous-groupes de G indexée par un ensemble I non vide. Alors leur intersection :*

$$H = \bigcap_{i\in I} H_i := \{g \in G : \forall\, i \in I,\ g \in H_i\}$$

est un sous-groupe de G.

EXERCICE 40. — Soient a et b des entiers naturels non nuls. Déterminer le sous-groupe $a\mathbf{Z} \cap b\mathbf{Z}$ de $(\mathbf{Z},+)$. □

EXERCICE 41. — Soit $(G,*)$ un groupe. Soient H et K deux sous-groupes de $(G,*)$. Déterminer une condition nécessaire et suffisante pour que $H \cup K$ soit un sous-groupe de G. □

PROPOSITION 42 (SOUS-GROUPE ENGENDRÉ PAR UNE PARTIE). — *Soient $(G,*)$ un groupe et A une partie non vide de G.*

1. *Parmi les sous-groupes de G qui contiennent la partie A, il en existe un plus petit (pour l'inclusion), appelé sous-groupe engendré par A et noté $< A >$.*
2. *En d'autres termes, $< A >$ est caractérisé par les deux propriétés suivantes :*
   - *$< A >$ est un sous-groupe de G tel que $A \subset < A >$;*
   - *si H sous-groupe de G tel que $A \subset H$, alors $< A > \subset H$ (propriété de minimalité).*
3. *Le sous-groupe engendré par A est l'intersection de tous les sous-groupes de G contenant A :*

$$< A > \;=\; \bigcap_{\substack{H \text{ sous-groupe de } G \\ \text{tel que } A\subset H}} H$$

EXERCICE 43. — Soient a et b des entiers naturels non nuls. Déterminer le sous-groupe $< a, b >$ de $(\mathbf{Z},+)$. □

THÉORÈME 44 (DESCRIPTION DU SOUS-GROUPE ENGENDRÉ PAR UNE PARTIE). — *Soient $(G,*)$ un groupe et $A \subset G$ une partie non vide de G. Notons A^{-1} l'ensemble des inverses des éléments de A :*

$$A^{-1} = \left\{x^{-1} \,:\, x \in A\right\}.$$

Le sous-groupe $< A >$ engendré par A est égal à l'ensemble de tous les produits finis d'éléments de $A \cup A^{-1}$:

$$< A >= \left\{x \in G \,:\, \exists n \in \mathbf{N}^*,\, \exists (x_1,\dots,x_n) \in \left(A \cup A^{-1}\right)^n \text{ tels que } x = x_1 * \dots * x_n\right\}.$$

DÉFINITION 45 (PARTIE GÉNÉRATRICE D'UN GROUPE). — *Soit $(G,*)$ un groupe. Une partie A de G est une partie génératrice si le sous-groupe engendré par A est le groupe G tout entier, i.e. si :*

$$G =< A > .$$

Exemple 46 (parties génératrices de groupes). —

1. Le groupe $(\mathbf{Z},+)$ des entiers relatifs est engendré par l'élément 1.
2. Soit un entier $n \geqslant 2$. Le groupe $\left(\mathbf{Z}^n,+\right)$ est engendré par :
$$\{(1,0,\dots,0),(0,1,\dots,0),\dots,(0,0,\dots,1)\}\ .$$
3. Soit un entier $n \geqslant 2$. Le groupe $(S_n,\circ)$ est engendré par les transpositions :
$$S_n =< \{(i\ j) \,:\, 1 \leqslant i < j \leqslant n\} > \qquad \left[\text{système générateur à } \binom{n}{2} \text{ éléments}\right].$$
4. Soit un entier $n \geqslant 2$. Le groupe $(\mathrm{GL}_n(\mathbf{K}),\times)$ est engendré par les matrices de transvection et les matrices de dilatation :
$$\mathrm{GL}_n(\mathbf{K}) =< \left\{T_{i,j}(\lambda) := I_n + \lambda \cdot E_{i,j} \,:\, (i,j) \in [\![1,n]\!]^2 \text{ tel que } i \neq j \text{ et } \lambda \in \mathbf{K}\right\} \cup \left\{D_i(\lambda) := I_n + (\lambda - 1)\cdot E_{i,i} \,:\, i \in [\![1,n]\!] \text{ et } \lambda \in \mathbf{K}^*\right\} > .$$

■

EXERCICE 47 (UN SYSTÈME GÉNÉRATEUR À DEUX ÉLÉMENTS DU GROUPE DES PERMUTATIONS). — Soit un entier $n \geqslant 2$. Notons :

$$\tau := (1\ 2)$$

la transposition de $[\![1,n]\!]$ échangeant 1 et 2 et σ le cycle de longueur n défini par :

$$\sigma := (1\ 2\ 3\ \dots\ n).$$

Démontrer que $\{(1\ 2),\sigma\}$ engendre le groupe $(S_n,\circ)$. □

EXERCICE 48 (DES SYSTÈMES GÉNÉRATEURS À DEUX ÉLÉMENTS DE $(\mathbf{Z},+)$). — Soient $(a,b) \in \mathbf{Z}^2$. Donner une condition nécessaire et suffisante pour que la partie $\{a,b\}$ engendre le groupe $(\mathbf{Z},+)$. □

EXERCICE 49 (GROUPES DE TYPE FINI). — Un groupe est dit *de type fini* s'il possède une famille génératrice finie.

1. Le groupe $(\mathbf{Q},+)$ est-il de type fini ?
2. Démontrer que $\left(\mathbf{R}^*,\times\right)$ n'est pas de type fini.
3. En déduire que pour tout entiers $n \geqslant 2$, le groupe $(\mathrm{GL}_n(\mathbf{R}),\times)$ n'est pas de type fini.

□

DÉFINITION 50 (NOTATION PUISSANCE DANS UN GROUPE). — *Soit $(G,*)$ un groupe, dont le neutre est noté e. Soit $x \in G$ et soit $n \in \mathbf{Z}$. La puissance n-ième de x est l'élément de G, noté x^n, défini par :*

$$x^n = \begin{cases} \underbrace{x * x * \dots * x}_{n \text{ fois}} & \text{si } n \geqslant 1\,; \\ e & \text{si } n = 0\,; \\ \underbrace{x^{-1} * x^{-1} * \dots * x^{-1}}_{-n \text{ fois}} & \text{si } n \leqslant -1. \end{cases}$$

PROPOSITION 51 (PROPRIÉTÉS DE LA NOTATION PUISSANCE). — *Soient $(G,*)$ un groupe et $(x,n,m) \in G \times \mathbf{Z} \times \mathbf{Z}$.*

$$x^n * x^m = x^{n+m} \qquad \text{et} \qquad \left(x^n\right)^m = x^{nm}.$$

Soient $(G,*)$ un groupe et $(x,y,n) \in G \times G \times \mathbf{Z}$. Les éléments $x^n * y^n$ et $(x*y)^n$ ne sont pas nécessairement égaux, en raison du défaut de commutativité éventuel de la loi $*$.

PROPOSITION 52 (SOUS-GROUPE ENGENDRÉ PAR UN ÉLÉMENT). — *Soient $(G,*)$ un groupe et $a \in G$.*

$$< a >= \{a^n \,:\, n \in \mathbf{Z}\}$$

§ 6. RAPPELS SUR LA RELATION DE CONGRUENCE

DÉFINITION 53 (RELATION DE CONGRUENCE). — *Soit $(n,a,b) \in \mathbf{N}^* \times \mathbf{Z} \times \mathbf{Z}$. On dit que a est congru à b modulo n, et on écrit $a \equiv b\ [n]$, si $a - b \in n\mathbf{Z}$.*

PROPOSITION 54 (CARACTÉRISATION DE LA RELATION DE CONGRUENCE PAR LES RESTES). — *Soit $(n,a,b) \in \mathbf{N}^* \times \mathbf{Z} \times \mathbf{Z}$. Alors $a \equiv b\ [n]$ si et seulement si a et b ont même reste dans la division euclidienne par n.*

PROPOSITION 55 (COMPATIBILITÉ AVEC LA SOMME ET LE PRODUIT). — *Soit $n \in \mathbf{N}^*$. Soit $(a,b,c,d) \in \mathbf{Z}^4$ tels que $a \equiv c\ [n]$ et $b \equiv d\ [n]$. Alors :*

$$a+b \equiv c+d\ [n] \quad \text{et} \quad a \cdot b \equiv c \cdot d\ [n].$$

DÉMONSTRATION. — Nous savons que n divise $(a-c)$ et $(b-d)$ i.e. qu'il existe $(u,v) \in \mathbf{Z}^2$ tel que $a - c = n \cdot u$ et $b - d = n \cdot v$.

- Comme :
$$(a+b) - (c+d) = n \cdot (u+v)$$
n divise $(a+b)-(c+d)$, i.e. $a+b \equiv c+d\ [n]$.
- Comme :
$$a \cdot b - c \cdot d = (c + n \cdot u) \cdot (d + n \cdot v) - c \cdot d = n \cdot (c \cdot v + u \cdot d + n \cdot u \cdot v)$$
n divise $a \cdot b - c \cdot d$, i.e $a \cdot b \equiv c \cdot d\ [n]$. ■

PROPOSITION 56 (COMPATIBILITÉ AVEC LES PUISSANCES). — *Soit $(n,a,b,k) \in \mathbf{N}^* \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{N}^*$. Alors :*

$$a \equiv b\ [n] \implies a^k \equiv b^k\ [n]\ .$$

ÉLÉMENTS DE DÉMONSTRATION. — Se déduit de la précédente proposition à l'aide d'un raisonnement par récurrence. □

EXERCICE 57. — Démontrer que pour tout $n \in \mathbf{N}$, 5 divise $2^{3n+5} + 3^{n+1}$. □

PROPOSITION 58 (LA RELATION DE CONGRUENCE EST UNE RELATION D'ÉQUIVALENCE). — *Soit $n \in \mathbf{N}^*$. La relation de congruence modulo n est une relation d'équivalence.*

Rappel 59 (classes d'équivalence et ensemble quotient). — Soit E un ensemble muni d'une relation d'équivalence $\mathscr{R}$. Pour tout $x \in E$, on note :

$$\overline{x} := \{y \in E\ :\ y \mathscr{R} x\} \in \mathscr{P}(E) \qquad [\text{classe d'équivalence de } x]$$

On rappelle trois propriétés fondamentales des classes d'équivalences.

