

Structures algébriques

1. Rappels sur les groupes	3
1.1. Définition d'un groupe	3
1.2. Définition d'un groupe commutatif ou abélien	3
1.3. Exemples de groupes	4
2. Rappels sur les sous-groupes	4
2.1. Définition d'un sous-groupe	4
2.2. Caractérisation des sous-groupes	5
2.3. Exemples de sous-groupes	5
3. Rappels sur les morphismes de groupes	6
3.1. Définition d'un morphisme de groupes	6
3.2. Exemples de morphismes de groupes	6
3.3. Image directe et image réciproque d'un sous-groupe par un morphisme de groupes	7
3.4. Noyau et image d'un morphisme de groupes	7
3.5. Critère d'injectivité et de surjectivité pour un morphisme de groupes	8
3.6. Composition de morphismes de groupes	8
3.7. Isomorphisme de groupes	8
4. Sous-groupes additifs de \mathbf{Z}	8
5. Sous-groupe engendré par une partie	9
5.1. Intersection de sous-groupes	9
5.2. Définition du sous-groupe engendré par une partie	9
5.3. Description du sous-groupe engendré par une partie	10
5.4. Sous-groupe engendré par un élément	10
5.5. Parties génératrices d'un groupe	10
6. Groupe $(\mathbf{Z}/n\mathbf{Z}, +)$	11
6.1. Rappels sur la relation de congruence	11
6.2. L'ensemble $\mathbf{Z}/n\mathbf{Z}$	12
6.3. Structure de groupe sur $\mathbf{Z}/n\mathbf{Z}$	13
6.4. Générateurs du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$	13
7. Classification des groupes monogènes	13
7.1. Définition d'un groupe monogène, d'un groupe cyclique	13
7.2. Exemples de groupes monogènes, de groupes cycliques	14
7.3. Les groupes $(\mathbf{Z}/n\mathbf{Z}, +)$ et (\mathbf{U}_n, \times) sont isomorphes	14
7.4. Théorème de classification des groupes monogènes	14
8. Théorème de Lagrange	15
9. Ordre d'un élément dans un groupe	16
9.1. Définition d'un élément d'ordre fini et de l'ordre d'un tel	16
9.2. Ordre d'un élément g d'un groupe versus sous-groupe $\langle g \rangle$ qu'il engendre	16
9.3. Une condition suffisante pour que tous les éléments d'un groupe aient un ordre fini	17
9.4. Puissances d'un éléments d'ordre fini	17
9.5. Propriété de divisibilité de l'ordre d'un élément d'un groupe fini	17
9.6. Une sélection d'exercices sur les groupes	18
10. Rappels sur les anneaux	18
10.1. Définition d'un anneau	18
10.2. Définition d'un anneau commutatif	19
10.3. Exemples d'anneaux	19
11. Rappels sur les sous-anneaux	19
11.1. Définition d'un sous-anneau	19
11.2. Caractérisation des sous-anneaux	20

12. Rappels sur les morphismes d'anneaux	20
12.1. Définition d'un morphisme d'anneaux	20
12.2. Exemples de morphismes d'anneaux	20
12.3. Composition de morphismes d'anneaux	21
12.4. Isomorphisme d'anneaux	21
13. Compléments sur les anneaux	22
13.1. Produit d'un nombre fini d'anneaux	22
13.2. Définition d'un idéal d'un anneau commutatif	22
13.3. Caractérisation des idéaux	23
13.4. Exemples d'idéaux	23
13.5. Le noyau d'un morphisme d'anneaux commutatifs est un idéal de la source	24
13.6. Idéal engendré par un élément	24
13.7. Divisibilité dans un anneau commutatif intègre	24
14. Idéaux de \mathbf{Z}	24
14.1. Sous-groupes additifs de \mathbf{Z} versus idéaux de \mathbf{Z}	24
14.2. Description des idéaux de \mathbf{Z}	25
14.3. PGCD d'un nombre fini d'entiers en termes d'idéaux	25
14.4. Relation de Bézout pour le PGCD d'un nombre fini d'entiers	25
15. L'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \times)$	25
15.1. Inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$	25
15.2. CNS pour que $\mathbf{Z}/n\mathbf{Z}$ soit un corps	26
15.3. Théorème des restes chinois	28
15.4. Théorème d'Euler	30
16. L'anneau $(\mathbf{K}[X], +, \times)$	31
16.1. Description des idéaux de $\mathbf{K}[X]$	31
16.2. PGCD d'un nombre fini de polynômes	32
16.3. Relation de Bézout pour le PGCD d'un nombre fini de polynômes	32
16.4. Notion de polynôme irréductible sur un corps	32
16.5. Irréductibles de $\mathbf{K}[X]$ de degré 1, 2, 3	32
16.6. Deux résultats de primalité relative dans $\mathbf{K}[X]$	33
16.7. Décomposition d'un polynôme de $\mathbf{K}[X]$ en produit de polynômes irréductibles sur \mathbf{K}	33
16.8. Irréductibles de $\mathbf{C}[X]$ et irréductibles de $\mathbf{R}[X]$	35
16.9. Décomposition en produit d'irréductibles dans $\mathbf{C}[X]$	35
16.10. Décomposition en produit d'irréductibles dans $\mathbf{R}[X]$	35
17. Algèbres	36
17.1. Définition d'une \mathbf{K} -algèbre	36
17.2. Exemples de \mathbf{K} -algèbres	37
17.3. Sous-algèbres	37
17.4. Morphisme d'algèbres	38

1. Rappels sur les groupes

1.1. Définition d'un groupe

Définition 1. — Soit G un ensemble et soit une loi de composition interne notée $*$:

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

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. — 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 $x \in G$, $x * e = x = x * e$. En effet, si e_1 et e_2 sont deux éléments de G tels que :

$$\forall x \in G \quad x * e_1 = x = x * e_1 \quad \text{et} \quad x * e_2 = x = x * e_2$$

alors :

$$e_1 = e_1 * e_2 = e_2 .$$

L'élément e est appelé neutre du groupe.

3. Si x est un élément de G il existe un seul élément y de G tel que $x * y = e = y * x$. En effet, si y_1, y_2 sont deux éléments de G tels que :

$$x * y_1 = e = y_1 * x \quad \text{et} \quad x * y_2 = e = y_2 * x$$

alors :

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2 .$$

Cet élément y est nommé symétrique de x et on le note x^{-1} .

4. L'inverse de e est e , i.e. $e^{-1} = e$. En effet, si on pose $y = e$, alors $e * y = e = y * e$.
5. Si x et y sont deux éléments de G , alors $(x * y)^{-1} = y^{-1} * x^{-1}$. En effet, si on pose $z = y^{-1} * x^{-1}$, alors :

$$(x * y) * z = x * \underbrace{(y * y^{-1})}_{=e} * x^{-1} = x * x^{-1} = e \quad \text{et} \quad z * (x * y) = y^{-1} * \underbrace{(x^{-1} * x)}_{=e} * y = y^{-1} * y = e .$$

6. Si x est un élément de G , alors $(x^{-1})^{-1} = x$. En effet, si on pose $y = x$, alors $x^{-1} * y = e$ et $y * x^{-1} = e$.

Remarque 3. — 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} .

1.2. Définition d'un groupe commutatif ou abélien

Définition 4. — 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. — 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}).

1.3. Exemples de groupes

Exemple 6. — Les ensembles de nombres livrent les groupes commutatifs suivants.

$$(\mathbf{Z}, +) \quad (\mathbf{Q}, +) \quad (\mathbf{R}, +) \quad (\mathbf{C}, +) \quad (\{-1, 1\}, \times) \quad (\mathbf{Q}^*, \times) \quad (\mathbf{R}^*, \times) \quad (\mathbf{C}^*, \times)$$

Exemple 7. — L'ensemble $\mathbf{R}[X]$ des polynômes à coefficients dans \mathbf{R} muni de l'addition usuelle $+$ est un groupe.

Exemple 8. — Soit $(p, n) \in \mathbf{N}^* \times \mathbf{N}^*$. L'ensemble $\mathcal{M}_{n,p}(\mathbf{C})$ des matrices à n lignes, p colonnes et à coefficients dans \mathbf{C} muni de l'addition usuelle est un groupe.

Exemple 9. — Si E est un ensemble non vide, alors l'ensemble $\mathfrak{S}(E)$ 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 $\llbracket 1, n \rrbracket$ dans lui-même muni de la loi \circ est un groupe.

Exemple 10. — Soit un entier $n \geq 2$. L'ensemble $\mathbf{GL}_n(\mathbf{R})$ 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 :

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

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

Exercice 12. — Soit (E, \circ) un ensemble non vide. Déterminer une condition nécessaire et suffisante pour que le groupe $(\mathfrak{S}(E), \circ)$ soit abélien.

2. Rappels sur les sous-groupes

2.1. Définition d'un sous-groupe

Définition 13. — 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 les trois propriétés suivantes sont vérifiées.

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

Remarque 15. — 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.

2.2. Caractérisation des sous-groupes

Proposition 16. — 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 17. — 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 :

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

2.3. Exemples de sous-groupes

Exemple 18. — L'ensemble :

$$\mathbf{U} := \{z \in \mathbf{C} : |z| = 1\} = \{e^{i\theta} : \theta \in \mathbf{R}\} \quad [\text{cercle unité}]$$

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

Exemple 19. — Soit $n \in \mathbf{N}^*$. L'ensemble :

$$\mathbf{U}_n := \{z \in \mathbf{C} : z^n = 1\} = \left\{ e^{i \frac{2k\pi}{n}} : k \in \llbracket 0, n-1 \rrbracket \right\} \quad [\text{ensemble des racines } n\text{-ièmes de l'unité}]$$

est un sous-groupe de (\mathbf{U}, \times) .

Exemple 20. — Soit un entier $n \geq 2$. Démontrer que :

$$\mathbf{A}_n := \{\sigma \in \mathfrak{S}_n : \varepsilon(\sigma) = 1\} \quad [\text{groupe alterné d'indice } n]$$

est un sous-groupe de (\mathfrak{S}_n, \circ) .

Exemple 21. — Si E est un \mathbf{K} -espace vectoriel, alors l'ensemble :

$$\mathbf{GL}(E) := \{f \in \mathcal{L}(E) : f \text{ est bijective}\} \quad [\text{groupe des automorphismes de } E]$$

est un sous-groupe de $(\mathcal{L}(E), \circ)$.

Exemple 22. — Soit $n \in \mathbf{N}^*$. L'ensemble :

$$\mathbf{SL}_n(\mathbf{R}) := \{M \in \mathcal{M}_n(\mathbf{R}) : \det(M) = 1\} \quad [\text{groupe spécial linéaire}]$$

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

Exercice 23. — Démontrer que :

$$\mathbf{O}_n(\mathbf{R}) := \{M \in \mathcal{M}_n(\mathbf{R}) : M \times M^T = I_n\} \quad [\text{groupe orthogonal}]$$

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

Exercice 24. — Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien. On note $\|\cdot\|$ la norme associée au produit scalaire $\langle \cdot, \cdot \rangle$. Démontrer que :

$$\mathbf{O}(E) := \{f \in \mathcal{L}(E) : \forall x \in E \quad \|f(x)\| = \|x\|\} \quad [\text{groupe orthogonal de } E]$$

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

3. Rappels sur les morphismes de groupes

3.1. Définition d'un morphisme de groupes

Définition 25. — Soient $(G, *)$ et (H, \cdot) deux groupes. Une application $f : G \rightarrow H$ est un morphisme de groupes si :

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

Proposition 26. — Soient $(G, *)$ et (H, \cdot) deux groupes, Soit $f : G \rightarrow H$ un morphisme de groupes. Notons respectivement e_G et e_H les éléments neutres de G et H .