1. Soit $(x,y) \in E^2$. Alors :
$$x \mathscr{R} y \iff \overline{x} = \overline{y}.$$
$\implies$ Supposons $x \mathscr{R} y$. Soit $z \in \overline{x}$. Alors $z \mathscr{R} y$. Par transitivité de $\mathscr{R}$, $z \mathscr{R} y$. Ainsi $z \in \overline{y}$. Nous en déduisons $\overline{x} \subset \overline{y}$. Par symétrie, $\overline{y} \subset \overline{x}$.
$\impliedby$ Supposons $\overline{x} = \overline{y}$. Comme $\mathscr{R}$ est réflexive, $x \in \overline{x}$. Ainsi $x \in \overline{y}$, d'où $x \mathscr{R} y$.
2. Soit $(x,y) \in E^2$. Alors :
$$\overline{x} = \overline{y} \quad \text{ou} \quad \overline{x} \cap \overline{y} = \emptyset.$$
Supposons $\overline{x} \cap \overline{y} \neq \emptyset$ et démontrons $\overline{x} = \overline{y}$. Soit $z \in \overline{x} \cap \overline{y}$. Alors $z \mathscr{R} x$ et $z \mathscr{R} y$. Par symétrie et transitivité de la relation $\mathscr{R}$, $x \mathscr{R} y$. Nous en déduisons, à l'aide de 1, que $\overline{x} = \overline{y}$.
3. L'ensemble des classes d'équivalence pour la relation $\mathscr{R}$ est appelé ensemble quotient de E par $\mathscr{R}$ et est noté $E/\mathscr{R}$.
$$E = \bigsqcup_{C \in E/\mathscr{R}} C \qquad [\text{partition de } E \text{ suivant les classes d'équivalence}].$$
$\supset$ Cette inclusion est claire car une classe d'équivalence est par essence une partie de E.
$\subset$ Puisque $\mathscr{R}$ est réflexive, $x \in \overline{x}$. Comme $\overline{x}$ est une classe d'équivalence, $\overline{x} \in E/\mathscr{R}$. Donc x appartient bien à la réunion des classes d'équivalence et l'inclusion $\subset$ est établie.
Caractère disjoint de l'union. D'après 2, deux classes d'équivalence distinctes sont disjointes et donc la réunion est bien disjointe.

DÉFINITION 60 (CLASSE D'ÉQUIVALENCE POUR LA RELATION DE CONGRUENCE). — *Soit $(n,a) \in \mathbf{N}^* \times \mathbf{Z}$. Notons :*

$$\overline{a} := \{b \in \mathbf{Z} \,:\, a \equiv b\ [n]\} \qquad [\textit{classe de } a \textit{ modulo } n]$$

l'ensemble des entiers congrus à a modulo n.

PROPOSITION 61 (NOMBRE DE CLASSES D'ÉQUIVALENCE). — *Soit $n \in \mathbf{N}^*$. Il y a exactement n classes d'équivalences distinctes pour la relation de congruence modulo n. Ces n classes sont :*

$$\overline{0}, \overline{1}, \dots, \overline{n-1}.$$

§ 7. LE GROUPE $(\mathbf{Z}/n\mathbf{Z}, +)$

DÉFINITION 62 (L'ENSEMBLE $\mathbf{Z}/n\mathbf{Z}$). — *Soit $n \in \mathbf{N}^*$. On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble des classes déquivalences pour la relation de congruence modulo n. Ainsi :*

$$\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

Soit $n \in \mathbf{N}^*$. On veillera à toujours vérifier soigneusement qu'une application dont la source met en jeu $\mathbf{Z}/n\mathbf{Z}$ est bien définie.
Par exemple l'application :

$$f \left| \begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \longrightarrow & \mathbf{Z} \\ \overline{a} & \longmapsto & a \end{array} \right.$$

n'est pas bien définie. En effet, $\overline{0} = \overline{n}$ dans $\mathbf{Z}/n\mathbf{Z}$, mais :

$$f(\overline{0}) = 0 \neq n = f(\overline{n}).$$

THÉORÈME 63 (LE GROUPE ADDITIF $\mathbf{Z}/n\mathbf{Z}$). — *Soit $n \in \mathbf{N}^*$. Posons :*

$$+ \left| \begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z}) & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \\ \left(\overline{a}, \overline{b}\right) & \longmapsto & \overline{a+b}. \end{array} \right.$$

Alors, l'application $+$ est une loi de composition interne sur $\mathbf{Z}/n\mathbf{Z}$, qui est bien définie et $(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe abélien, de neutre $\overline{0}$.

Exemple 64 (le groupe additif $\mathbf{Z}/6\mathbf{Z}$). — La table du groupe $(\mathbf{Z}/6\mathbf{Z}, +)$ est la suivante.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

1. L'opposé de $\overline{5}$ dans $(\mathbf{Z}/6\mathbf{Z}, +)$ est donc $\overline{1}$.
2. Le sous-groupe engendré par $\overline{2}$ dans $(\mathbf{Z}/6\mathbf{Z}, +)$ est :
$$\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\}.$$
3. L'élément $\overline{1}$ engendre le groupe $(\mathbf{Z}/6\mathbf{Z}, +)$. Il en est de même de de l'élément $\overline{5}$.

PROPOSITION 65 (GÉNÉRATEURS DU GROUPE ADDITIF $\mathbf{Z}/n\mathbf{Z}$). — *Soient $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}$. L'élément $\overline{a}$ de $\mathbf{Z}/n\mathbf{Z}$ engendre le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ si et seulement si a est premier avec n, i.e. :*

$$< \overline{a} >= \mathbf{Z}/n\mathbf{Z} \iff a \wedge n = 1.$$

Exemple 66 (générateurs du groupe additif $\mathbf{Z}/12\mathbf{Z}$). — Les seuls éléments qui engendrent le groupe $(\mathbf{Z}/12\mathbf{Z}, +)$ sont $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.

§ 8. CLASSIFICATION DES GROUPES MONOGÈNES

DÉFINITION 67 (GROUPE MONOGÈNE ET GROUPE CYCLIQUE). — *Soit $(G,*)$ un groupe.*

1. *Le groupe $(G,*)$ est dit monogène s'il est engendré par un élément, i.e. si :*
$$\exists x \in G, \quad G = < x > = \left\{x^n : n \in \mathbf{Z}\right\}.$$
2. *Le groupe $(G,*)$ est dit cyclique s'il est monogène et cyclique.*

***Remarque 68.* —** Tout groupe monogène est abélien. ■

Exemple 69 (groupes monogènes et groupes cycliques). —

1. Le groupe $(\mathbf{Z},+)$ est engendré par l'élément 1. Il est donc monogène
2. Pour tout $n \in \mathbf{N}^*$, le groupe $(\mathbf{Z}/n\mathbf{Z},+)$ est fini et engendré par l'élément $\overline{1}$. Il est donc cyclique.
3. Pour tout $n \in \mathbf{N}^*$, le groupe multiplicatif :
$$\mathbb{U}_n := \left\{z \in \mathbf{C} : z^n = 1\right\} = \left\{e^{i\frac{2k\pi}{n}} : k \in [\![0, n-1]\!]\right\}$$
est fini et engendré par l'élément $e^{i\frac{2\pi}{n}}$. Il est donc cyclique.

■

EXERCICE 70. — Démontrer que le groupe $\left(\mathbf{Z}^2,+\right)$ n'est pas monogène. En déduire que les groupes $(\mathbf{Z},+)$ et $\left(\mathbf{Z}^2,+\right)$ ne sont pas isomorphes. □

EXERCICE 71. — Les groupes $(\mathbf{Z},+)$ et $(\mathbb{Q},+)$ sont-ils isomorphes ? □

PROPOSITION 72 ($\mathbf{Z}/n\mathbf{Z}$ VERSUS $\mathbb{U}_n$). — *Soit $n \in \mathbf{N}^*$. L'application :*
$$\varphi \left| \begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z},+) & \longrightarrow & (\mathbb{U}_n,\times) \\ \overline{a} & \longmapsto & e^{i\frac{2a\pi}{n}} \end{array} \right.$$
est bien définie et est un isomorphisme de groupes.

THÉORÈME 73 (CLASSIFICATION DES GROUPES MONOGÈNES). — *Soit $(G,*)$ un groupe monogène.*

1. *Si G est infini, alors $(G,*)$ est isomorphe à $(\mathbf{Z},+)$.*
2. *Si G est fini de cardinal $n \geqslant 1$, alors $(G,*)$ est isomorphe à $(\mathbf{Z}/n\mathbf{Z},+)$.*

§ 9. THÉORÈME DE LAGRANGE (HP)

THÉORÈME 74 (THÉORÈME DE LAGRANGE). — *Soient $(G,*)$ un groupe fini et H un sous-groupe de G. Alors le cardinal de H divise le cardinal de G.*

DÉMONSTRATION. —

- Pour tout $(x,y) \in G^2$, posons $x\mathscr{R}y$ si et seulement si $x * y^{-1} \in H$. Établissons que $\mathscr{R}$ est une relation d'équivalence sur G.
  - — *La relation $\mathscr{R}$ est réflexive.* Soit $x \in G$. Comme $x * x^{-1} = e_G \in H$, $x\mathscr{R}x$.
  - — *La relation $\mathscr{R}$ est symétrique.* Soient $(x,y) \in G^2$ tels que $x\mathscr{R}y$. Alors $x * y^{-1} \in H$. Comme H est stable par passage à l'inverse :
$$y * x^{-1} = \left(x * y^{-1}\right)^{-1} \in H.$$
Ainsi $y\mathscr{R}x$.
  - — *La relation $\mathscr{R}$ est transitive.* Soient $(x,y,z) \in G^3$ tels que $x\mathscr{R}y$ et $y\mathscr{R}z$. Alors $x * y^{-1} \in H$ et $y * z^{-1} \in H$. Comme H est stable pour la loi $*$:
$$x * z^{-1} = x * y^{-1} * y * z^{-1} \in H.$$
- Comme G est fini, l'ensemble $\mathscr{P}(G)$ des parties de G est fini et donc il n'y a qu'un nombre fini de classes d'équivalence, disons p. Notons $\overline{x_1},\ldots,\overline{x_p}$ la liste exhaustive, sans répétition, des différentes classes d'équivalence. Alors :
$$G = \bigsqcup_{i=1}^{p} \overline{x_i}$$
En conséquence :
$$(\star) \qquad \mathrm{Card}\,(G) = \sum_{i=1}^{p} \mathrm{Card}\left(\overline{x_i}\right).$$

- Soit $i \in [\![1,p]\!]$. Démontrons $\mathrm{Card}\left(\overline{x_i}\right) = \mathrm{Card}\,(H)$, ce qui grâce à l'identité $(\star)$ nous permettra de conclure. L'application :
$$\varphi \left| \begin{array}{ccc} \overline{x_i} & \longrightarrow & H \\ y & \longmapsto & x_i * y^{-1} \end{array} \right. .$$
est bien définie (cf. définition de $\mathscr{R}$). L'application :
$$\psi \left| \begin{array}{ccc} H & \longrightarrow & \overline{x_i} \\ z & \longmapsto & z^{-1} * x_i \end{array} \right.$$
est bien définie. En effet :
$$\begin{array}{rcl} z \in H & \Rightarrow & x_i * x_i^{-1} * z \in H \\ & \Rightarrow & x_i * \left(z^{-1} * x_i\right)^{-1} \in H \\ & \Rightarrow & x_i * \psi(z)^{-1} \in H \\ & \Rightarrow & x_i \mathscr{R} \psi(z) \\ & \Rightarrow & \psi(z) \in \overline{x_i}. \end{array}$$
On vérifie de plus que $\psi \circ \varphi = \mathrm{id}_{\overline{x_i}}$ et $\varphi \circ \psi = \mathrm{id}_H$. Donc φ est une bijection (idem pour ψ). Ainsi $\overline{x_i}$ et H ont le même cardinal.

■

Exemple 75. — Nous donnons deux applications élémentaires du théorème de Lagrange sur les groupes finis.

1. Soit G un groupe de cardinal 17, dont le neutre est noté e. Alors G ne possède aucun sous-groupe autre que $\{e\}$ et G. Il en est de même pour tout groupe fini de cardinal premier.
2. Un groupe fini de cardinal 32 ne possède aucun sous-groupe de cardinal 5.

■

§ 10. ORDRE D'UN ÉLÉMENT

DÉFINITION 76 (ORDRE D'UN ÉLÉMENT). — *Soient $(G,*)$ un groupe, de neutre noté e, et $x \in G$.*

1. *On dit que x est d'ordre fini si :*
$$\exists\, n \in \mathbf{N}^*, \quad x^n = e.$$
2. *Si x est d'ordre fini, on appelle ordre de x et on note $\mathrm{ord}\,(x)$ le plus petit $n \in \mathbf{N}^*$ tel que $x^n = e$, i.e. :*
$$\mathrm{ord}\,(x) := \min\left\{n \in \mathbf{N}^* \ : \ x^n = e\right\}.$$

PROPOSITION 77 (CS POUR QUE TOUS LES ÉLÉMENTS D'UN GROUPE AIENT UN ORDRE FINI). — *Dans un groupe fini, tout élément est d'ordre fini.*

Remarque 78 (la CS de la proposition n'est pas une CN). — On vérifie que :
$$\mathbb{U}_\infty := \bigcup_{n=1}^{+\infty} \mathbb{U}_n$$
est un sous-groupe de $(\mathbf{C}^*, \times)$. Ainsi, $\mathbb{U}_\infty$ est-il naturellement muni d'une structure de groupe multiplicatif. Tous les éléments du groupe $(\mathbb{U}_\infty, \times)$ sont d'ordre fini, mais l'ensemble $\mathbb{U}_\infty$ est infini. ■

Exemple 79 (éléments d'ordres finis et ordres d'iceux). —

1. Dans le groupe $(\mathbf{Z}, +)$, le seul élément d'ordre fini est 0.
2. Dans le groupe $(\{-1,1\}, \times)$, 1 est d'ordre 1 et -1 est d'ordre 2.
3. Soit un entier $n \geqslant 2$. L'élément $e^{i\frac{2\pi}{n}}$ est d'ordre n dans le groupe $(\mathbb{U}_n, \times)$.
4. Soient un entier $n \geqslant 2$ et $p \in [\![2,n]\!]$. Dans le groupe $(S_n, \circ)$, tout p-cycle est d'ordre p.

■

EXERCICE 80. — Soit E un $\mathbf{R}$-espace vectoriel non réduit à $\{0_E\}$. Que dire d'un élément d'ordre 2 du groupe $(\mathrm{GL}(E), \circ)$? On s'efforcera d'être aussi exhaustif que possible. □

PROPOSITION 81 (PROPRIÉTÉ DE DIVISIBILITÉ DE L'ORDRE D'UN ÉLÉMENT). — *Soient $(G,*)$ un groupe dont le neutre est noté e et x un élément de G d'ordre fini.*
$$\forall\, n \in \mathbf{Z}, \quad x^n = e \iff \mathrm{ord}\,(x) \mid n.$$

DÉMONSTRATION. — Nous posons $d := \mathrm{ord}\,(x)$.
$\Longrightarrow$ Soit $n \in \mathbf{Z}$ tel que $x^n = e$. Écrivons la division euclidienne de n par d :
$$n = q \cdot d + r$$

où $q \in \mathbf{Z}$ et $r \in [\![0, d-1]\!]$. Alors :

$$e = x^n = x^{q\cdot d+r} = \left(x^d\right)^q * x^r = e^q * x^r = x^r.$$

Si $r \neq 0$, alors r vérifie $1 \leqslant r \leqslant d-1$ et $x^r = e$, ce qui contredit la minimalité de d. Donc $r = 0$ et d divise n.
$\Longleftarrow$ Soit $n \in \mathbf{Z}$ tel que d divise n. Alors il existe $q \in \mathbf{Z}$ tel que $n = q \cdot d$. Donc :

$$x^n = x^{q\cdot d} = \left(x^d\right)^q = e^q = e.$$

■

PROPOSITION 82 (CARDINAL DU SOUS-GROUPE ENGENDRÉ PAR UN ÉLÉMENT D'ORDRE FINI). — *Soient $(G,*)$ un groupe et x un élément de G d'ordre fini. Alors le sous-groupe $< x >$ est fini et :*

$$\mathrm{Card}\,(< x >) = \mathrm{ord}\,(x).$$

ÉLÉMENTS DE DÉMONSTRATION. — Nous posons $d := \mathrm{ord}\,(x)$ et nous vérifions que l'application :

$$f \left| \begin{array}{ccc} [\![0,d-1]\!] & \longrightarrow & \mathrm{Card}\,(< x >) \\ k & \longmapsto & x^k \end{array} \right.$$

est bijective. □

THÉORÈME 83 (ORDRE D'UN ÉLÉMENT DANS UN GROUPE FINI). — *Soient $(G,*)$ un groupe fini et $x \in G$. Alors x est d'ordre fini et*

$$\mathrm{ord}\,(x) \mid \mathrm{Card}\,(G).$$

DÉMONSTRATION. — Il s'agit d'une conséquence de la précédente proposition et du théorème de Lagrange. ■

EXERCICE 84 (SOUS-GROUPES D'UN GROUPE CYCLIQUE). — Soient $(G,*)$ un groupe cyclique de cardinal noté n et d un diviseur positif de n.

1. Démontrer que G possède un sous-groupe de cardinal d.
2. Soit H un sous-groupe de cardinal d. Démontrer que :

$$H = \left\{x \in G \,:\, x^d = e_G\right\}.$$

Nous en déduisons que, pour tout diviseur positif d de n, il existe un unique sous-groupe de $(G,*)$ de cardinal d. □

EXERCICE 85. — Soient un entier $n \geqslant 2$ et $\sigma \in S_n$. Considérons « la » décomposition de σ en produit de cycles à supports disjoints :

$$\sigma = c_1 \circ \ldots \circ c_r$$

et notons $\ell_1, \ldots, \ell_r$ les longueurs respectives des cycles $c_1, \ldots, c_r$. Démontrer que l'ordre de σ est le PPCM des longueurs des cycles $\ell_1, \ldots, \ell_r$. □

EXERCICE 86. — Si $(G,*)$ est un groupe et si g_1, g_2 sont deux éléments de G, a-t-on nécessairement :

$$\mathrm{ord}\left(g_1 * g_2\right) = \mathrm{ord}\left(g_1\right) \vee \mathrm{ord}\left(g_2\right) \ ?$$

□

EXERCICE 87. — Si $(G,*)$ un groupe tel que, pour tout $g \in G$, $g^2 = e_G$. Démontrer que le groupe $(G,*)$ est abélien. □

§ 11. RAPPELS SUR LES ANNEAUX

DÉFINITION 88 (ANNEAU). — *Soit A un ensemble non vide muni de deux lois de compositions internes $+$ et $\times$. On dit que $(A,+,\times)$ est un anneau si les quatre propriétés suivantes sont vérifiées.*

(A1) *$(A,+)$ est un groupe commutatif (dont le neutre est noté 0_A) ;*

(A2) *la loi $\times$ est associative, i.e. :*

$$\forall\,(x,y,z) \in A^3, \quad (x \times y) \times z = x \times (y \times z);$$

(A3) *la loi $\times$ possède un élément neutre 1_A, i.e. :*

$$\exists 1_A \in A, \quad \forall\, x \in A, \quad x \times 1_A = x = 1_A \times x;$$

(A4) *La loi $\times$ est distributive par rapport à la loi $+$, i.e. :*

$$\forall (x,y,z) \in A^3, \quad x \times (y+z) = (x \times y) + (x \times z) \quad \text{et} \quad (y+z) \times x = (y \times x) + (z \times x).$$

On dit alors que $(A,+,\times)$ est un anneau. Si de plus la loi $\times$ est commutative, i.e. :

$$\forall\,(x,y) \in A^2, \quad x \times y = y \times x$$

on dit que $(A,+,\times)$ est un anneau commutatif.

Remarque 89 (conséquence de la définition d'anneau). — Soit $(A,+,\times)$ un anneau.

1. Il existe un seul élément 1_A vérifiant la propriété (A3) de la définition précédente. On l'appelle élément unité de l'anneau $(A,+,\times)$.
2. L'élément 0_A est absorbant, i.e. :
$$\forall x \in A, \quad x \times 0_A = 0_A \times x = 0_A .$$
3. Soit $x \in A$. Le symétrique de x pour la loi de groupe $+$ est noté $-x$ et est appelé opposé de x.
4. Pour tout $x \in A$, $(-1_A) \times x = -x$.

■

Exemple 90 (anneaux). —

1. Les ensembles de nombres livrent les anneaux commutatifs suivants.
$$(\mathbf{Z},+,\times) \qquad (\mathbb{Q},+,\times) \qquad (\mathbf{R},+,\times) \qquad (\mathbf{C},+,\times)$$
2. Si E est un $\mathbf{R}$-espace vectoriel alors $(\mathscr{L}(E),+,\circ)$ est un anneau, qui est non commutatif si E n'est pas de dimension 0 ou 1. Son élément neutre pour la multiplication $\circ$ est id_E.
3. Si n est un entier tel que $n \geqslant 2$, alors $(\mathscr{M}_n(\mathbf{K}),+,\times)$ est un anneau non commutatif. Son élément neutre pour la multiplication $\times$ est la matrice I_n.
4. Si $\mathbf{K}$ est un corps (i.e. un anneau dans lequel tout élément non nul est inversible pour la multiplication), alors $(\mathbf{K}[X],+,\times)$ est un anneau commutatif. Son élément neutre est le polynôme constant 1.