(a) L'application f respecte les neutres, i.e. :

$$f(e_G) = e_H.$$

(b) L'application f respecte les symétriques, i.e. :

$$\forall x \in G \quad f(x^{-1}) = f(x)^{-1}.$$

3.2. Exemples de morphismes de groupes

Exemple 27. — Si $a \in \mathbb{Z}$, l'application :

$$\varphi_a \left| \begin{array}{l} (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +) \\ n \longmapsto an \end{array} \right.$$

est un morphisme de groupes.

Exemple 28. — L'application :

$$\ln \left| \begin{array}{l} (\mathbb{R}_{>0}, \times) \longrightarrow (\mathbb{R}, +) \\ x \longmapsto \ln(x) \end{array} \right.$$

est un morphisme de groupes.

Exemple 29. — Soit $n \in \mathbb{N}^*$. Pour tout $\sigma \in \mathfrak{S}_n$, on pose :

$$I(\sigma) := \text{card}(\{(i, j) \in \llbracket 1, n \rrbracket^2 : i < j \text{ et } \sigma(i) > \sigma(j)\}) \quad [\text{nombre d'inversions de } \sigma].$$

La signature :

$$\varepsilon \left| \begin{array}{l} (\mathfrak{S}_n, \circ) \longrightarrow (\{-1, 1\}, \times) \\ \sigma \longmapsto \varepsilon(\sigma) = (-1)^{I(\sigma)} \end{array} \right.$$

est un morphisme de groupes.

Exemple 30. — Soit n^* . L'application :

$$\left| \begin{array}{l} (\mathbf{GL}_n(\mathbf{C}), \times) \longrightarrow (\mathbf{C}^*, \times) \\ M \longmapsto \det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{k=1}^n [M]_{k, \sigma(k)} \end{array} \right.$$

est un morphisme de groupes.

Exercice 31. — Soit un entier $n \geq 2$. L'application :

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

est-elle un morphisme de groupes ?

Exercice 32. — Soit f un morphisme de groupes de $(\mathbb{Z}, +)$ dans lui-même. Démontrer que :

$$\exists a \in \mathbb{Z} \quad \forall n \in \mathbb{Z} \quad f(n) = an.$$

3.3. Image directe et image réciproque d'un sous-groupe par un morphisme de groupes

Proposition 33. — Soient $(G, *)$, (H, \cdot) deux groupes et $f : G \longrightarrow H$ un morphisme de groupes.

(a) Soit K un sous-groupe de $(G, *)$. Alors :

$$f(K) := \{f(k) : k \in K\}$$

est un sous-groupe de (H, \cdot) .

(b) Soit L un sous-groupe de (H, \cdot) . Alors :

$$f^{-1}(L) := \{g \in G : f(g) \in L\}$$

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

3.4. Noyau et image d'un morphisme de groupes

Définition 34. — Soient $(G, *)$, (H, \cdot) deux groupes et $f : G \longrightarrow H$ un morphisme de groupes.

(a) L'ensemble :

$$\text{Ker}(f) := \{x \in G : f(x) = e_H\} = f^{-1}(\{e_H\})$$

est appelé noyau du morphisme f .

(b) L'ensemble :

$$\text{Im}(f) := \{f(x) : x \in G\} = f(G)$$

est appelé image du morphisme f .

Proposition 35. — 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. $\text{Ker}(f)$ est un sous-groupe de G .
2. $\text{Im}(f)$ est un sous-groupe de H .

Exemple 36. — Soit un entier $n \geq 2$. L'application :

$$\left| \begin{array}{ll} (\text{O}_n(\mathbf{R}), \times) & \longrightarrow (\mathbf{R}^*, \times) \\ M & \longmapsto \det(M) \end{array} \right.$$

est un morphisme de groupes. Son noyau est noté $\text{SO}_n(\mathbf{R})$, i.e. :

$$\text{SO}_n(\mathbf{R}) := \{M \in \text{O}_n(\mathbf{R}) : \det(M) = 1\} \quad [\text{groupe spécial orthogonal}] .$$

Exercice 37. — On considère l'application :

$$\rho \left| \begin{array}{ll} (\mathbf{R}, +) & \longrightarrow (\text{SO}_2(\mathbf{R}), \times) \\ \theta & \longmapsto \rho(\theta) := \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} . \end{array} \right.$$

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.

3.5. Critère d'injectivité et de surjectivité pour un morphisme de groupes

Proposition 38. — Soient $(G, *)$, (H, \cdot) deux groupes et $f : G \longrightarrow H$ un morphisme de groupes.

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

3.6. Composition de morphismes de groupes

Théorème 39. — 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 :

$$g \circ f \quad \left| \begin{array}{l} (G_1, *_1) \longrightarrow (G_3, *_3) \\ x_1 \longmapsto g(f(x_1)) \end{array} \right.$$

est un morphisme de groupes.

3.7. Isomorphisme de groupes

Définition 40. — 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 :

- (a) f est un morphisme de groupes ;
 (b) f est bijectif.

Remarque 41. — Deux groupes sont dits isomorphes s'il existe un isomorphisme de groupes de l'un vers l'autre.

Exercice 42. — Déterminer tous les isomorphismes de groupes de $(\mathbf{Z}, +)$ dans lui-même.

Exercice 43. — Les groupes (\mathbf{R}^*, \times) et (\mathbf{R}_+^*, \times) sont-ils isomorphes ?

Proposition 44. — Soit $f : (G_1, *_1) \longrightarrow (G_2, *_2)$ un isomorphisme de groupes. Sa bijection réciproque :

$$f^{-1} \quad \left| \begin{array}{l} (G_2, *_2) \longrightarrow (G_1, *_1) \\ g_2 \longmapsto \text{l'unique } g_1 \in G_1 \text{ tel que } f(g_1) = g_2 \end{array} \right.$$

est un morphisme de groupes.

4. Sous-groupes additifs de \mathbf{Z}

Rappel 45. — 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 :

$$a = qb + r \quad \text{et} \quad 0 \leq r < b.$$

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

Proposition 46. — Soit $a \in \mathbf{N}$. Alors l'ensemble :

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

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

Théorème 47. — Soit H un sous-groupe de $(\mathbf{Z}, +)$. Alors :

$$\exists ! a \in \mathbf{N} \quad H = a\mathbf{Z} := \{an : n \in \mathbf{Z}\} .$$

Remarque 48. — La proposition et le théorème qui précèdent nous livrent le résultat suivant. Les parties de \mathbf{Z} de la forme $a\mathbf{Z}$ (avec $a \in \mathbf{N}$) sont les seuls sous-groupes de $(\mathbf{Z}, +)$.

Exercice 49. — Soit H un sous-groupe de $(\mathbf{R}, +)$ distinct de $\{0_{\mathbf{R}}\}$.

1. Démontrer que $a := \inf(H \cap \mathbf{R}_+^*)$ 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

5.1. Intersection de sous-groupes

Proposition 50. — 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 51. — Soient a et b des entiers naturels non nuls. Déterminer le sous-groupe $a\mathbf{Z} \cap b\mathbf{Z}$ de $(\mathbf{Z}, +)$.

5.2. Définition du sous-groupe engendré par une partie

Exercice 52. — 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 53. — Soient $(G, *)$ un groupe et A une partie non vide de G .

- (a) 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 $\langle A \rangle$.
- (b) En d'autres termes, $\langle A \rangle$ est caractérisé par les deux propriétés suivantes :
 - $\langle A \rangle$ est un sous-groupe de G tel que $A \subset \langle A \rangle$;
 - si H sous-groupe de G tel que $A \subset H$, alors $\langle A \rangle \subset H$ (propriété de minimalité).
- (c) Le sous-groupe engendré par A est l'intersection de tous les sous-groupes de G contenant A :

$$\langle A \rangle = \bigcap_{\substack{H \text{ sous-groupe de } G \\ \text{tel que } A \subset H}} H .$$

Exercice 54. — Soient a et b des entiers naturels non nuls. Déterminer le sous-groupe $\langle a, b \rangle$ de $(\mathbf{Z}, +)$.

Exercice 55. — On pose $\zeta_3 := e^{i\frac{2\pi}{3}}$ et $\zeta_5 := e^{i\frac{2\pi}{5}}$. Déterminer le sous-groupe $\langle \zeta_3, \zeta_5 \rangle$ de (\mathbf{C}^*, \times) .

5.3. Description du sous-groupe engendré par une partie

Théorème 56. — 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 :

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

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

$$\langle A \rangle = \bigcup_{n \in \mathbf{N}^*} \{x_1 * \dots * x_n : (x_1, \dots, x_n) \in (A \cup A^{-1})^n\} .$$


5.4. Sous-groupe engendré par un élément

Définition 57. — 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 :

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

Proposition 58. — Soient $(G, *)$ un groupe et $(x, n, m) \in G \times \mathbf{Z} \times \mathbf{Z}$. Alors :

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

 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 59. — Soient $(G, *)$ un groupe et $a \in G$. Alors :

$$\langle a \rangle = \{a^n : n \in \mathbf{Z}\} .$$

5.5. Parties génératrices d'un groupe

Définition 60. — 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 $G = \langle A \rangle$.

Exemple 61. — Le groupe $(\mathbf{Z}, +)$ des entiers relatifs est engendré par l'élément 1.

Exemple 62. — Soit un entier $n \geq 2$. Le groupe $(\mathbf{Z}^n, +)$ est engendré par :

$$\{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)\} .$$

Exemple 63. — Soit un entier $n \geq 2$. Le groupe (\mathfrak{S}_n, \circ) est engendré par les transpositions :

$$\mathfrak{S}_n = \langle \{(i \ j) : 1 \leq i < j \leq n\} \rangle \quad \left[\text{partie génératrice à } \binom{n}{2} \text{ éléments} \right] .$$

Exemple 64. — Soit un entier $n \geq 2$. Le groupe $(\mathbf{GL}_n(\mathbf{K}), \times)$ est engendré par les matrices de transvection et les matrices de dilatation, i.e. $\mathbf{GL}_n(\mathbf{K})$ est engendré par :

$$\{T_{i,j}(\lambda) := I_n + \lambda \cdot E_{i,j} : (i,j) \in \llbracket 1, n \rrbracket^2 \text{ tel que } i \neq j \text{ et } \lambda \in \mathbf{K}\} \cup \{D_i(\lambda) := I_n + (\lambda - 1) \cdot E_{i,i} : i \in \llbracket 1, n \rrbracket \text{ et } \lambda \in \mathbf{K}^*\}.$$

Exercice 65. — Soit un entier $n \geq 2$.