■

PROPOSITION 91 (PRODUIT D'UN NOMBRE FINI D'ANNEAUX). — *Soient un entier $n \geqslant 2$ et $(A_1,+_1,\times_1),\dots,(A_n,+_n,\times_n)$ des anneaux. On définit deux opérations sur*
$$\prod_{k=1}^{n} A_k = \{(a_1,\dots,a_n) : a_1 \in A_1,\dots,a_n \in A_n\}$$
en posant :
$$+ \left| \begin{array}{ccc} \left(\prod_{k=1}^{n} A_k\right) \times \left(\prod_{k=1}^{n} A_k\right) & \longrightarrow & \prod_{k=1}^{n} A_k \\ ((a_1,\dots,a_n),(b_1,\dots,b_n)) & \longmapsto & (a_1 +_1 b_1,\dots,a_n +_n b_n) \end{array} \right. \quad \text{et} \quad \times \left| \begin{array}{ccc} \left(\prod_{k=1}^{n} A_k\right) \times \left(\prod_{k=1}^{n} A_k\right) & \longrightarrow & \prod_{k=1}^{n} A_k \\ ((a_1,\dots,a_n),(b_1,\dots,b_n)) & \longmapsto & (a_1 \times_1 b_1,\dots,a_n \times_n b_n) \end{array} \right. .$$
Alors $\left(\prod_{k=1}^{n} A_k,+,\times\right)$ est un anneau. Son neutre pour la loi $+$ est $(0_{A_1},\dots,0_{A_n})$ et son neutre pour la loi $\times$ est $(1_{A_1},\dots,1_{A_n})$.

ÉLÉMENTS DE DÉMONSTRATION. —
- On vérifie que le neutre de $\prod_{k=1}^{n} A_k$ pour la loi $+$ est $(0_{A_1},\dots,0_{A_n})$.
- On vérifie que l'élément $(a_1,\dots,a_n) \in \prod_{k=1}^{n} A_k$ a pour opposé $(-a_1,\dots,-a_n)$.
- On vérifie que le neutre de $A_1 \times \dots \times A_p$ pour la loi $\times$ est $(1_{A_1},\dots,1_{A_n})$.
- Enfin, l'associativité de $+$, l'associativité de $\times$ et la distributivité de $+$ par rapport à $\times$ résulte essentiellement des propriétés correspondantes pour les lois $+_1,\times_1,\dots,+_n,\times_n$. □

Rappel 92 (anneau commutatif intègre). — Un anneau commutatif $(A,+,\times)$ est intègre si les deux propriétés suivantes sont vérifiées.

1. $A \neq \{0_A\}$
2. $\forall (a,b) \in A^2, \quad a \times b = 0_A \implies (a = 0_A \text{ ou } b = 0_A)$.

■

EXERCICE 93. — Soient $(A_1,+_1,\times_1)$ et $(A_2,+_2,\times_2)$ deux anneaux commutatifs intègres. L'anneau produit $A_1 \times A_2$ est-il intègre ? □

§ 12. RAPPELS SUR LES SOUS-ANNEAUX

DÉFINITION 94 (SOUS-ANNEAU). — *Soit $(A,+,\times)$ un anneau. Une partie B de A est appelée sous-anneau de $(A,+,\times)$ si les propriétés suivantes sont vérifiées.*

(A1) *B contient 0_A et 1_A, i.e. $0_A \in B$ et $1_A \in B$;*

(A2) *B est stable pour les lois $+$ et $\times$:*
$$\forall (x,y) \in B^2, \quad x+y \in B \quad \text{et} \quad x \times y \in B ;$$

(A3) *B est stable par passage à l'opposé, i.e.*
$$\forall x \in B, \quad -x \in B .$$

PROPOSITION 95 (STRUCTURE NATURELLE D'ANNEAU SUR UN SOUS-ANNEAU). — *Soit $(A,+,\times)$ un anneau et soit B un sous-anneau de $(A,+,\times)$. Alors les applications induites :*

$$+_B \left| \begin{array}{ccc} B^2 & \longrightarrow & B \\ (x,y) & \longmapsto & x+y \end{array} \right. \qquad \times_B \left| \begin{array}{ccc} B^2 & \longrightarrow & B \\ (x,y) & \longmapsto & x\times y \end{array} \right.$$

sont biens définies et $\left(B,+_B,\times_B\right)$ est un anneau.

PROPOSITION 96 (CRITÈRE POUR ÊTRE UN SOUS-ANNEAU). — *Soit $(A,+,\times)$ un anneau. Une partie B de A est un sous-anneau de $(A,+,\times)$ si et seulement si les propriétés suivantes sont vérifiées.*

1. *B contient 1_A, i.e. $1_A \in B$.*
2. *B est stable par somme tordue, i.e.*
$$\forall (x,y)\in B^2,\quad x-y\in B\,.$$
3. *B est stable pour la loi $\times$, i.e.*
$$\forall (x,y)\in B^2,\quad x\times y\in B\,.$$

EXERCICE 97. — Soient un entier $\geqslant 2$ et $\zeta := e^{i\frac{2\pi}{n}}$. On définit l'ensemble $\mathbf{Z}[\zeta]$ par :

$$\mathbf{Z}[\zeta] := \left\{ \sum_{k=0}^{n-1} a_k \zeta^k \,:\, (a_0,a_1,\dots,a_{n-1})\in\mathbf{Z}^n \right\}.$$

Démontrer que $\mathbf{Z}[\zeta]$ est un sous-anneau de $(\mathbf{C},+,\times)$. □

§ 13. RAPPELS SUR LES MORPHISMES D'ANNEAUX

DÉFINITION 98 (MORPHISME D'ANNEAUX). — *Soient $\left(A,+_A,\times_A\right)$ et $\left(B,+_B,\times_B\right)$ deux anneaux. Une application $f\colon \left(A,+_A,\times_A\right)\longrightarrow \left(B,+_B,\times_B\right)$ est un morphisme d'anneaux si :*

1. *f respecte les unités, i.e. :*
$$f\left(1_A\right)=1_B\,;$$
2. *f respecte les additions, i.e. :*
$$\forall (x,y)\in A^2,\quad f\left(x+_A y\right)=f(x)+_B f(y)\,;$$
3. *f respecte les multiplications, i.e.*
$$\forall (x,y)\in A^2,\quad f\left(x\times_A y\right)=f(x)\times_B f(y)\,.$$

Exemple 99 (morphisme d'anneaux de $(\mathbf{Z},+,\times)$ dans lui-même). — L'identité $\mathrm{id}_{\mathbf{Z}}$ est l'unique morphisme d'anneaux de $(\mathbf{Z},+,\times)$ dans $(\mathbf{Z},+,\times)$. ■

Exemple 100 (morphisme d'anneaux fondamental de la réduction). — Soient $n\in\mathbf{N}^*$ et $M\in\mathscr{M}_n(\mathbf{R})$. L'application :

$$\mathrm{eval}_M \left| \begin{array}{ccc} (\mathbf{K}[X],+,\circ) & \longrightarrow & (\mathscr{M}_n(\mathbf{R}),+,\times) \\ P=\sum_{k=0}^{+\infty} a_k\cdot X^k & \longmapsto & P(M):=\sum_{k=0}^{+\infty} a_k\cdot M^k \end{array} \right.$$

est un morphisme d'anneaux. ■

EXERCICE 101. — L'application transposée :

$$f \left| \begin{array}{ccc} (\mathscr{M}_n(\mathbf{R}),+,\times) & \longrightarrow & (\mathscr{M}_n(\mathbf{R}),+,\times) \\ M & \longmapsto & M^\top \end{array} \right.$$

est-elle un automorphisme d'anneau? □

PROPOSITION 102 (COMPOSITION DE MORPHISMES D'ANNEAUX). — *Soient $(A_1,+_1,\times_1)$, $(A_2,+_2,\times_2)$, $(A_3,+_3,\times_3)$ trois anneaux et*

$$f\colon (A_1,+_1,\times_1)\longrightarrow(A_2,+_2,\times_2) \qquad g\colon (A_2,+_2,\times_2)\longrightarrow(A_3,+_3,\times_3)$$

deux morphismes d'anneaux. Alors l'application :

$$g\circ f \left| \begin{array}{ccc} (A_1,+_1,\times_1) & \longrightarrow & (A_3,+_3,\times_3) \\ x_1 & \longmapsto & g(f(x_1)) \end{array} \right.$$

est un morphisme d'anneaux.

DÉFINITION 103 (ISOMORPHISME D'ANNEAUX). — *Un morphisme d'anneaux qui est bijectif est appelé isomorphisme d'anneaux.*

Exemple 104 (isomorphisme d'anneaux fondamental de l'algèbre linéaire). — Soient E un $\mathbf{R}$-espace vectoriel de dimension finie $n \geqslant 2$, muni d'une base $\mathscr{B}$. L'application :

$$\mathrm{Mat}_{\mathscr{B}}(\cdot) \left| \begin{array}{ccc} (\mathscr{L}(E),+,\circ) & \longrightarrow & (\mathscr{M}_n(\mathbf{R}),+,\times) \\ f & \longmapsto & \mathrm{Mat}_{\mathscr{B}}(f) \end{array} \right.$$

est un isomorphisme d'anneaux. ■

PROPOSITION 105 (INVERSE D'UN ISOMORPHISME D'ANNEAUX). — *Soient $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ deux anneaux et $f : A \longrightarrow B$ un isomorphisme d'anneaux. Alors la bijection réciproque :*

$$f^{-1} \left| \begin{array}{ccc} (B,+_B,\times_B) & \longrightarrow & (A,+_A,\times_A) \\ b & \longmapsto & \text{l'unique élément } a \text{ de } A \text{ tel que } f(a)=b \end{array} \right.$$

est un isomorphisme d'anneaux.

DÉMONSTRATION. — • Notons 1_A et 1_B les éléments unités respectifs des anneaux $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$. En appliquant f^{-1} à chaque membre de l'égalité $f(1_A)=1_B$, il vient $1_A = f^{-1}(1_B)$.
• Soit $(y_1,y_2)\in B^2$.

$$f^{-1}(y_1+_B y_2) = f^{-1}\left(f(f^{-1}(y_1))+_B f(f^{-1}(y_2))\right) \underset{(\star)}{=} f^{-1}\left(f(f^{-1}(y_1)+_A f^{-1}(y_2))\right) = f^{-1}(y_1)+_A f^{-1}(y_2)$$

où $(\star)$ provient du fait que f est un morphisme d'anneaux.
• En reprenant le calcul précédent, en échangeant $+$ par $\times$, il vient :

$$f^{-1}(y_1\times_B y_2) = f^{-1}(y_1)\times_A f^{-1}(y_2).$$

■

§ 14. L'ANNEAU $(\mathbf{Z}/n\mathbf{Z},+,\times)$

THÉORÈME 106 (STRUCTURE D'ANNEAU SUR $\mathbf{Z}/n\mathbf{Z}$). — *Soit $n\in\mathbf{N}^*$. Posons :*

$$+ \left| \begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})\times(\mathbf{Z}/n\mathbf{Z}) & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \\ (\overline{a},\overline{b}) & \longmapsto & \overline{a+b} \end{array} \right. \quad \text{et} \quad \times \left| \begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})\times(\mathbf{Z}/n\mathbf{Z}) & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \\ (\overline{a},\overline{b}) & \longmapsto & \overline{a\times b} \end{array} \right. .$$

Les lois $+$ et $\times$ sont bien définies et $(\mathbf{Z}/n\mathbf{Z},+,\times)$ est un anneau commutatif à n éléments. L'élément neutre additif est $\overline{0}$ et l'élément neutre multiplicatif est $\overline{1}$.

Rappel 107 (groupe des inversibles d'un anneau). — Soit $(A,+,\times)$ un anneau.

1. Un élément $x\in A$ est dit inversible si :
$$(\star) \qquad \exists\, y\in A, \quad x\times y = y\times x = 1_A.$$
2. Si $x\in A$ est inversible, alors l'élément y de $(\star)$ est unique. On le nomme inverse de x et on le note x^{-1}.
3. L'élément 1_A de A est inversible et $(1_A)^{-1}=1_A$.
4. Si des éléments x, y de A sont inversibles, alors $x\times y$ est inversible et $(x\times y)^{-1} = y^{-1}\times x^{-1}$.
5. Si l'on note $U(A)$ l'ensemble des éléments inversibles de A, alors l'application notée abusivement $\times$ définie par :
$$\times \left| \begin{array}{ccc} U(A)\times U(A) & \longrightarrow & U(A) \\ (x,y) & \longmapsto & x\times y \end{array} \right.$$
est bien définie et $(U(A),\times)$ est un groupe (non nécessairement abélien), appelé groupe des inversibles de A.

■

EXERCICE 108. — Résoudre l'équation :

$$x^2 + \overline{2}\times x = \overline{0}$$

dans l'anneau $(\mathbf{Z}/5\mathbf{Z},+,\times)$, puis dans l'anneau $(\mathbf{Z}/8\mathbf{Z},+,\times)$, □

THÉORÈME 109 (ÉLÉMENTS INVERSIBLES DE L'ANNEAU $\mathbf{Z}/n\mathbf{Z}$). — *Soit $n\in\mathbf{N}^*$. Alors :*

$$U(\mathbf{Z}/n\mathbf{Z}) = \left\{\overline{a}\in\mathbf{Z}/n\mathbf{Z} \,:\, a\wedge n = 1\right\}.$$

Remarque 110. — Soient $n\in\mathbf{N}^*$ et $a\in\mathbf{Z}$. Alors :

$$\overline{a}\in U(\mathbf{Z}/n\mathbf{Z}) \iff \langle\overline{a}\rangle = \mathbf{Z}/n\mathbf{Z}.$$

■

Rappel 111 (corps). — Un corps est un anneau commutatif $(A,+,\times)$ distinct de $\{0_A\}$ dans lequel tout élément distinct de 0_A est inversible, i.e. $U(A) = A\setminus\{0_A\}$. ■

COROLLAIRE 112 (CRITÈRE POUR QUE L'ANNEAU $\mathbf{Z}/n\mathbf{Z}$ SOIT UN CORPS). — *Soit $n\in\mathbf{N}^*$. Alors :*

$$\text{l'anneau } (\mathbf{Z}/n\mathbf{Z},+,\times) \text{ est un corps} \iff n \text{ est premier.}$$

DÉFINITION 113 (LE CORPS À p ÉLÉMENTS). — *Pour tout nombre premier p, on note $\mathbb{F}_p$ le corps $(\mathbf{Z}/p\mathbf{Z},+,\times)$.*

Remarque 114 (unicité du corps à p éléments). — Soit p un nombre premier et $\mathbf{K}$ un corps à p éléments.
- Le morphisme d'anneaux canonique :

$$f \left| \begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{K} \\ a & \longmapsto & a\,1_{\mathbf{K}} \end{array} \right.$$

est surjectif car son image est un sous-groupe non trivial de $(\mathbf{K},+)$, groupe de cardinal p premier (cf. théorème de Lagrange).
- Le noyau de f est un sous-groupe de $(\mathbf{Z},+)$ non trivial (f est non injective). Il existe donc unique $n\in\mathbf{N}^*$ tel que $\mathrm{Ker}(f) = n\mathbf{Z}$.
- On démontre alors que :

$$g \left| \begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \longrightarrow & \mathbf{K} \\ \overline{a} & \longmapsto & a\,1_{\mathbf{K}} \end{array} \right.$$

est une application bien définie, qui est un isomorphisme d'anneaux. Nous en déduisons $n = p$.
- Nous avons démontré que les corps $\mathbb{F}_p$ et $\mathbf{K}$ sont isomorphes.
- On vérifie sans peine que l'application g est l'unique morphisme de corps entre $\mathbb{F}_p$ et $\mathbf{K}$. Le corps à p éléments $\mathbb{F}_p$ est donc unique à unique isomorphisme près.

■

Remarque 115 (structure du groupe des unités du corps $\mathbb{F}_p$). — Soit p un nombre premier. Comme le $\mathscr{F}_p$ est un corps, le groupe des unités de $\mathbb{F}_p$ est :

$$\left(U\left(\mathbb{F}_p\right),\times\right) = \left(\mathbb{F}_p\setminus\left\{0_{\mathbb{F}_p}\right\},\times\right).$$

On peut démontrer que $\left(\mathbb{F}_p\setminus\left\{0_{\mathbb{F}_p}\right\},\times\right)$ est un groupe cyclique (HP) d'ordre $p-1$, bien qu'il soit « en général » délicat d'en trouver un générateur explicite. ■

EXERCICE 116. — Quels sont les inverses de $\overline{4}$ dans $\mathbf{Z}/5\mathbf{Z}$ et de $\overline{16}$ dans $\mathbf{Z}/17\mathbf{Z}$? □

EXERCICE 117. — Soit $n\in\mathbf{N}^*$.
1. Quels sont les éléments inversibles de $\mathbf{Z}/2^n\mathbf{Z}$?
2. Calculer le cardinal de $U\left(\mathbf{Z}/2^n\mathbf{Z}\right)$.

□

§ 15. THÉORÈME DES RESTES CHINOIS

NOTATION. — Si $d\in\mathbf{N}^*$ et $a\in\mathbf{Z}$, alors on note $\overline{a}^{[d]}$ la classe de a dans $\mathbf{Z}/d\mathbf{Z}$.

THÉORÈME 118 (DES RESTES CHINOIS). — *Soient un entier $r\geqslant 2$ et des entiers $n_1\geqslant 1, n_2\geqslant 1,\dots,n_r\geqslant 1$ deux-à-deux premiers entre eux. Posons $n := n_1\cdot n_2\cdot\ldots\cdot n_r$.*

1. *L'application :*

$$\varphi \left| \begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \longrightarrow & (\mathbf{Z}/n_1\mathbf{Z})\times(\mathbf{Z}/n_2\mathbf{Z})\times\ldots\times(\mathbf{Z}/n_r\mathbf{Z}) \\ \overline{a}^{[n]} & \longmapsto & \left(\overline{a}^{[n_1]},\overline{a}^{[n_2]},\dots,\overline{a}^{[n_r]}\right) \end{array} \right.$$

est bien définie et est un isomorphisme d'anneaux.

2. *Soit $(a_1,a_2,\dots,a_r)\in\mathbf{Z}^r$. Le système de congruences simultanées :*

$$\left\{ \begin{array}{rcll} x & \equiv & a_1 & [n_1] \\ x & \equiv & a_2 & [n_2] \\ & \vdots & & \\ x & \equiv & a_r & [n_r] \end{array} \right.$$

d'inconnue $x\in\mathbf{Z}$ admet une unique solution modulo n, qui est :

$$x = a_1\cdot N_1\cdot y_1 + a_2\cdot N_2\cdot y_2 + \ldots + a_r\cdot N_r\cdot y_r$$

où, pour tout $i\in[\![1,r]\!]$, $N_i := \prod_{\substack{j=1\\ j\neq i}}^{r} n_j$ et y_i est un entier tel que $\overline{y_i}^{[n_i]}$ est l'inverse de $\overline{N_i}^{[n_i]}$ dans $\mathbf{Z}/n_i\mathbf{Z}$.

Remarque 119 (origine du théorème des restes chinois). — L'énoncé suivant figure dans le livre « Sunzi suanjing » (traduction : « classique mathématique de Sunzi ») datant du 3ème siècle.

> *Suppose que l'on ait un nombre inconnu d'objets. S'ils sont comptés par 3, il en reste 2, s'ils sont comptés par 5, il en reste 3 et s'ils sont comptés par 7, il en reste 2. Combien d'objets y a-t-il ?*

■

EXERCICE 120 (CONGRUENCES SIMULTANEES). — Résoudre le système de congruences simultanées :

$$\begin{cases} x & \equiv & 1 & [5] \\ x & \equiv & 2 & [6] \\ x & \equiv & 3 & [7] \end{cases}$$

d'inconnue $x \in \mathbf{Z}$. □

§ 16. THÉORÈME D'EULER

DÉFINITION 121 (INDICATRICE D'EULER). — *L'application :*

$$\varphi \left| \begin{array}{ccc} \mathbf{N}^* & \longrightarrow & \mathbf{N}^* \\ n & \longmapsto & \mathrm{Card}\left(U(\mathbf{Z}/n\mathbf{Z})\right) = \mathrm{Card}\left(\{a \in [\![1,n]\!] \,:\, a \wedge n = 1\}\right) \end{array} \right.$$

est appelée indicatrice d'Euler.