1. Soient a_1, \dots, a_p des éléments distincts de $\llbracket 1, n \rrbracket$ et σ une permutation de $\llbracket 1, n \rrbracket$. Démontrer que :

$$\sigma \circ \underbrace{(a_1 \ a_2 \ \dots \ a_p)}_{\text{cycle de longueur } p} \circ \sigma^{-1} = \underbrace{(\sigma(a_1) \ \sigma(a_2) \ \dots \ \sigma(a_p))}_{\text{cycle de longueur } p}.$$

2. Notons $\tau := (1 \ 2)$ la transposition de $\llbracket 1, n \rrbracket$ échangeant 1 et 2 et le cycle $\sigma := (1 \ 2 \ 3 \ \dots \ n)$ de longueur n . Démontrer que $\{(1 \ 2), \sigma\}$ engendre le groupe (\mathfrak{S}_n, \circ) .

Exercice 66. — 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 67. — 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 (\mathbf{R}^*, \times) n'est pas de type fini.
3. En déduire que pour tout entiers $n \geq 2$, le groupe $(\mathbf{GL}_n(\mathbf{R}), \times)$ n'est pas de type fini.

6. Groupe $(\mathbf{Z}/n\mathbf{Z}, +)$

6.1. Rappels sur la relation de congruence

Définition 68. — 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 69. — 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 70. — 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 :

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

Proposition 71. — Soit $(n, a, b, k) \in \mathbf{N}^* \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{N}^*$. Alors :

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

Exercice 72. — Démontrer que pour tout $n \in \mathbf{N}$, 5 divise $2^{3n+5} + 3^{n+1}$.

Proposition 73. — Soit $n \in \mathbf{N}^*$. La relation de congruence modulo n est une relation d'équivalence.

6.2. L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Rappel 74. — Soit E un ensemble muni d'une relation d'équivalence \mathcal{R} . Pour tout $x \in E$, on note :

$$\bar{x} := \{y \in E : y \mathcal{R} x\} \in \mathcal{P}(E) \quad [\text{classe d'équivalence de } x] .$$

On rappelle trois propriétés fondamentales des classes d'équivalences.

1. Deux éléments de E ont la même classe si et seulement s'ils sont en relation. — Soit $(x, y) \in E^2$. Alors :

$$x \mathcal{R} y \iff \bar{x} = \bar{y}$$

\implies Supposons $x \mathcal{R} y$. Soit $z \in \bar{x}$. Alors $z \mathcal{R} x$. Par transitivité de \mathcal{R} , $z \mathcal{R} y$. Ainsi $z \in \bar{y}$. Nous en déduisons $\bar{x} \subset \bar{y}$. Par symétrie, $\bar{y} \subset \bar{x}$.

\impliedby Supposons $\bar{x} = \bar{y}$. Comme \mathcal{R} est réflexive, $x \in \bar{x}$. Ainsi $x \in \bar{y}$, d'où $x \mathcal{R} y$.

2. Deux classes d'équivalence sont soit disjointes, soit confondues. — Soit $(x, y) \in E^2$. Alors :

$$\bar{x} = \bar{y} \quad \text{ou} \quad \bar{x} \cap \bar{y} = \emptyset .$$

Supposons $\bar{x} \cap \bar{y} \neq \emptyset$ et démontrons $\bar{x} = \bar{y}$. Soit $z \in \bar{x} \cap \bar{y}$. Alors $z \mathcal{R} x$ et $z \mathcal{R} y$. Par symétrie et transitivité de la relation \mathcal{R} , $x \mathcal{R} y$. Nous en déduisons, à l'aide de 1, que $\bar{x} = \bar{y}$.

3. Les classes d'équivalence partitionnent l'ensemble E . — L'ensemble des classes d'équivalence pour la relation \mathcal{R} est appelé ensemble quotient de E par \mathcal{R} et est noté E/\mathcal{R} .

$$E = \bigsqcup_{C \in E/\mathcal{R}} C \quad [\text{partition de } E \text{ suivant les classes d'équivalence}] .$$

\supset Cette inclusion est claire car une classe d'équivalence est par essence une partie de E .

\subset Puisque \mathcal{R} est réflexive, $x \in \bar{x}$. Comme \bar{x} est une classe d'équivalence, $\bar{x} \in E/\mathcal{R}$. Donc x appartient bien à la réunion des classes d'équivalence et l'inclusion \subset est établie.

Nous avons établi que E est bien la réunion des classes d'équivalence. Le caractère disjoint de cette réunion est déjà connu (cf. 2).

Définition 75. — Soit $(n, a) \in \mathbb{N}^* \times \mathbb{Z}$. Notons :

$$\bar{a} := \{b \in \mathbb{Z} : a \equiv b [n]\} = a + n\mathbb{Z} \quad [\text{classe de } a \text{ modulo } n]$$

l'ensemble des entiers congrus à a modulo n .

Proposition 76. — Soit $n \in \mathbb{N}^*$. Il y a exactement n classes d'équivalences distinctes pour la relation de congruence modulo n . Ces n classes sont :

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

Définition 77. — Soit $n \in \mathbb{N}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences pour la relation de congruence modulo n . Ainsi :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\} \quad [\text{ensemble fini de cardinal } n] .$$

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



$$f \left| \begin{array}{l} \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z} \\ \bar{a} \longmapsto a \end{array} \right.$$

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

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

6.3. Structure de groupe sur $\mathbb{Z}/n\mathbb{Z}$

Théorème 78. — Soit $n \in \mathbb{N}^*$. Posons

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

Alors :

- (a) l'application $+$ est une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$, qui est bien définie ;
- (b) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien, de neutre $\bar{0}$.

Exemple 79. — La table du groupe $(\mathbb{Z}/6\mathbb{Z}, +)$ est la suivante.

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

1. L'opposé de $\bar{5}$ dans $(\mathbb{Z}/6\mathbb{Z}, +)$ est donc $\bar{1}$.
2. Le sous-groupe engendré par $\bar{2}$ dans $(\mathbb{Z}/6\mathbb{Z}, +)$ est :

$$\langle \bar{2} \rangle = \{ \bar{0}, \bar{2}, \bar{4} \}.$$
3. L'élément $\bar{1}$ engendre le groupe $(\mathbb{Z}/6\mathbb{Z}, +)$. Il en est de même de de l'élément $\bar{5}$.

6.4. Générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Proposition 80. — Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. L'élément \bar{a} de $\mathbb{Z}/n\mathbb{Z}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si a est premier avec n , i.e. :

$$\langle \bar{a} \rangle = \mathbb{Z}/n\mathbb{Z} \iff a \wedge n = 1.$$

Exemple 81. — Les seuls éléments qui engendrent le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$ sont $\bar{1}, \bar{5}, \bar{7}, \bar{11}$.

7. Classification des groupes monogènes

7.1. Définition d'un groupe monogène, d'un groupe cyclique

Définition 82. — Soit $(G, *)$ un groupe.

- (a) Le groupe $(G, *)$ est dit monogène s'il est engendré par un élément, i.e. si :

$$\exists x \in G \quad G = \langle x \rangle = \{ x^n : n \in \mathbb{Z} \}.$$

- (b) Le groupe $(G, *)$ est dit cyclique s'il est monogène et fini.

Remarque 83. — Tout groupe monogène est abélien.

7.2. Exemples de groupes monogènes, de groupes cycliques

Exemple 84. — Le groupe $(\mathbb{Z}, +)$ est engendré par l'élément 1. Il est donc monogène

Exemple 85. — Pour tout $n \in \mathbb{N}^*$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est fini et engendré par l'élément $\bar{1}$. Il est donc cyclique.

Exemple 86. — Pour tout $n \in \mathbb{N}^*$, le groupe multiplicatif :

$$U_n := \{z \in \mathbb{C} : z^n = 1\} = \left\{ e^{i\frac{2k\pi}{n}} : k \in \llbracket 0, n-1 \rrbracket \right\}$$

est fini et engendré par l'élément $e^{i\frac{2\pi}{n}}$. Il est donc cyclique.

Exercice 87. — Démontrer que le groupe $(\mathbb{Z}^2, +)$ n'est pas monogène. En déduire que les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$ ne sont pas isomorphes.

Exercice 88. — Les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont-ils isomorphes ?

7.3. Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et (U_n, \times) sont isomorphes

Proposition 89. — Soit $n \in \mathbb{N}^*$. L'application :

$$\varphi \left| \begin{array}{l} (\mathbb{Z}/n\mathbb{Z}, +) \longrightarrow (U_n, \times) \\ \bar{k} \longmapsto e^{i\frac{2k\pi}{n}} \end{array} \right.$$

est bien définie et est un isomorphisme de groupes.

7.4. Théorème de classification des groupes monogènes

Théorème 90. — Soit $(G, *)$ un groupe monogène.

- (a) Si G est infini, alors $(G, *)$ est isomorphe à $(\mathbb{Z}, +)$.
- (b) Si G est fini de cardinal $n \geq 1$, alors $(G, *)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Éléments de démonstration. Soit x un générateur du groupe G . D'après les propriétés de la notation puissance, l'application :

$$\varphi \left| \begin{array}{l} (\mathbb{Z}, +) \longrightarrow (G, *) \\ k \longmapsto x^k \end{array} \right.$$

est un morphisme de groupes, qui est surjectif.

Son noyau est un sous-groupe de $(\mathbb{Z}, +)$. Il existe donc un unique entier $n \in \mathbb{N}$ tel que $\text{Ker}(\varphi) = n\mathbb{Z}$.

- Cas où $n = 0$. — Alors l'application φ est un isomorphisme.
- Cas où $n \geq 1$. — On vérifie alors que l'application :

$$\varphi \left| \begin{array}{l} (\mathbb{Z}/n\mathbb{Z}, +) \longrightarrow (G, *) \\ \bar{k} \longmapsto x^k \end{array} \right.$$

induite par φ est un isomorphisme de groupes.

□

8. Théorème de Lagrange

Théorème 91. — 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 $x \mathcal{R} y$ si et seulement si $x * y^{-1} \in H$. Établissons que \mathcal{R} est une relation d'équivalence sur G .

— La relation \mathcal{R} est réflexive. — Soit $x \in G$. Comme $x * x^{-1} = e_G \in H$, $x \mathcal{R} x$.

— La relation \mathcal{R} est symétrique. — Soient $(x, y) \in G^2$ tels que $x \mathcal{R} y$. Alors $x * y^{-1} \in H$. Comme H est stable par passage à l'inverse :

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

Ainsi $y \mathcal{R} x$.