THÉORÈME 122 (EULER). — *Soient $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}$ tel que $a \wedge n = 1$. Alors :*

$$a^{\varphi(n)} \equiv 1 \quad [n].$$

Remarque 123 (petit théorème de Fermat). — Si $n = p$ est un nombre premier, le théorème d'Euler se spécialise en le petit théorème de Fermat :

$$\forall a \in [\![1, p-1]\!], \quad a^{p-1} \equiv 1 \quad [p].$$

■

PROPOSITION 124 (GROUPE DES INVERSIBLES D'UN PRODUIT D'ANNEAUX). — *Soient $(A_1, +_1, \times_1), \ldots, (A_p, +_p, \times_p)$ des anneaux et $\left(\prod_{i=1}^{p} A_i, +, \times\right)$ l'anneau produit. Alors :*

$$U\left(\prod_{i=1}^{p} A_i\right) = U(A_1) \times \ldots \times U(A_p)$$

où $U(?)$ désigne le groupe des éléments inversibles de l'anneau ? pour la multiplication.

THÉORÈME 125 (CALCUL DE L'INDICATRICE D'EULER). — *On note $\mathscr{P}$ l'ensemble des nombres premiers.*

1. $\forall (n,m) \in \mathbf{N}_{\geqslant 2} \times \mathbf{N}_{\geqslant 2}, \quad n \wedge m = 1 \Longrightarrow \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$
2. $\forall p \in \mathscr{P}, \quad \forall k \in \mathbf{N}^*, \quad \varphi\left(p^k\right) = (p-1) \cdot p^{k-1}$
3. *Pour tout $n \in \mathbf{N}_{\geqslant 2}$:*

$$\varphi(n) = n \cdot \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)$$

où $p_1 \in \mathscr{P}, \ldots, p_r \in \mathscr{P}$ sont les diviseurs premiers de n.

EXERCICE 126. — Justifier que $10^6 \equiv 1 \quad [7]$, puis que :

$$\sum_{k=1}^{12} 10^{10^k} \equiv -1 \quad [7].$$

□

EXERCICE 127 (THÉORÈME DE WILSON). — Soit $p \in \mathbf{N}^*$ un entier premier. Démontrer :

$$(p-1)! \equiv -1 \quad [p].$$

□

§ 17. IDÉAUX D'UN ANNEAU COMMUTATIF

DÉFINITION 128 (IDÉAL D'UN ANNEAU COMMUTATIF). — *Soient $(A,+,\times)$ un anneau commutatif et I une partie de A. On dit que I est un idéal de A si :*

1. *I est un sous-groupe de $(A,+)$;*
2. *I est absorbant pour la multiplication par des éléments de A, i.e. :*

$$\forall\, x \in I, \quad \forall\, a \in A, \quad a \times x \in I.$$

Exemple 129 (idéaux triviaux). — Si $(A,+,\times)$ est un anneau commutatif, alors $\{0_A\}$ et A sont des idéaux de A, appelés idéaux triviaux. ■

EXERCICE 130 (IDÉAUX CONTENANT UN INVERSIBLE DE L'ANNEAU). — Soit $(A,+,\times)$ un anneau commutatif.

1. Que dire d'un idéal I de A tel que $1_A \in I$?
2. Que dire d'un idéal I de A qui contient un élément inversible de A ?

□

PROPOSITION 131 (CRITÈRE POUR ÊTRE UN IDÉAL). — *Pour montrer que I est un idéal d'un anneau commutatif $(A,+,\times)$, il suffit de vérifier les trois propriétés suivantes :*

1. *I est non vide ;*
2. *I est stable par addition tordue, i.e. :*

$$\forall\, (x,y) \in I^2, \quad x - y \in I\,;$$

3. *I est absorbant, i.e. :*

$$\forall\, x \in I, \quad \forall\, a \in A, \quad a \times x \in I.$$

Exemple 132 (idéaux). —

1. L'ensemble :
$$I := \left\{ f \in \mathscr{C}^0(\mathbf{R},\mathbf{R}) \,:\, f(1) = 0 \right\}$$
est un idéal de l'anneau $\left(\mathscr{C}^0(\mathbf{R},\mathbf{R}),+,\times\right)$.
2. L'ensemble
$$I := \left\{ (u_n)_{n\in\mathbf{N}} \in \mathbf{R}^{\mathbf{N}} \,:\, \exists N \in \mathbf{N},\, \forall\, n \geqslant N,\, u_n = 0 \right\}$$
est un idéal de $\left(\mathbf{R}^{\mathbf{N}},+,\times\right)$.

■

PROPOSITION 133 (IDÉAUX ET MORPHISMES D'ANNEAUX COMMUTATIFS). — *Soit $f : (A,+_A,\times_A) \longrightarrow (B,+_B,\times_B)$ un morphisme d'anneaux commutatifs. Alors :*

$$\mathrm{Ker}\left(f\right) := \left\{ x \in A \,:\, f(x) = 0_B \right\}$$

est un idéal de A.

EXERCICE 134 (OPERATIONS SUR LES IDÉAUX). — Soit $(A,+,\times)$ un anneau commutatif.

1. Soit $(I_j)_{j\in J}$ une famille d'idéaux de A. Démontrer que leur intersection :
$$\bigcap_{j\in J} I_j := \left\{ x \in A : \forall\, j \in J,\, x \in I_j \right\}$$
est un idéal de A.
2. Soient un entier $r \geqslant 2$ et $I_1, I_2, \ldots, I_r$ des idéaux de A. Démontrer que leur somme :
$$I_1 + I_2 + \ldots + I_r := \left\{ x_1 + x_2 + \ldots + x_r \,:\, (x_1,x_2,\ldots,x_r) \in \prod_{j=1}^{r} I_j \right\}$$
est un idéal de A.
3. Soient I, J deux idéaux de A. Posons :
$$IJ := \bigcup_{n\in\mathbf{N}^*} \left\{ a_1 \times b_1 + \ldots + a_n \times b_n \,:\, (a_1,\ldots,a_n) \in I^n \text{ et } (b_1,\ldots,b_n) \in J^n \right\}.$$
Démontrer que IJ est un idéal de A. A-t-on $IJ = I \cap J$?

□

PROPOSITION 135 (IDÉAL ENGENDRÉ PAR UN ÉLÉMENT). — *Soit $(A,+,\times)$ un anneau et $x \in A$. Alors :*

$$xA := \{x \times a \,:\, a \in A\} \qquad \left[\text{idéal de } A \text{ engendré par } x\right]$$

est un idéal de A.

DÉFINITION 136 (DIVISIBILITÉ DANS UN ANNEAU COMMUTATIF INTÈGRE). — *Soit $(A,+,\times)$ un anneau commutatif intègre. On dit que $x \in A$ divise $y \in A$, et on note $x \mid y$, si :*

$$(\star) \qquad \exists q \in A \text{ tel que } y = x \times q.$$

Si tel est le cas, alors l'élément q de A qui apparaît en $(\star)$ est unique.

PROPOSITION 137 (CARACTÉRISATION DE LA DIVISIBILITÉ EN TERMES D'IDÉAUX). — *Soit $(A,+,\times)$ un anneau commutatif intègre et $(x,y) \in A^2$. Alors :*

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

DÉMONSTRATION. —
$\Longrightarrow$ Supposons $x \mid y$. Alors il existe $q \in A$ tel que $y = x \times q$.
Soit alors $z \in yA$. Il existe $a \in A$ tel que $z = y \times a$, d'où :

$$z = (x \times q) \times a = x \times \big(q \times a\big) \qquad \left[\text{associativité de la multiplication}\right]$$

donc $z \in xA$. D'où $yA \subset xA$.
$\Longleftarrow$ Supposons $yA \subset xA$. Comme $y = y \times 1_A \in yA$, $y \in xA$. Donc il existe $q \in A$ tel que $y = x \times q$, donc $x \mid y$.

■

§ 18. IDÉAUX DE Z

LEMME 138 (SOUS-GROUPES ADDITIFS DE Z VERSUS IDÉAUX DE Z). — *Soit I une partie de $\mathbf{Z}$. Alors :*

$$I \text{ est un sous-groupe de } (\mathbf{Z},+) \iff I \text{ est un idéal de } (\mathbf{Z},+,\times).$$

THÉORÈME 139 (DESCRIPTION DES IDÉAUX DE Z). —

1. *Soit $a \in \mathbf{Z}$. L'ensemble :*
$$a\mathbf{Z} := \{an \,:\, n \in \mathbf{Z}\}$$
des multiples de a est un idéal de $\mathbf{Z}$.
2. *Soit I un idéal de l'anneau $\mathbf{Z}$. Alors il existe un unique $a \in \mathbf{N}$, appelé <u>générateur de I</u>, tel que $I = a\mathbf{Z}$.*

PROPOSITION 140 (IDÉAUX DE Z ET PGCD). — *Soient un entier $r \geqslant 2$ et $(a_1,a_2,\dots,a_r) \in \left(\mathbf{Z}^*\right)^r$. Alors :*

$$a_1\mathbf{Z} + a_2\mathbf{Z} + \dots + a_r\mathbf{Z} := \left\{a_1n_1 + a_2n_2 + \dots + a_rn_r \,:\, (a_1,a_2,\dots,a_r) \in \mathbf{Z}^r\right\}$$

est un idéal. Son générateur est le PCGD des entiers $a_1,a_2,\dots,a_r$, i.e. :

$$a_1\mathbf{Z} + a_2\mathbf{Z} + \dots + a_r\mathbf{Z} = (a_1 \wedge a_2 \wedge \dots \wedge a_r)\mathbf{Z}$$

COROLLAIRE 141 (RELATION DE BÉZOUT POUR LE PGCD DE $r \geqslant 2$ ÉLÉMENTS DE Z). — *Soient un entier $r \geqslant 2$ et $(a_1,a_2,\dots,a_r) \in \left(\mathbf{Z}^*\right)^r$. Alors :*

$$\exists (n_1,n_2,\dots,n_r) \in \mathbf{Z}^r, \quad a_1 \wedge a_2 \wedge \dots \wedge a_r = a_1n_1 + a_2n_2 + \dots + a_rn_r.$$

EXERCICE 142 (IDÉAUX DE Z ET PPCM). — Soient un entier $r \geqslant 2$ et $(a_1,a_2,\dots,a_r) \in \left(\mathbf{Z}^*\right)^r$. Démontrer que $\bigcap_{i=1}^{r} a_i\mathbf{Z}$ est un idéal de $\mathbf{Z}$ et que son générateur est le PPCM $a_1 \wedge a_2 \wedge \dots \wedge a_r$ des entiers $a_1,a_2,\dots,a_r$. □

§ 19. IDÉAUX DE $\mathbf{K}[X]$

NOTATION. — Dans cette partie, la lettre $\mathbf{K}$ désigne un corps.