— La relation \mathcal{R} est transitive. — Soient $(x, y, z) \in G^3$ tels que $x \mathcal{R} y$ et $y \mathcal{R} z$. 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 $\mathcal{P}(G)$ de ses parties est fini et donc il n'y a qu'un nombre fini de classes d'équivalence, disons p . Notons $\overline{x_1}, \dots, \overline{x_p}$ la liste exhaustive, sans répétition, des différentes classes d'équivalence. Alors :

$$G = \bigsqcup_{i=1}^p \overline{x_i}.$$

En conséquence :

$$(*) \quad \text{card}(G) = \sum_{i=1}^p \text{card}(\overline{x_i}).$$

- Soit $i \in \llbracket 1, p \rrbracket$. Démontrons $\text{card}(\overline{x_i}) = \text{card}(H)$, ce qui grâce à l'identité $(*)$ nous permettra de conclure. L'application :

$$\varphi \left| \begin{array}{l} \overline{x_i} \longrightarrow H \\ y \longmapsto x_i * y^{-1} \end{array} \right.$$

est bien définie (cf. définition de \mathcal{R}). L'application :

$$\psi \left| \begin{array}{l} H \longrightarrow \overline{x_i} \\ z \longmapsto z^{-1} * x_i \end{array} \right.$$

est également bien définie. En effet :

$$\begin{aligned} z \in H &\implies x_i * x_i^{-1} * z \in H \\ &\implies x_i * (z^{-1} * x_i)^{-1} \in H \\ &\implies x_i * \psi(z)^{-1} \in H \\ &\implies x_i \mathcal{R} \psi(z) \\ &\implies \psi(z) \in \overline{x_i}. \end{aligned}$$

On vérifie de plus que $\psi \circ \varphi = \text{id}_{\overline{x_i}}$ et $\varphi \circ \psi = \text{id}_H$. Donc φ est une bijection (idem pour ψ). Ainsi $\overline{x_i}$ et H ont le même cardinal. □

Remarque 92. — 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 , aussi est-il cyclique. 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.

9. Ordre d'un élément dans un groupe

9.1. Définition d'un élément d'ordre fini et de l'ordre d'un tel

Définition 93. — Soient $(G, *)$ un groupe, de neutre noté e , et $x \in G$.

(a) On dit que x est d'ordre fini si :

$$\exists n \in \mathbf{N}^* \quad x^n = e .$$

(b) Si x est d'ordre fini, on appelle ordre de x et on note $\text{ord}(x)$ le plus petit $n \in \mathbf{N}^*$ tel que $x^n = e$, i.e. :

$$\text{ord}(x) := \min \{n \in \mathbf{N}^* : x^n = e\} .$$

Exercice 94. — Déterminer l'ordre de tous les éléments de $(\mathbf{Z}/5\mathbf{Z}, +)$, puis l'ordre de tous les éléments de $(\mathbf{Z}/p\mathbf{Z}, +)$ pour un nombre premier p .

Exercice 95. — Déterminer l'ordre de tous les éléments de $(\mathbf{Z}/12\mathbf{Z}, +)$.

9.2. Ordre d'un élément g d'un groupe versus sous-groupe $\langle g \rangle$ qu'il engendre

Proposition 96. — Soient $(G, *)$ un groupe et $x \in G$. Alors :

(a) x est d'ordre fini si et seulement si $\langle x \rangle$ est un ensemble fini ;

(b) si x est d'ordre fini, alors $\text{card}(\langle x \rangle) = \text{ord}(x)$.

Démonstration. Considérons l'application :

$$\varphi \left| \begin{array}{l} (\mathbf{Z}, +) \longrightarrow (\langle x \rangle, *) \\ k \longmapsto x^k \end{array} \right.$$

qui est un morphisme de groupes surjectif (d'après la description de $\langle x \rangle$).

Son noyau est un sous-groupe de $(\mathbf{Z}, +)$. Il existe donc un unique entier $n \in \mathbf{N}$ tel que $\text{Ker}(\varphi) = n\mathbf{Z}$.

- Cas où $n = 0$. — Supposons que $n = 0$. Alors l'application φ est bijective. Nous en déduisons que x n'est pas d'ordre fini et que $\langle x \rangle$ est infini.
- Cas où $n \geq 1$. — Supposons que $n \geq 1$. On vérifie alors que l'application :

$$\bar{\varphi} \left| \begin{array}{l} (\mathbf{Z}/n\mathbf{Z}, +) \longrightarrow (\langle x \rangle, *) \\ \bar{k} \longmapsto x^k \end{array} \right.$$

induite par φ est un isomorphisme de groupes.

Dans ce cas, $\langle x \rangle$ est de cardinal n .

De plus, comme $\bar{\varphi}(\bar{1}) = x$, l'ordre de x dans $(G, *)$ coïncide avec l'ordre de $\bar{1}$ dans $(\mathbf{Z}/n\mathbf{Z}, +)$. Comme ce dernier vaut n , il vient :

$$\text{card}(\langle x \rangle) = n = \text{ord}(x) .$$

□

De cette démonstration, nous déduisons que si x est un élément d'ordre fini d'un groupe G , alors :



$$e_G, x, x^2, \dots, x^{\text{ord}(x)-1}$$

est une liste exhaustive et sans répétition des éléments du sous-groupe $\langle x \rangle$ de G engendré par x .

9.3. Une condition suffisante pour que tous les éléments d'un groupe aient un ordre fini

Proposition 97. — Dans un groupe fini, tout élément est d'ordre fini.

Remarque 98. — On vérifie que :

$$U_\infty := \bigcup_{n=1}^{+\infty} U_n$$

est un sous-groupe de (\mathbf{C}^*, \times) . Ainsi, U_∞ est-il naturellement muni d'une structure de groupe multiplicatif. Tous les éléments du groupe (U_∞, \times) sont d'ordre fini, mais l'ensemble U_∞ est infini.

Exemple 99. — Dans le groupe $(\mathbf{Z}, +)$, le seul élément d'ordre fini est 0.

Exemple 100. — Dans le groupe $(\{-1, 1\}, \times)$, 1 est d'ordre 1 et -1 est d'ordre 2.

Exemple 101. — Soit un entier $n \geq 2$. L'élément $e^{i\frac{2\pi}{n}}$ est d'ordre n dans le groupe (U_n, \times) .

Exemple 102. — Soient un entier $n \geq 2$ et $p \in \llbracket 2, n \rrbracket$. Dans le groupe (S_n, \circ) , tout p -cycle est d'ordre p .

Exercice 103. — Soit E un \mathbf{R} -espace vectoriel non réduit à $\{0_E\}$. Que dire d'un élément d'ordre 2 du groupe $(\text{GL}(E), \circ)$? On s'efforcera d'être aussi exhaustif que possible.

9.4. Puissances d'un éléments d'ordre fini

Proposition 104. — Soient $(G, *)$ un groupe dont le neutre est noté e et x un élément de G d'ordre fini. Alors, pour tout $n \in \mathbf{Z}$:

$$x^n = e \iff \text{ord}(x) \mid n.$$

9.5. Propriété de divisibilité de l'ordre d'un élément d'un groupe fini

Théorème 105. — Soient $(G, *)$ un groupe fini et $x \in G$.

1. x est d'ordre fini.
2. $\text{ord}(x) \mid \text{card}(G)$.
3. $x^{\text{card}(G)} = e_G$

Démonstration.

1. Le sous-groupe $\langle x \rangle$ de G étant une partie de G , il est fini. D'après la proposition 96, x est d'ordre fini.
2. D'après la proposition 96 :

$$\text{ord}(x) = \text{card}(\langle x \rangle).$$

D'après le théorème de Lagrange (théorème 91) :

$$\text{card}(\langle x \rangle) \mid \text{card}(G).$$

Ainsi $\text{ord}(x) \mid \text{card}(G)$.

3. Comme $\text{ord}(x) \mid \text{card}(G)$, la proposition 104 livre $x^{\text{card}(G)} = e_G$.

□

9.6. Une sélection d'exercices sur les groupes

Exercice 106. — Soient $(G, *)$ un groupe cyclique de cardinal noté n et d un diviseur positif de n .

1. Démontrer que :

$$H_d = \{x \in G : x^d = e_G\}$$

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

2. Démontrer que H_d est l'unique sous-groupe de cardinal d de $(G, *)$.

3. Qu'en déduire quant aux sous-groupes de $(G, *)$?

Exercice 107. — Soient un entier $n \geq 2$ et $\sigma \in S_n$. Considérons « la » décomposition de σ en produit de cycles à supports disjoints :

$$\sigma = c_1 \circ \dots \circ c_r \quad [\text{unique à l'ordre près}]$$

et notons ℓ_1, \dots, ℓ_r les longueurs respectives des cycles c_1, \dots, c_r . Démontrer que l'ordre de σ est le PPCM des longueurs des cycles ℓ_1, \dots, ℓ_r .

Exercice 108. — Si $(G, *)$ est un groupe et si g_1, g_2 sont deux éléments de G , a-t-on nécessairement :

$$\text{ord}(g_1 * g_2) = \text{ord}(g_1) \vee \text{ord}(g_2) ?$$

Exercice 109. — Si $(G, *)$ un groupe tel que, pour tout $g \in G$, $g^2 = e_G$. Démontrer que le groupe $(G, *)$ est abélien.

10. Rappels sur les anneaux

10.1. Définition d'un anneau

Définition 110. — 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. :

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

Remarque 111. — Soit $(A, +, \times)$ un anneau.

1. Il existe un seul élément 1_A vérifiant la propriété (A3) de la définition précédente. En effet, si u_1, u_2 sont deux éléments de A tels que :

$$\forall x \in G \quad x * u_1 = x = u_1 * x \text{ et } x * u_2 = x = u_2 * x$$

alors :

$$u_1 = u_1 * u_2 = u_2.$$

Cet élément 1_A est appelé élément unité de l'anneau $(A, +, \times)$.

2. L'élément 0_A est absorbant, i.e. :

$$\forall x \in A \quad x \times 0_A = 0_A \times x = 0_A .$$

En effet, si x est un élément de A , alors :

$$0_A \times x = (0_A + 0_A) \times x = 0_A \times x + 0_A \times x .$$

En ajoutant $-(0_A \times x)$ à chaque membre, il vient $0_A = 0_A \times x$.

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 $x \in A$, $(-1_A) \times x = -x$. En effet, si x est un élément de A , alors

$$0_A = 0_A \cdot x = (1_A + (-1)_A) \times x = 1_A \times x + (-1_A) \times x = x + (-1_A) \times x$$

En ajoutant $-x$ à chaque membre, il vient $(-1_A) \times x = -x$.

10.2. Définition d'un anneau commutatif

Définition 112. — Soit $(A, +, \times)$ un anneau. Si 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.

10.3. Exemples d'anneaux

Exemple 113. — Les ensembles de nombres livrent les anneaux commutatifs suivants.

$$(\mathbf{Z}, +, \times) \quad (\mathbf{Q}, +, \times) \quad (\mathbf{R}, +, \times) \quad (\mathbf{C}, +, \times)$$

Exemple 114. — Si E est un \mathbf{R} -espace vectoriel alors $(\mathcal{L}(E), +, \circ)$ 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 .

Exemple 115. — Si n est un entier tel que $n \geq 2$, alors $(\mathcal{M}_n(\mathbf{K}), +, \times)$ est un anneau non commutatif. Son élément neutre pour la multiplication \times est la matrice I_n .

Exemple 116. — Si \mathbf{K} est un corps (i.e. un anneau distinct de $\{0\}$, dans lequel tout élément non nul est inversible pour la multiplication), alors $(\mathbf{K}[X], +, \times)$ est un anneau commutatif.

11. Rappels sur les sous-anneaux

11.1. Définition d'un sous-anneau

Définition 117. — 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 , i.e. :

$$\forall (x, y) \in B^2 \quad x + y \in B \quad \text{et} \quad x \times y \in B .$$

(A3) B est stable par passage à l'opposé, i.e. :

$$\forall x \in B \quad -x \in B .$$

Proposition 118. — Soit $(A, +, \times)$ un anneau et soit B un sous-anneau de $(A, +, \times)$. Alors les applications induites :

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

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

11.2. Caractérisation des sous-anneaux

Proposition 119. — 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.

- (a) B contient 1_A , i.e. $1_A \in B$.
- (b) B est stable par somme tordue, i.e. :

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

- (c) B est stable pour la loi \times , i.e. :

$$\forall (x, y) \in B^2 \quad x \times y \in B .$$

Exercice 120. — Soient un entier ≥ 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 $(\mathbf{C}, +, \times)$.

12. Rappels sur les morphismes d'anneaux

12.1. Définition d'un morphisme d'anneaux

Définition 121. — Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux. Une application :

$$f : (A, +_A, \times_A) \longrightarrow (B, +_B, \times_B)$$

est un morphisme d'anneaux si les trois propriétés suivantes sont vérifiées.

- (a) f respecte les additions, i.e. :

$$\forall (x, y) \in A^2 \quad f(x +_A y) = f(x) +_B f(y) .$$

- (b) f respecte les multiplications, i.e. :

$$\forall (x, y) \in A^2 \quad f(x \times_A y) = f(x) \times_B f(y) .$$

- (c) f respecte les neutres pour la multiplication, i.e. :

$$f(1_A) = 1_B .$$

12.2. Exemples de morphismes d'anneaux

Exemple 122. — L'identité $\text{id}_{\mathbf{Z}}$ est l'unique morphisme d'anneaux de $(\mathbf{Z}, +, \times)$ dans $(\mathbf{Z}, +, \times)$.

Exemple 123. — Soient $n \in \mathbf{N}^*$ et $M \in \mathcal{M}_n(\mathbf{R})$. L'application :

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

est un morphisme d'anneaux.

Exercice 124. — L'application transposée :

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

est-elle un automorphisme d'anneau ?

12.3. Composition de morphismes d'anneaux

Proposition 125. — Soient $(A_1, +_1, \times_1)$, $(A_2, +_2, \times_2)$, $(A_3, +_3, \times_3)$ trois anneaux et :

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

deux morphismes d'anneaux. Alors l'application :

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

est un morphisme d'anneaux.

12.4. Isomorphisme d'anneaux

Définition 126. — Un morphisme d'anneaux qui est bijectif est appelé isomorphisme d'anneaux.

Exemple 127. — Soient E un \mathbf{R} -espace vectoriel de dimension finie $n \geqslant$, muni d'une base \mathcal{B} . L'application :

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

est un isomorphisme d'anneaux.

Proposition 128. — 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 :

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

est un isomorphisme d'anneaux.

Démonstration.

- Soit $(y_1, y_2) \in B^2$.

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

où $(*)$ provient du fait que f est un morphisme d'anneaux.

- En reprenant le calcul précédent, en échangeant $+$ par \times , il vient :

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

- Notons 1_A et 1_B les éléments neutres pour les multiplications 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 $1_A = f^{-1}(1_B)$.

□

13. Compléments sur les anneaux

13.1. Produit d'un nombre fini d'anneaux

Proposition 129. — Soient un entier $n \geq 2$ 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 :

$$+ \left| \begin{array}{l} \left(\prod_{k=1}^n A_k \right) \times \left(\prod_{k=1}^n A_k \right) \longrightarrow \prod_{k=1}^n A_k \\ ((a_1, \dots, a_n), (b_1, \dots, b_n)) \longmapsto (a_1 +_1 b_1, \dots, a_n +_n b_n) \end{array} \right.$$

et :

$$\times \left| \begin{array}{l} \left(\prod_{k=1}^n A_k \right) \times \left(\prod_{k=1}^n A_k \right) \longrightarrow \prod_{k=1}^n A_k \\ ((a_1, \dots, a_n), (b_1, \dots, b_n)) \longmapsto (a_1 \times_1 b_1, \dots, a_n \times_n b_n). \end{array} \right.$$

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 130. — 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 131. — 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 ?

13.2. Définition d'un idéal d'un anneau commutatif

Définition 132. — Soient $(A, +, \times)$ un anneau commutatif et I une partie de A . On dit que I est un idéal de A si les deux propriétés suivantes sont vérifiées.

- (a) I est un sous-groupe de $(A, +)$.
- (b) 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 133. — Si $(A, +, \times)$ est un anneau commutatif, alors $\{0_A\}$ et A sont des idéaux de A , appelés idéaux triviaux.

Exercice 134. — 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 ?
3. On suppose que $(A, +, \times)$ un corps commutatif. Quels sont alors ses idéaux ?

13.3. Caractérisation des idéaux

Proposition 135. — Pour montrer que I est un idéal d'un anneau commutatif $(A, +, \times)$, il suffit de vérifier les trois propriétés suivantes.

(a) I est non vide.

(b) I est stable par addition tordue, i.e. :

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

(c) I est absorbant, i.e. :

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

13.4. Exemples d'idéaux

Exemple 136. — L'ensemble :

$$I := \{f \in \mathcal{C}^0(\mathbf{R}, \mathbf{R}) : f(1) = 0\}$$

est un idéal de l'anneau $(\mathcal{C}^0(\mathbf{R}, \mathbf{R}), +, \times)$.

Exemple 137. — L'ensemble :

$$I := \{(u_n)_{n \in \mathbf{N}} \in \mathbf{R}^{\mathbf{N}} : \exists N \in \mathbf{N}, \forall n \geq N, u_n = 0\}$$

est un idéal de $(\mathbf{R}^{\mathbf{N}}, +, \times)$.

Exercice 138. — Soit $(A, +, \times)$ un anneau commutatif.

1. Soit $(I_j)_{j \in J}$ une famille d'idéaux de A . Démontrer que leur intersection :

$$\bigcap_{j \in J} I_j := \{x \in A : \forall j \in J \quad x \in I_j\}$$

est un idéal de A .

2. Soient un entier $r \geq 2$ et I_1, I_2, \dots, I_r des idéaux de A . Démontrer que leur somme :

$$I_1 + I_2 + \dots + I_r := \left\{ x_1 + x_2 + \dots + x_r : (x_1, x_2, \dots, x_r) \in \prod_{j=1}^r I_j \right\}$$

est un idéal de A .

3. Soient I, J deux idéaux de A . Posons :

$$IJ := \bigcup_{n \in \mathbf{N}^*} \left\{ \sum_{i=1}^n a_i \times b_i : (a_1, \dots, a_n) \in I^n \text{ et } (b_1, \dots, b_n) \in J^n \right\}.$$

Démontrer que IJ est un idéal de A . A-t-on $IJ = I \cap J$?

13.5. Le noyau d'un morphisme d'anneaux commutatifs est un idéal de la source

Proposition 139. — Soit $f : (A, +_A, \times_A) \longrightarrow (B, +_B, \times_B)$ un morphisme d'anneaux commutatifs. Alors :

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

est un idéal de A .

13.6. Idéal engendré par un élément

Proposition 140. — Soit $(A, +, \times)$ un anneau et $x \in A$. Alors :

$$xA := \{x \times a : a \in A\} \quad [\text{idéal de } A \text{ engendré par } x]$$

est un idéal de A , que l'on appelle « idéal engendré par x ».

Exemple 141. — Démontrer que l'idéal :

$$I := \{f \in \mathcal{C}^0(\mathbf{R}, \mathbf{R}) : f(1) = 0\}$$

de l'anneau $(\mathcal{C}^0(\mathbf{R}, \mathbf{R}), +, \times)$ (cf. exemple 136) n'est pas engendré par un élément, i.e. qu'il n'existe pas de fonction $f \in \mathcal{C}^0(\mathbf{R}, \mathbf{R})$ telle que :

$$I = f \mathcal{C}^0(\mathbf{R}, \mathbf{R}) := \{fg : g \in \mathcal{C}^0(\mathbf{R}, \mathbf{R})\} .$$

Exemple 142. — Démontrer :

$$I := \{P \in \mathbf{R}[X] : P(1) = 0\}$$

est un idéal de l'anneau de l'anneau $(\mathbf{R}[X], +, \times)$, qui est engendré par un élément, i.e. qu'il existe un polynôme $P \in \mathbf{R}[X]$ tel que :

$$I = P \mathbf{R}[X] := \{PQ : Q \in \mathcal{C}^0(\mathbf{R}, \mathbf{R})\} .$$

13.7. Divisibilité dans un anneau commutatif intègre

Définition 143. — Soit $(A, +, \times)$ un anneau commutatif intègre. On dit que $x \in A$ divise $y \in A$, et on note $x \mid y$, si :

$$\exists q \in A \quad y = x \times q .$$

Si tel est le cas, alors l'élément q de A est unique.

Proposition 144. — Soit $(A, +, \times)$ un anneau commutatif intègre et $(x, y) \in A^2$. Alors :

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

14. Idéaux de \mathbf{Z}

14.1. Sous-groupes additifs de \mathbf{Z} versus idéaux de \mathbf{Z}

Lemme 145. — Soit I une partie de \mathbf{Z} . Alors :

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

14.2. Description des idéaux de \mathbf{Z}

Théorème 146. —

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 générateur de I , tel que $I = a\mathbf{Z}$.

14.3. PGCD d'un nombre fini d'entiers en termes d'idéaux

Proposition 147. — Soient un entier $r \geq 2$ et $(a_1, a_2, \dots, a_r) \in (\mathbf{Z}^*)^r$. Alors :

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

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

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

14.4. Relation de Bézout pour le PGCD d'un nombre fini d'entiers

Corollaire 148. — Soient un entier $r \geq 2$ et $(a_1, a_2, \dots, a_r) \in (\mathbf{Z}^*)^r$. 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 149. — Soient un entier $r \geq 2$ et $(a_1, a_2, \dots, a_r) \in (\mathbf{Z}^*)^r$. Démontrer que $\bigcap_{i=1}^r a_i\mathbf{Z}$ est un idéal de \mathbf{Z} et que son générateur est le PPCM $a_1 \vee a_2 \vee \dots \vee a_r$ des entiers a_1, a_2, \dots, a_r .

15. L'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \times)$

Notation. — Dans cette partie, n désigne un entier naturel non nul.

Théorème 150. — Soit $n \in \mathbf{N}^*$. Posons :

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

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 $\bar{0}$ et l'élément neutre multiplicatif est $\bar{1}$.

Exercice 151. — Résoudre l'équation :

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

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

15.1. Inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$

Rappel 152. — Soit $(A, +, \times)$ un anneau.

1. Un élément $x \in A$ est dit inversible si :

$$(*) \quad \exists y \in A, \quad x \times y = y \times x = 1_A.$$

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 :

$$\times \left| \begin{array}{ll} U(A) \times U(A) & \longrightarrow U(A) \\ (x, y) & \longmapsto x \times y \end{array} \right.$$

est bien définie et $(U(A), \times)$ est un groupe (non nécessairement abélien), appelé groupe des inversibles de A .