THÉORÈME 143 (DESCRIPTION DES IDÉAUX D'UN ANNEAU DE POLYNÔMES EN UNE INDÉTERMINÉE). —

1. *Soit $A \in \mathbf{K}[X]$. L'ensemble :*
$$A\mathbf{K}[X] := \{AP \,:\, P \in \mathbf{K}[X]\}$$
des multiples de A est un idéal de $\mathbf{K}[X]$.
2. *Soit I un idéal de $\mathbf{K}[X]$ distinct de $\{0_{\mathbf{K}[X]}\}$. Alors il existe un unique polynôme unitaire $A \in \mathbf{K}[X]$, appelé générateur de I, tel que $I = A\mathbf{K}[X]$.*

PROPOSITION 144 (IDÉAUX D'UN ANNEAU DE POLYNÔMES EN UNE INDÉTERMINÉE ET PGCD). — *Soient un entier $r \geqslant 2$ et $(A_1, A_2, \dots, A_r) \in \left(\mathbf{K}[X] \setminus \{0_{\mathbf{K}[X]}\}\right)^r$. Alors :*
$$A_1\mathbf{K}[X] + A_2\mathbf{K}[X] + \dots + A_r\mathbf{K}[X] := \left\{A_1P_1 + A_2P_2 + \dots + A_rP_r \,:\, (A_1, A_2, \dots, A_r) \in \mathbf{K}[X]^r\right\}$$
est un idéal. Son générateur est le PCGD des polynômes $A_1, A_2, \dots, A_r$, i.e. :
$$A_1\mathbf{K}[X] + A_2\mathbf{K}[X] + \dots + A_r\mathbf{K}[X] = (A_1 \wedge A_2 \wedge \dots \wedge A_r)\mathbf{K}[X]$$

COROLLAIRE 145 (RELATION DE BÉZOUT POUR LE PGCD DE $r \geqslant 2$ ÉLÉMENTS D'UN ANNEAU DE POLYNÔMES EN UNE INDÉTERMINÉE). — *Soient un entier $r \geqslant 2$ et $(A_1, A_2, \dots, A_r) \in (\mathbf{K}[X])^r$. Alors :*
$$\exists (A_1, A_2, \dots, A_r) \in \mathbf{K}[X]^r, \quad A_1 \wedge A_2 \wedge \dots \wedge A_r = A_1P_1 + A_2P_2 + \dots + A_rP_r.$$

EXERCICE 146 (IDÉAUX D'UN ANNEAU DE POLYNÔMES EN UNE INDÉTERMINÉE ET PPCM). — Soient un entier $r \geqslant 2$ et $(A_1, A_2, \dots, A_r) \in (\mathbf{K}[X])^r$. Démontrer que $\bigcap_{i=1}^{r} A_i\mathbf{K}[X]$ est un idéal de $\mathbf{K}[X]$ et que son générateur est le PPCM $P_1 \wedge P_2 \wedge \dots \wedge P_r$ des polynômes $A_1, A_2, \dots, A_r$. □

EXERCICE 147 (SOUS-CORPS ENGENDRÉ DE C PAR UN NOMBRE ALGÉBRIQUE). — Soit α un nombre complexe. On suppose que α est algébrique sur $\mathbf{Q}$, i.e. qu'il existe $P \in \mathbf{Q}[X] \setminus \{0\}$ tel que $P(\alpha) = 0$.

1. Démontrer que :
$$\mathrm{Ann}(\alpha) := \{A \in \mathbf{Q}[X] \,:\, A(\alpha) = 0\}$$
est un idéal de $\mathbf{Q}[X]$.
2. Démontrer que :
$$\mathbf{Q}[\alpha] := \mathrm{Vect}_{\mathbf{Q}}\left(\left(\alpha^k\right)_{k \in \mathbf{N}}\right)$$
est un $\mathbf{Q}$-espace vectoriel de dimension finie, qui est un sous-corps de $\mathbf{C}$.

□

§ 20. ALGÈBRES

NOTATION. — Dans toute la suite du document, la lettre $\mathbf{K}$ désigne un corps.

DÉFINITION 148 ($\mathbf{K}$-ALGÈBRE). — *Soit A un ensemble muni :*

- *d'une loi de composition notée $+_A$:*
$$+_A \left| \begin{array}{ccc} A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & x +_A y \end{array} \right.$$
- *d'une loi de composition notée $\times$:*
$$\times_A \left| \begin{array}{ccc} A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & x \times_A y \end{array} \right.$$
- *d'une loi de composition externe à domaine d'opérateurs dans $\mathbf{K}$:*
$$\cdot \left| \begin{array}{ccc} \mathbf{K} \times A & \longrightarrow & A \\ (\lambda, x) & \longmapsto & \lambda \cdot x \end{array} \right.$$

On dit que $(A, +_A, \times_A, .)$ est une $\mathbf{K}$-algèbre si les propriétés suivantes sont vérifiées.

(A1) *$(A, +_A, \cdot)$ est un $\mathbf{K}$-espace vectoriel ;*

(A2) *$(A, +_A, \times_A)$ est un anneau ;*

(A3) *les trois opérations $\times_A$, . et $\times_{\mathbf{K}}$ vérifient la propriété de compatibilité suivante.*
$$\forall (\lambda, \mu, x, y) \in \mathbf{K} \times \mathbf{K} \times A \times A, \quad (\lambda \cdot x) \times_A (\mu \cdot y) = (\lambda \times_{\mathbf{K}} \mu) \cdot (x \times_A y).$$

***Exemple 149 (algèbres).* —**

1. Le corps $\mathbf{K}$ est naturellement une $\mathbf{K}$-algèbre. En effet, $(\mathbf{K}, +_{\mathbf{K}}, \times_{\mathbf{K}}, \times_{\mathbf{K}})$ est une $\mathbf{K}$-algèbre.
2. Soit un entier $n \geqslant 2$. Soit $n \in \mathbf{N}_{\geqslant 2}$. Sur $\mathscr{M}_n(\mathbf{K})$, nous disposons d'une addition et d'une multiplications internes et nous avons déjà observé que $(\mathscr{M}_n(\mathbf{K}), +, \times)$ est un anneau. Si l'on définit l'opération $\cdot$ par :
$$\cdot \left| \begin{array}{ccc} \mathbf{K} \times \mathscr{M}_n(\mathbf{K}) & \longrightarrow & \mathscr{M}_n(\mathbf{K}) \\ (\lambda, M) & \longmapsto & \lambda \cdot M := \left(\lambda \times_{\mathbf{K}} [M]_{i,j}\right)_{1 \leqslant i,j \leqslant n} \end{array} \right.$$
alors$(\mathscr{M}_n(\mathbf{K}), +, \cdot)$ est un $\mathbf{K}$-espace vectoriel, de dimension finie n^2. On vérifie que $(\mathscr{M}_n(\mathbf{K}), +, \times, \cdot)$ est une $\mathbf{K}$-algèbre.
3. Soit E un $\mathbf{K}$ espace vectoriel. Sur $\mathscr{L}(E)$, muni de nous disposons d'une addition et d'une multiplications internes et nous avons déjà observé que $(\mathscr{L}(E), +, \circ)$ est un anneau. Si l'on définit l'opération $\cdot$ par :
$$\cdot \left| \begin{array}{ccc} \mathbf{K} \times \mathscr{L}(E) & \longrightarrow & \mathscr{L}(E) \\ (\lambda, f) & \longmapsto & \lambda \cdot f \left| \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & \lambda \cdot f(x) \end{array} \right. \end{array} \right.$$
alors $(\mathscr{L}(E), +, \cdot)$ est un $\mathbf{K}$-espace vectoriel. On vérifie que $(\mathscr{L}(E), +, \circ, \cdot)$ est une $\mathbf{K}$-algèbre.
Sur $\mathbf{K}[X]$, muni de nous disposons d'une addition et d'une multiplications internes et nous avons déjà observé que $(\mathbf{K}[X], +, \times)$ est un anneau. Si l'on définit l'opération $\cdot$ par :
$$\cdot \left| \begin{array}{ccc} \mathbf{K} \times \mathbf{K}[X] & \longrightarrow & \mathbf{K}[X] \\ (\lambda, P) & \longmapsto & \lambda \cdot P := \displaystyle\sum_{k=0}^{+\infty} \lambda \times_{\mathbf{K}} [P]_k X^k \end{array} \right.$$
alors $(\mathbf{K}[X], +, \cdot)$ est un $\mathbf{K}$-espace vectoriel. On vérifie que $(\mathbf{K}[X], +, \times, \cdot)$ est une $\mathbf{K}$-algèbre.

■

EXERCICE 150. — Soit X un ensemble non vide. On note $\mathscr{F}(X, \mathbf{K})$ l'ensemble des applications de X dans $\mathbf{K}$. Munir $\mathscr{F}(X, \mathbf{K})$ d'une structure de $\mathbf{K}$-algèbre naturelle. □

§ 21. SOUS-ALGÈBRES

DÉFINITION 151 (SOUS-ALGÈBRE). — *Soit $\mathbf{K}$ un corps et soit $(A, +, \times, \cdot)$ une $\mathbf{K}$-algèbre. Une partie B de A est appelée sous-$\mathbf{K}$-algèbre de $(A, +, \times, \cdot)$ si B est à la fois un sous-$\mathbf{K}$-espace vectoriel de $(A, +, \cdot)$ et un sous-anneau de $(A, +, \times)$.*

EXERCICE 152. — Soit un entier $n \geqslant 2$. On note $\mathscr{T}_n(\mathbf{K})$ l'ensemble des matrices triangulaires supérieures de $\mathscr{M}_n(\mathbf{K})$. Démontrer que $\mathscr{T}_n(\mathbf{K})$ est une sous-algèbre de $\mathscr{M}_n(\mathbf{K})$. □

EXERCICE 153. — Soit x un nombre réel. Démontrer que $\mathrm{Vect}_{\mathbf{Q}}\left(\left(x^n\right)_{n \in \mathbf{N}}\right)$ est une sous-$\mathbf{Q}$-algèbre de $\mathbf{R}$. □

PROPOSITION 154 (STRUCTURE NATURELLE D'ALGÈBRE SUR UNE SOUS-ALGÈBRE). — *Soit $(A, +, \times, \cdot)$ une $\mathbf{K}$-algèbre et soit B une sous-$\mathbf{K}$-algèbre de $(A, +, \times, \cdot)$. Alors les applications induites :*
$$+_B \left| \begin{array}{ccc} B & \longrightarrow & B \\ (x, y) & \longmapsto & x + y \end{array} \right. \qquad \times_B \left| \begin{array}{ccc} B^2 & \longrightarrow & B \\ (x, y) & \longmapsto & x \times y \end{array} \right. \qquad \cdot_B \left| \begin{array}{ccc} \mathbf{K} \times B & \longrightarrow & B \\ (\lambda, x) & \longmapsto & \lambda \cdot x \end{array} \right.$$
sont biens définies et $\left(B, +_B, \times_B, \cdot_B\right)$ est une $\mathbf{K}$-algèbre.