Théorème 153. — Soit $n \in \mathbf{N}^*$. Alors :

$$U(\mathbf{Z}/n\mathbf{Z}) = \{\bar{a} \in \mathbf{Z}/n\mathbf{Z} : a \wedge n = 1\} .$$

Soit $a \in \mathbf{Z}$ tel que $a \wedge n = 1$. D'après le théorème de Bézout :

$$\exists (u, v) \in \mathbf{Z}^2 \quad a \times u + n \times v = 1 .$$



Un tel couple peut être calculé « en remontant l'algorithme d'Euclide », par exemple. Alors :

$$\bar{a}^{-1} = \bar{u} \quad [\text{identité dans } \mathbf{Z}/n\mathbf{Z}] .$$

Remarque 154. — Soient $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}$. Alors :

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

15.2. CNS pour que $\mathbf{Z}/n\mathbf{Z}$ soit un corps

Rappel 155. — 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 156. — 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 157. — Pour tout nombre premier p , on note \mathbf{F}_p le corps $(\mathbf{Z}/p\mathbf{Z}, +, \times)$.

Remarque 158. — Soit p un nombre premier et \mathbf{K} un corps à p éléments.

1. Il existe un unique morphisme d'anneaux de \mathbf{Z} dans \mathbf{K} , donné par :

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

L'application f est surjective car son image est un sous-groupe non trivial de $(\mathbf{K}, +)$, groupe de cardinal p premier (cf. théorème de Lagrange).

2. 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 $\text{Ker}(f) = n\mathbf{Z}$.
3. On démontre alors que l'application :

$$\bar{f} \left| \begin{array}{ll} \mathbf{Z}/n\mathbf{Z} & \longrightarrow \mathbf{K} \\ \bar{a} & \longmapsto a \mathbf{1}_{\mathbf{K}} \end{array} \right.$$

est une application bien définie, qui est un isomorphisme d'anneaux. Nous en déduisons $n = p$.

4. Nous avons démontré que les corps \mathbf{F}_p et \mathbf{K} sont isomorphes.
5. On vérifie sans peine que l'application g est l'unique morphisme de corps entre \mathbf{F}_p et \mathbf{K} . Le corps à p éléments \mathbf{F}_p est donc unique à unique isomorphisme près.

Remarque 159. — Soit p un nombre premier. Comme le \mathcal{F}_p est un corps, le groupe des unités de \mathbf{F}_p est :

$$(U(\mathbf{F}_p), \times) = (\mathbf{F}_p \setminus \{0_{\mathbf{F}_p}\}, \times)$$

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

Exemple 160. — Le nombre 43 étant premier, $\overline{34} \neq \overline{0}$ est inversible dans le corps $\mathbf{Z}/43\mathbf{Z}$. Calculons :

$$\overline{34}^{-1} = \overline{17}^{-1} \times \overline{2}^{-1}.$$

Nous allons calculer séparément $\overline{17}^{-1}$ et $\overline{2}^{-1}$.

- Dans $\mathbf{Z}/43\mathbf{Z}$, on observe que : $\overline{2} \times \overline{22} = \overline{1}$. Donc $\overline{2}^{-1} = \overline{22}$.
- Comme aucun nombre entier a tel que $\overline{a} \times \overline{17} = \overline{1}$ ne nous apparaît immédiatement, nous allons calculer une relation de Bézout liant 17 et 43 pour déterminer $\overline{17}^{-1}$.

Commençons par appliquer l'algorithme d'Euclide pour calculer le PGCD de 17 et 53 (que nous savons valoir 1) :

$$\begin{aligned} 43 &= 2 \times 17 + 9 \\ 17 &= 1 \times 9 + 8 \\ 9 &= 1 \times 8 + 1. \end{aligned}$$

En « remontant ses divisions euclidiennes successives », il vient :

$$\begin{aligned} 1 &= 9 - 1 \times 8 \\ &= 9 - 1 \times (17 - 1 \times 9) = 2 \times 9 - 1 \times 17 \\ &= 2 \times (43 - 2 \times 17) - 1 \times 17 = 2 \times 43 - 5 \times 17. \end{aligned}$$

De la relation de Bézout :

$$2 \times 43 - 5 \times 17 = 1$$

nous tirons $\overline{17}^{-1} = \overline{-5}$.

Des deux points précédents, nous déduisons que :

$$\overline{34}^{-1} = \overline{2}^{-1} \times \overline{17}^{-1} = \overline{22} \times (\overline{-5}) = \overline{19}.$$

Exercice 161. — Quels sont les inverses de $\overline{4}$ dans $\mathbf{Z}/5\mathbf{Z}$ et de $\overline{16}$ dans $\mathbf{Z}/17\mathbf{Z}$?

Exercice 162. — Résoudre l'équation :

$$x^2 + x + \overline{1} = \overline{0}$$

d'inconnue $\mathbf{Z}/37\mathbf{Z}$.

Exercice 163. — Soit $n \in \mathbf{N}^*$.

1. Quels sont les éléments inversibles de l'anneau $\mathbf{Z}/2^n\mathbf{Z}$?
2. Calculer le cardinal de $U(\mathbf{Z}/2^n\mathbf{Z})$.

15.3. Théorème des restes chinois

Lemme 164. — Soient $n_1, \dots, n_r \in \mathbf{N}^*$ deux à deux premiers entre eux et $x \in \mathbf{Z}$.

(a) Pour tout $i \in \llbracket 1, r \rrbracket$, $n_i \wedge \prod_{\substack{j=1 \\ j \neq i}}^r n_j = 1$.

(b) Si tous les entiers n_1, \dots, n_r divisent x alors $\prod_{j=1}^r n_j$ divise x .

Démonstration. Soit p un nombre premier.

(a) Soit $i \in \llbracket 1, r \rrbracket$.

- Supposons que p divise n_i . Alors p ne divise aucun des entiers $n_1, \dots, n_{i-1}, n_{i+1}, \dots, n_r$, puisque chacun d'entre eux est premier avec n_i . Ainsi :

$$v_p \left(n_i \wedge \prod_{\substack{j=1 \\ j \neq i}}^r n_j \right) = \min \left\{ v_p(n_i), \underbrace{\sum_{\substack{j=1 \\ j \neq i}}^r v_p(n_j)}_{=0} \right\} = 0.$$

- Supposons que p ne divise pas n_i . Alors :

$$v_p \left(n_i \wedge \prod_{\substack{j=1 \\ j \neq i}}^r n_j \right) = \min \left\{ \underbrace{v_p(n_i)}_{=0}, \sum_{\substack{j=1 \\ j \neq i}}^r v_p(n_j) \right\} = 0.$$

Ainsi, pour tout premier p , $v_p \left(n_i \wedge \prod_{\substack{j=1 \\ j \neq i}}^r n_j \right) = 0$, donc $n_i \wedge \prod_{\substack{j=1 \\ j \neq i}}^r n_j = 1$.

(b) Supposons que n_1, \dots, n_r divisent x .

- Supposons qu'il existe $i \in \llbracket 1, r \rrbracket$ tel que $p \mid n_i$. Alors p ne divise aucun des entiers $n_1, \dots, n_{i-1}, n_{i+1}, \dots, n_r$, puisque chacun d'entre eux est premier avec n_i . Ainsi :

$$v_p \left(\prod_{j=1}^r n_j \right) = \sum_{j=1}^r v_p(n_j) = v_p(n_i) + \underbrace{\sum_{\substack{j=1 \\ j \neq i}}^r v_p(n_j)}_{=0} = v_p(n_i) \leq v_p(x)$$

la dernière inégalité découlant de $n_i \mid x$.

- Supposons à présent que p ne divise aucun des entiers n_1, \dots, n_r . Alors :

$$v_p \left(\prod_{j=1}^r n_j \right) = \underbrace{\sum_{j=1}^r v_p(n_j)}_{=0} = 0 \leq v_p(x).$$

Ainsi, pour tout nombre premier p , $v_p \left(\prod_{j=1}^r n_j \right) \leq v_p(x)$, donc $\prod_{j=1}^r n_j \mid x$.

□

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

Théorème 165. — Soient un entier $r \geq 2$ et des entiers $n_1 \geq 1, n_2 \geq 1, \dots, n_r \geq 1$ deux-à-deux premiers entre eux. L'application :

$$\varphi \left\{ \begin{array}{l} \mathbf{Z}/n_1 n_2 \dots n_r \mathbf{Z} \longrightarrow (\mathbf{Z}/n_1 \mathbf{Z}) \times (\mathbf{Z}/n_2 \mathbf{Z}) \times \dots \times (\mathbf{Z}/n_r \mathbf{Z}) \\ \bar{a}^{[n_1 n_2 \dots n_r]} \longmapsto (\bar{a}^{[n_1]}, \bar{a}^{[n_2]}, \dots, \bar{a}^{[n_r]}) \end{array} \right.$$

est bien définie et est un isomorphisme d'anneaux.

Corollaire 166. — Soient un entier $r \geq 2$ et des entiers $n_1 \geq 1, n_2 \geq 1, \dots, n_r \geq 1$ deux-à-deux premiers entre eux.

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

$$(S) \quad \begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

d'inconnue $x \in \mathbf{Z}$ admet une unique solution modulo $n_1 n_2 \dots n_r$.

(b) Si u_1, \dots, u_r sont des nombres entiers tels que :

- $\bar{u}_1^{[n_1]}$ est l'inverse de $\overline{n_2 n_3 n_4 \dots n_r}^{[n_1]}$ dans $\mathbf{Z}/n_1 \mathbf{Z}$
- $\bar{u}_2^{[n_2]}$ est l'inverse de $\overline{n_1 n_3 n_4 \dots n_r}^{[n_2]}$ dans $\mathbf{Z}/n_2 \mathbf{Z}$
- $\bar{u}_3^{[n_3]}$ est l'inverse de $\overline{n_1 n_2 n_4 \dots n_r}^{[n_3]}$ dans $\mathbf{Z}/n_3 \mathbf{Z}$
- ...
- $\bar{u}_r^{[n_r]}$ est l'inverse de $\overline{n_1 n_2 n_3 \dots n_{r-1}}^{[n_r]}$ dans $\mathbf{Z}/n_r \mathbf{Z}$

alors :

$$x_0 := \sum_{i=1}^r a_i \times \left(u_i \times \prod_{\substack{j=1 \\ j \neq i}}^r n_j \right)$$

est une solution particulière de (S). L'ensemble solution de (S) est donc $x_0 + n_1 n_2 \dots n_r \mathbf{Z}$.

Éléments de démonstration.

(a) L'assertion est une conséquence directe de la bijectivité de l'application :

$$\varphi \left\{ \begin{array}{l} \mathbf{Z}/n_1 n_2 \dots n_r \mathbf{Z} \longrightarrow (\mathbf{Z}/n_1 \mathbf{Z}) \times (\mathbf{Z}/n_2 \mathbf{Z}) \times \dots \times (\mathbf{Z}/n_r \mathbf{Z}) \\ \bar{a}^{[n_1 n_2 \dots n_r]} \longmapsto (\bar{a}^{[n_1]}, \bar{a}^{[n_2]}, \dots, \bar{a}^{[n_r]}) \end{array} \right.$$

livrée par le théorème des restes chinois.

(b) Soit $i \in \llbracket 1, r \rrbracket$. Nous observons que :

$$\forall k \in \llbracket 1, r \rrbracket \quad u_i \times \prod_{\substack{j=1 \\ j \neq i}}^r n_j \equiv \delta_{i,k} \pmod{n_k}.$$

Comme la relation de congruence modulo un entier est compatible avec l'addition et la multiplication, il vient :

$$\forall k \in \llbracket 1, r \rrbracket \quad x_0 := \sum_{i=1}^r a_i \times \left(u_i \times \prod_{\substack{j=1 \\ j \neq i}}^r n_j \right) \equiv \sum_{i=1}^r a_i \times \delta_{i,k} \equiv a_k \pmod{n_k}.$$

□

Remarque 167. — Le nom « théorème des restes chinois » attribué au théorème 166 pourrait trouver son origine dans l'énoncé suivant, qui figure dans le livre « Sunzi suanjing » (traduction : « classique mathématique de Sunzi ») du mathématicien et astronome chinois Sunzi (qui n'est pas le général chinois auteur de *L'art de la guerre*), datant du 3^{ème}-4^{ème} 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 ?

La question nous invite à étudier le système de congruences simultanées :

$$(S) \quad \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

d'inconnue $x \in \mathbf{Z}$.

(a) Remarquons que les nombres premiers distincts 3, 5, 7 sont deux à deux premiers entre eux. Le système (S) possède donc une unique solution modulo $3 \times 5 \times 7 = 105$.

(b) Comme :

$$12 \times 3 + (-1) \times 5 \times 7 = 1 \quad ; \quad (-4) \times 5 + 1 \times 3 \times 7 = 1 \quad ; \quad (-2) \times 7 + 3 \times 5 = 1$$

il vient :

$$\begin{cases} (-1) \times 5 \times 7 \equiv 1 \pmod{3} \\ (-1) \times 5 \times 7 \equiv 0 \pmod{5} \\ (-1) \times 5 \times 7 \equiv 0 \pmod{7} \end{cases} \quad \begin{cases} 1 \times 3 \times 7 \equiv 0 \pmod{3} \\ 1 \times 3 \times 7 \equiv 1 \pmod{5} \\ 1 \times 3 \times 7 \equiv 0 \pmod{7} \end{cases} \quad \begin{cases} 3 \times 5 \equiv 0 \pmod{3} \\ 3 \times 5 \equiv 0 \pmod{5} \\ 3 \times 5 \equiv 1 \pmod{7} \end{cases}$$

puis :

$$2 \times ((-1) \times 5 \times 7) + 3 \times (1 \times 3 \times 7) + 2 \times (3 \times 5) = 23$$

est solution particulière de (S).

(c) L'ensemble solution de (S) est donc $23 + 105\mathbf{Z}$.

Exercice 168. — Résoudre le système de congruences simultanées :

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{11} \end{cases}$$

d'inconnue $x \in \mathbf{Z}$.

Exercice 169. — Résoudre le système de congruences simultanées :

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 2 \pmod{6} \\ x \equiv 3 \pmod{7} \end{cases}$$

d'inconnue $x \in \mathbf{Z}$.

15.4. Théorème d'Euler

Définition 170. — *L'application :*

$$\varphi \quad \begin{array}{l} \mathbf{N}^* \longrightarrow \mathbf{N}^* \\ n \longmapsto \text{card}(U(\mathbf{Z}/n\mathbf{Z})) = \text{card}(\{a \in \llbracket 1, n \rrbracket : a \wedge n = 1\}) \end{array}$$

est appelée *indicatrice d'Euler*.

Théorème 171. — Soient $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}$ tel que $a \wedge n = 1$. Alors :

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad [\text{théorème d'Euler}] .$$

Remarque 172. — Si $n = p$ est un nombre premier, le théorème d'Euler se spécialise en le petit théorème de Fermat :

$$\forall a \in \llbracket 1, p-1 \rrbracket \quad a^{p-1} \equiv 1 \pmod{p} .$$

Proposition 173. — Soient $(A_1, +_1, \times_1), \dots, (A_p, +_p, \times_p)$ des anneaux et $\left(\prod_{i=1}^p A_i, +, \times\right)$ l'anneau produit.

Alors :

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

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

Théorème 174. — On note \mathbf{P} l'ensemble des nombres premiers.

(a) $\forall (n, m) \in \mathbf{N}_{\geq 2} \times \mathbf{N}_{\geq 2} \quad n \wedge m = 1 \implies \varphi(n \times m) = \varphi(n) \times \varphi(m)$

(b) $\forall p \in \mathbf{P} \quad \forall k \in \mathbf{N}^* \quad \varphi(p^k) = (p-1) \times p^{k-1}$

(c) Pour tout $n \in \mathbf{N}_{\geq 2}$:

$$\varphi(n) = n \times \prod_{k=1}^r \left(1 - \frac{1}{p_k}\right) \quad \text{où } p_1, \dots, p_r \text{ sont les diviseurs premiers de } n .$$

Exercice 175. — Calculer $\varphi(4040)$.

Exercice 176. — Démontrer que :

$$10^6 \equiv 1 \pmod{7} \quad \text{et} \quad \sum_{k=1}^{12} 10^{10^k} \equiv -1 \pmod{7} .$$

Exercice 177. — Soit $p \in \mathbf{N}^*$ un entier premier. Démontrer :

$$(p-1)! \equiv -1 \pmod{p} \quad [\text{théorème de Wilson}] .$$

16. L'anneau $(\mathbf{K}[X], +, \times)$

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


16.1. Description des idéaux de $\mathbf{K}[X]$

Proposition 178. — Soit $A \in \mathbf{K}[X]$. L'ensemble :

$$A\mathbf{K}[X] := \{AP : P \in \mathbf{K}[X]\} \quad [\text{ensemble des multiples de } A]$$

est un idéal de $\mathbf{K}[X]$.

Théorème 179. — 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 unitaire* de I , tel que $I = A\mathbf{K}[X]$.

 Soient I un idéal de $\mathbf{K}[X]$ distinct de $\{0_{\mathbf{K}[X]}\}$ et A son générateur unitaire. D'après la démonstration du théorème précédent, le polynôme A est le polynôme de plus petit degré parmi les polynômes unitaires de $I \setminus \{0_{\mathbf{K}[X]}\}$.

16.2. PGCD d'un nombre fini de polynômes

Proposition 180. — Soient un entier $r \geq 2$ et $(A_1, A_2, \dots, A_r) \in (\mathbf{K}[X] \setminus \{0_{\mathbf{K}[X]}\})^r$. Alors :

$$A_1\mathbf{K}[X] + A_2\mathbf{K}[X] + \dots + A_r\mathbf{K}[X] := \{A_1P_1 + A_2P_2 + \dots + A_rP_r : (P_1, P_2, \dots, P_r) \in \mathbf{K}[X]^r\}$$

est un idéal. Son générateur unitaire est le PGCD des polynômes A_1, A_2, \dots, A_r , i.e. :

$$A_1\mathbf{K}[X] + A_2\mathbf{K}[X] + \dots + A_r\mathbf{K}[X] = (A_1 \wedge A_2 \wedge \dots \wedge A_r)\mathbf{K}[X].$$

16.3. Relation de Bézout pour le PGCD d'un nombre fini de polynômes

Corollaire 181. — Soient un entier $r \geq 2$ et $(A_1, A_2, \dots, A_r) \in (\mathbf{K}[X])^r$. Alors :

$$\exists (P_1, P_2, \dots, P_r) \in \mathbf{K}[X]^r \quad A_1 \wedge A_2 \wedge \dots \wedge A_r = A_1P_1 + A_2P_2 + \dots + A_rP_r.$$


Exercice 182. — Soient un entier $r \geq 2$ 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 unitaire est le PPCM $P_1 \wedge P_2 \wedge \dots \wedge P_r$ des polynômes A_1, A_2, \dots, A_r .

16.4. Notion de polynôme irréductible sur un corps

Définition 183. — Soit $P \in \mathbf{K}[X]$. P est dit *irréductible sur \mathbf{K}* si :

$$\left\{ \begin{array}{l} \deg(P) \geq 1 \\ \text{et} \\ \forall (P_1, P_2) \in \mathbf{K}[X]^2 \quad P = P_1P_2 \implies (P_1 \in \mathbf{K}_0[X] \text{ ou } P_2 \in \mathbf{K}_0[X]) \end{array} \right.$$

Le polynôme P est dit *réductible sur \mathbf{K}* , s'il n'est pas irréductible sur \mathbf{K} .

 On peut donc penser à un polynôme de $\mathbf{K}[X]$, irréductible sur \mathbf{K} , comme à un polynôme non constant, qui n'admet pas de factorisation non triviale dans $\mathbf{K}[X]$.

Soit $P \in \mathbf{K}[X]$. Soit L un sur-corps de \mathbf{K} qui est un sous-corps de \mathbf{C} : $\mathbf{K} \subset L \subset \mathbf{C}$. Le polynôme P peut être irréductible sur \mathbf{K} , mais réductible sur L . Par exemple, le polynôme $X^2 + 1$ est irréductible sur \mathbf{R} , mais réductible sur \mathbf{C} puisqu'il se factorise en :



$$X^2 + 1 = (X - i)(X + i)$$

dans $\mathbf{C}[X]$.

16.5. Irréductibles de $\mathbf{K}[X]$ de degré 1, 2, 3

Exercice 184. — Démontrer que tout polynôme de $\mathbf{K}[X]$ de degré 1 est irréductible sur \mathbf{K} .

Exercice 185. — Soit P un polynôme de $\mathbf{K}[X]$ tel que $\deg(P) \in \{2, 3\}$. Démontrer que P est irréductible sur \mathbf{K} si et seulement si il ne possède pas de racine dans \mathbf{K} .

Exercice 186. — Démontrer qu'un polynôme de $\mathbf{R}[X]$, de degré impair supérieur ou égal à 3, n'est pas irréductible sur \mathbf{R} .

Exercice 187. — Donner un exemple de polynôme P dans $\mathbf{R}[X]$ qui n'admet pas de racine dans \mathbf{R} , et qui n'est pas irréductible sur \mathbf{R} .

16.6. Deux résultats de primalité relative dans $\mathbf{K}[X]$

Lemme 188. — Soient A et B des polynômes de $\mathbf{K}[X]$ tels que $A \wedge B = 1$. Alors, pour tout $(n, m) \in \mathbf{N}^2$, $A^n \wedge B^m = 1$.

Lemme 189. — Soient A, B_1, \dots, B_n des polynômes de $\mathbf{K}[X]$ tels que A est premier avec chacun des polynômes B_1, \dots, B_n . Alors $A \wedge \prod_{k=1}^n B_k = 1$.

16.7. Décomposition d'un polynôme de $\mathbf{K}[X]$ en produit de polynômes irréductibles sur \mathbf{K}

Lemme 190. — Soient A et B des polynômes irréductibles sur \mathbf{K} , unitaires et distincts. Alors $A \wedge B = 1$.

Démonstration. On raisonne par l'absurde. Supposons donc que $D := A \wedge B \neq 1$. Alors $\deg(D) \geq 1$. Comme D divise A , il existe $Q \in \mathbf{K}[X]$ tel que $A = DQ$. Comme A est irréductible sur \mathbf{K} et $\deg(D) \geq 1$, il vient $Q \in \mathbf{K}_0[X]$. Comme A et D sont unitaires, nous avons $Q = 1$, soit $D = A$. De même, nous établissons $D = B$. Ainsi $A = B$, ce qui contredit une des hypothèses. □

Théorème 191. — Soit $P \in \mathbf{K}[X]$ tel que $\deg(P) \geq 1$.