§ 22. MORPHISME D'ALGÈBRES

DÉFINITION 155 (MORPHISMES D'ALGÈBRES). — *Soient $(A_1, +_1, \times_1, \cdot_1)$ et $(A_2, +_2, \times_2, \cdot_2)$ deux $\mathbf{K}$-algèbres. Une application $f : (A_1, +_1, \times_1, \cdot_1) \longrightarrow (A_2, +_2, \times_2, \cdot_2)$ est appelé morphisme de $\mathbf{K}$-algèbres si les deux propriétés suivantes sont vérifiées.*

1. *f est une application $\mathbf{K}$-linéaire de $(A_1, +_1, \cdot_2)$ vers $(A_2, +_2, \cdot_2)$.*
2. *f est un morphisme d'anneaux de $(A_1, +_1, \times_1)$ et $(A_2, +_2, \times_2)$.*

***Exemple 156 (morphisme d'algèbres fondamental de la réduction).* —** Soient $n \in \mathbf{N}_{\geqslant 2}$ et $M \in \mathscr{M}_n(\mathbf{R})$. On considère de nouveau l'application :
$$\varphi \left| \begin{array}{ccc} (\mathbf{K}[X], +, \circ, \cdot) & \longrightarrow & (\mathscr{M}_n(\mathbf{R}), +, \times, \cdot) \\ P = \displaystyle\sum_{k=0}^{+\infty} a_k X^k & \longmapsto & P(M) := \displaystyle\sum_{k=0}^{+\infty} a_k M^k \end{array} \right.$$
L'application φ est un morphisme de $\mathbf{R}$-algèbres. ■

PROPOSITION 157 (COMPOSITION DE MORPHISMES D'ALGÈBRES). — *Soient* $(A_1,+_1,\times_1,\cdot_1)$, $(A_2,+_2,\times_2,\cdot_2)$, $(A_3,+_3,\times_3,\cdot_3)$ *trois* **K***-algèbres et*

$$f\colon (A_1,+_1,\times_1,\cdot_1)\longrightarrow(A_2,+_2,\times_2,\cdot_2) \qquad g\colon (A_2,+_2,\times_2,\cdot_2)\longrightarrow(A_3,+_3,\times_3,\cdot_3)$$

deux morphismes de **K***-algèbres. Alors l'application :*

$$g\circ f \left|\begin{array}{ccc}(A_1,+_1,\times_1,\cdot_1) & \longrightarrow & (A_3,+_3,\times_3,\cdot_3)\\ x_1 & \longmapsto & g(f(x_1))\end{array}\right.$$

est un morphisme de **K***-algèbres.*

DÉFINITION 158 (ISOMORPHISME DE K-ALGÈBRES). — *Un morphisme de* **K***-algèbre qui est bijectif est appelé isomorphisme de* **K***-algèbres.*

Exemple 159 (isomorphisme d'algèbres fondamental de l'algèbre linéaire). — Soit E un $\mathbf{R}$-espace vectoriel de dimension finie $n\geqslant 2$, muni d'une base $\mathscr{B}$. On considère de nouveau l'application :

$$\mathrm{Mat}_{\mathscr{B}}(\cdot)\left|\begin{array}{ccc}(\mathscr{L}(E),+,\circ,\cdot) & \longrightarrow & (\mathscr{M}_n(\mathbf{R}),+,\times,\cdot)\\ f & \longmapsto & \mathrm{Mat}_{\mathscr{B}}(f)\end{array}\right.$$

Alors $\mathrm{Mat}_{\mathscr{B}}(\cdot)$ est un isomorphisme de $\mathbf{R}$-algèbres. ■

PROPOSITION 160 (INVERSE D'UN ISOMORPHISME DE K-ALGÈBRES). — *Soit* **K** *un corps, soient* $(A,+_A,\times_A,\cdot_A)$ *et* $(B,+_B,\times_B,\cdot_B)$ *deux* **K***-algèbres et* $f\colon (A,+_A,\times_A,\cdot_A)\longrightarrow(B,+_B,\times_B,\cdot_B)$ *un isomorphisme d'anneaux. Alors la bijection réciproque :*

$$f^{-1}\left|\begin{array}{ccc}(B,+_B,\times_B,\cdot_B) & \longrightarrow & (A,+_A,\times_A,\cdot_A)\\ b & \longmapsto & \text{l'unique élément } a \text{ de } A \text{ tel que } f(a)=b\end{array}\right.$$

est un isomorphisme de **K***-algèbres.*

PROPOSITION 161 (PROPRIÉTÉ UNIVERSELLE DE K[X]). — *Pour tout* **K***-algèbre* A *et tout élément* a *de* A*, il existe un unique morphisme :*

$$\varphi\colon \mathbf{K}[X]\longrightarrow A$$

tel que $\varphi(X)=a$.

DÉMONSTRATION. — Soient A une $\mathbf{K}$-algèbre et $a\in A$.

• Unicité. Supposons que le morphisme de $\mathbf{K}$-algèbre $\varphi\colon \mathbf{K}[X]\longrightarrow A$ tel que $\varphi(X)=a$ existe. Comme $\varphi(1)=1_A$ et φ respecte les multiplications :

$$\forall\, n\in\mathbf{N},\quad \varphi\left(X^n\right)=a^n.$$

Comme φ est de plus $\mathbf{K}$-linéaire :

$$\forall\, P\in\mathbf{K}[X],\quad \varphi(P)=\varphi\left(\sum_{n=0}^{+\infty}[P]_n\cdot X^n\right)=\sum_{n=0}^{+\infty}[P]_n\cdot\varphi(X^n)=\sum_{n=0}^{+\infty}[P]_n\cdot a^n.$$

Ainsi, φ est nécessairement l'application :

$$\left|\begin{array}{ccc}\mathbf{K}[X] & \longrightarrow & A\\ P & \longmapsto & \displaystyle\sum_{n=0}^{+\infty}[P]_n\cdot a^n\end{array}\right.$$

ce qui assure son unicité.

• Existence. Guidés par notre étude de l'unicité, nous considérons l'application :

$$\varphi\left|\begin{array}{ccc}\mathbf{K}[X] & \longrightarrow & A\\ P & \longmapsto & \displaystyle\sum_{n=0}^{+\infty}[P]_n\cdot a^n.\end{array}\right.$$

— $\mathbf{K}$-linéarité de φ. Soient $(\lambda,\mu)\in\mathbf{K}^2$ et $(P,Q)\in\mathbf{K}[X]^2$.

$$\begin{aligned}\varphi(\lambda\cdot P+\mu\cdot Q) &= \sum_{n=0}^{+\infty}[\lambda\cdot P+\mu\cdot Q]_n\cdot a^n && \text{[définition de } \varphi\text{]}\\ &= \sum_{n=0}^{+\infty}\left(\lambda[P]_n+\mu[Q]_n\right)\cdot a^n && \text{[définition de + dans } \mathbf{K}[X]\text{]}\\ &= \lambda\cdot\left(\sum_{n=0}^{+\infty}[P]_n\cdot a^n\right)+\left(\sum_{n=0}^{+\infty}[Q]_n\cdot a^n\right) && \text{[règles de calcul dans la } \mathbf{K}\text{-algèbre } A\text{]}\\ &= \lambda\cdot\varphi(P)+\mu\cdot\varphi(Q) && \text{[définition de } \varphi\text{]}\end{aligned}$$

— L'application φ respecte les multiplications. Nous introduisons deux applications :

$$B_1 \left| \begin{array}{ccc} \mathbf{K}[X]\times\mathbf{K}[X] & \longrightarrow & A \\ (P,Q) & \longmapsto & \varphi(PQ) \end{array} \right. \quad \text{et} \quad B_2 \left| \begin{array}{ccc} \mathbf{K}[X]\times\mathbf{K}[X] & \longrightarrow & A \\ (P,Q) & \longmapsto & \varphi(P)\times_A\varphi(Q) \end{array} \right. .$$

En utilisant les règles de calculs dans les $\mathbf{K}$-algèbres $\mathbf{K}[X]$, A et la linéarité de φ nous vérifions que :

$$(\star) \qquad \text{les applications } B_1 \text{ et } B_2 \text{ sont bilinéaires.}$$

Par ailleurs, pour tout $(n,m)\in\mathbf{N}^2$:

$$B_1\left(X^n,X^m\right)=\varphi\left(X^{n+m}\right)=a^{n+m} \qquad \text{et} \qquad B_2\left(X^n,X^m\right)=\varphi\left(X^n\right)\times_A\varphi\left(X^m\right)=a^n\times_A a^m=a^{n+m}$$

Ainsi :

$$(\star\star) \qquad \forall\,(n,m)\in\mathbf{N}^2,\quad B_1\left(X^n,X^m\right)=B_2\left(X^n,X^m\right).$$

Soit $(P,Q)\in\mathbf{K}[X]^2$.

$$\begin{aligned}
\varphi(PQ) &= B_1(P,Q) \\
&= B_1\left(\sum_{n=0}^{+\infty}[P]_nX^n,\sum_{m=0}^{+\infty}[Q]_mX^m\right) \\
&= \sum_{n=0}^{+\infty}\sum_{m=0}^{+\infty}([P]_n\cdot[Q]_m)\cdot B_1\left(X^n,X^m\right) \qquad \left[\text{d'après } (\star)\right] \\
&= \sum_{n=0}^{+\infty}\sum_{m=0}^{+\infty}([P]_n\cdot[Q]_m)\cdot B_2\left(X^n,X^m\right) \qquad \left[\text{d'après } (\star\star)\right] \\
&= B_2\left(\sum_{n=0}^{+\infty}[P]_nX^n,\sum_{m=0}^{+\infty}[Q]_mX^m\right) \qquad \left[\text{d'après } (\star)\right] \\
&= B_2(P,Q) \\
&= \varphi(P)\times_A\varphi(Q)
\end{aligned}$$

— Valeur de $\varphi(1)$. D'après la définition de φ, $\varphi(1)=a^0:=1_A$.

— Valeur de $\varphi(X)$. D'après la définition de φ, $\varphi(X)=a$.

■

Remarque 162. — La proposition précédente généralise l'exemple 156 et caractérise la $\mathbf{K}$-algèbre $\mathbf{K}[X]$ à unique isomorphime près. ■