(a) Il existe $r \in \mathbf{N}^*$, des polynômes $P_1, \dots, P_r \in \mathbf{K}[X]$ irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, des entiers naturels non nuls n_1, \dots, n_r tels que :

$$P = \text{dom}(P) P_1^{n_1} \dots P_r^{n_r} .$$

(b) Cette décomposition de P en produit de facteurs irréductibles est unique à l'ordre près, i.e. étant donnés $s \in \mathbf{N}^*$, des polynômes $Q_1, \dots, Q_s \in \mathbf{K}[X]$ irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, des entiers naturels non nuls m_1, \dots, m_s tels que $P = \text{dom}(P) Q_1^{m_1} \dots Q_s^{m_s}$, alors :

- $r = s$
- il existe une bijection $\sigma : \llbracket 1, r \rrbracket \longrightarrow \llbracket 1, r \rrbracket$ telle que, pour tout $i \in \llbracket 1, r \rrbracket$, $Q_i = P_{\sigma(i)}$ et $m_i = n_{\sigma(i)}$.

Démonstration. Quitte à remplacer P par son normalisé, on peut supposer que $\text{dom}(P) = 1$.

• *Existence.* — On raisonne par récurrence forte sur le degré de P . Pour tout $d \in \mathbf{N}^*$, notons $\mathcal{P}(d)$ le prédicat en la variable d : tout polynôme unitaire de $\mathbf{K}[X]$ de degré d admet une décomposition en produit d'irréductibles, comme dans l'assertion 1 du théorème.

– *Initialisation à $d = 1$.* — Soit $P \in \mathbf{K}[X]$ un polynôme unitaire, tel que $\deg(P) = 1$. Alors P est irréductible sur \mathbf{K} . On peut donc l'écrire sous la forme introduite dans l'assertion 1 du théorème, en posant :

$$r = 1 \quad , \quad P_1 = P \quad , \quad n_1 = 1 .$$

– *Hérédité.* — Soit $d \in \mathbf{N}^*$ fixé. Supposons $\mathcal{P}(k)$ vraie pour tout $k \in \llbracket 1, d \rrbracket$. Soit P un polynôme unitaire de degré $d + 1$.

• Si P est irréductible sur \mathbf{K} , alors on peut l'écrire sous la forme introduite dans l'assertion 1 du théorème, en posant :

$$r = 1 \quad , \quad P_1 = P \quad , \quad n_1 = 1 .$$

- Si P n'est pas irréductible sur \mathbf{K} alors il existe $A, B \in \mathbf{K}[X]$ des polynômes unitaires tels que $P = AB$, $\deg(A) \geq 1$ et $\deg(B) \geq 1$. Puisque :

$$\deg(A) + \deg(B) = \deg(AB) = \deg(P) = d + 1$$

nous en déduisons $\deg(A) \in \llbracket 1, d \rrbracket$ et $\deg(B) \in \llbracket 1, d \rrbracket$. Nous appliquons l'hypothèse de récurrence à A et à B pour obtenir l'existence de $r, s \in \mathbf{N}^*$, de polynômes A_1, \dots, A_r irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, de polynômes B_1, \dots, B_s irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, d'entiers naturels non nuls $n_1, \dots, n_r, m_1, \dots, m_s$ tels que :

$$A = P_1^{n_1} \dots P_r^{n_r} \quad \text{et} \quad B = Q_1^{m_1} \dots Q_s^{m_s} .$$

D'où :

$$P = P_1^{n_1} \dots P_r^{n_r} Q_1^{m_1} \dots Q_s^{m_s} .$$

En regroupant éventuellement les polynômes P_i et Q_j égaux ($i \in \llbracket 1, r \rrbracket, j \in \llbracket 1, s \rrbracket$), nous obtenons une écriture de P comme dans l'assertion 1 du théorème.

- *Unicité.* — On présente uniquement une esquisse de preuve, en étant moins formel que pour l'existence, en raisonnant « par itérations successives ». Soient deux décompositions en produits d'irréductibles de P , comme dans l'assertion 2 du théorème :

$$P_1^{n_1} \dots P_r^{n_r} = P = Q_1^{m_1} \dots Q_s^{m_s} .$$

- Le polynôme P_1 divise le polynôme P (car $n_1 \geq 1$), donc le polynôme $Q_1^{m_1} \dots Q_s^{m_s}$. Le polynôme P_1 ne peut pas être premier avec tous les polynômes Q_1, \dots, Q_s , sinon le théorème de Gauß serait mis en défaut. Par conséquent, quitte à ré-indexer les polynômes Q_1, \dots, Q_s , on peut supposer $P_1 \wedge Q_1 \neq 1$. Alors, d'après le lemme 190, $P_1 = Q_1$. D'après le lemme 190 et le lemme 188, $P_1^{n_1}$ est premier avec les polynômes $Q_2^{m_2}, \dots, Q_s^{m_s}$. Grâce au lemme 189, nous en déduisons que $P_1^{n_1}$ est premier avec le polynôme $Q_2^{m_2} \dots Q_s^{m_s}$. D'après le théorème de Gauß, $P_1^{n_1}$ divise $Q_1^{m_1} = P_1^{m_1}$ et donc $n_1 \leq m_1$. Alors :

$$P_2^{n_2} \dots P_r^{n_r} = Q_1^{m_1 - n_1} \dots Q_s^{m_s} .$$

Si $m_1 > n_1$, alors le polynôme $Q_1 = P_1$ divise le polynôme $P_2^{n_2} \dots P_r^{n_r}$, ce qui n'est pas possible, puisque P_1 est premier avec les polynômes P_2, \dots, P_r (adapter le raisonnement précédent). Ainsi, $n_1 = m_1$ et :

$$P_2^{n_2} \dots P_r^{n_r} = Q_2^{m_2} \dots Q_s^{m_s} .$$

- En itérant ce procédé, on démontre le résultat souhaité. La bijection σ qui figure dans l'assertion 2 du théorème est « cachée » dans les ré-indexations éventuelles des polynômes $Q_j, j \in \llbracket 1, s \rrbracket$.

□

Exercice 192. — Soit $P \in \mathbf{K}[X]$ un polynôme unitaire, de degré supérieur ou égal à 1. On considère la décomposition de P en produit de polynômes irréductibles :

$$P = P_1^{n_1} \dots P_r^{n_r}$$

où $r \in \mathbf{N}^*$, $P_1, \dots, P_r \in \mathbf{K}[X]$ sont des polynômes irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, n_1, \dots, n_r sont des entiers naturels non nuls.

1. Quels sont les diviseurs unitaires de P ?
2. Combien P possède-t-il de diviseurs unitaires ?

16.8. Irréductibles de $\mathbf{C}[X]$ et irréductibles de $\mathbf{R}[X]$ **Théorème 193.** —(a) Soit $P \in \mathbf{C}[X]$. Alors :

$$P \text{ est irréductible sur } \mathbf{C} \iff \deg(P) = 1.$$

(b) Soit $P \in \mathbf{R}[X]$. Alors :

$$P \text{ est irréductible sur } \mathbf{R} \iff \begin{cases} \deg(P) = 1 \\ \text{ou} \\ P \text{ est de degré 2 et de discriminant strictement négatif.} \end{cases}$$

16.9. Décomposition en produit d'irréductibles dans $\mathbf{C}[X]$ **Corollaire 194.** — Soit $P \in \mathbf{C}[X]$ tel que $\deg(P) \geq 1$. La décomposition de P en produit de facteurs irréductibles dans $\mathbf{C}[X]$ est « de la forme » :

$$P = \text{dom}(P) \prod_{k=1}^r (X - \alpha_k)^{n_k}$$

où :

- r est un entier naturel non nul ;
- $\alpha_1, \dots, \alpha_r$ sont des complexes deux-à-deux distincts ;
- n_1, \dots, n_r sont des entiers naturels non nuls.

Démonstration. Il s'agit d'une conséquence des théorèmes 191 et 193. □**Remarque 195.** — L'entier r est le nombre de racines complexes deux-à-deux distinctes de P , les complexes $\alpha_1, \dots, \alpha_r$ sont les racines complexes deux-à-deux distinctes de P et pour tout $k \in \llbracket 1, r \rrbracket$, n_k est l'ordre de multiplicité de la racine α_k de P .**Remarque 196.** — Soit $P \in \mathbf{C}[X]$ de degré supérieur ou égal à 1. Soient $\alpha_1, \dots, \alpha_r$ les racines complexes deux-à-deux distinctes de P et n_1, \dots, n_r leurs multiplicités respectives. Alors, dans le corps des fractions rationnelles $\mathbf{C}(X)$:

$$\frac{P'}{P} = \sum_{k=1}^r \frac{n_k}{X - \alpha_k}.$$

16.10. Décomposition en produit d'irréductibles dans $\mathbf{R}[X]$ **Corollaire 197.** — Soit $P \in \mathbf{R}[X]$ tel que $\deg(P) \geq 1$. La décomposition de P en produit de facteurs irréductibles dans $\mathbf{R}[X]$ est « d'une des formes suivantes »(a) Cas où P n'a aucune racine dans \mathbf{R}

$$P = \text{dom}(P) \prod_{\ell=1}^s (X^2 + a_\ell X + b_\ell)^{m_\ell}$$

(b) Cas où P n'a aucune racine dans $\mathbf{C} \setminus \mathbf{R}$ (i.e. est scindé sur \mathbf{R})

$$P = \text{dom}(P) \prod_{k=1}^r (X - \alpha_k)^{n_k}$$

(c) Cas où P a une racine dans \mathbf{R} et une racine dans $\mathbf{C} \setminus \mathbf{R}$

$$P = \text{dom}(P) \prod_{k=1}^r (X - \alpha_k)^{n_k} \prod_{\ell=1}^s (X^2 + a_\ell X + b_\ell)^{m_\ell}$$

où :

- r et s sont des entiers non nuls ;
- $n_1, \dots, n_r, m_1, \dots, m_s$ sont des entiers non nuls ;
- $\alpha_1, \dots, \alpha_r$ sont des réels deux-à-deux distincts ;
- $(a_1, b_1), \dots, (a_s, b_s)$ sont des couples deux-à-deux distincts de réels tels que pour tout $k \in \llbracket 1, s \rrbracket$, $a_k^2 < 4b_k$.

Démonstration. Il s'agit d'une conséquence des théorèmes 191 et 193. □

Exercice 198. — Décomposer le polynôme $P = X^4 + 16$ en produit d'irréductibles dans $\mathbf{C}[X]$, puis dans $\mathbf{R}[X]$.

Exercice 199. — Soit $n \in \mathbf{N}_{\geq 2}$. Nous posons $P := X^n - 1$.

1. Décomposer P en produit de facteurs irréductibles dans $\mathbf{C}[X]$.
2. En déduire la décomposition de P en produit de facteurs irréductibles dans $\mathbf{R}[X]$, en distinguant deux cas, suivant la parité de n .

17. Algèbres

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

17.1. Définition d'une \mathbf{K} -algèbre

Définition 200. — Soit A un ensemble muni :

- d'une loi de composition notée $+_A$

$$+_A \left| \begin{array}{l} A \times A \longrightarrow A \\ (x, y) \longmapsto x +_A y \end{array} \right.$$

- d'une loi de composition notée \times

$$\times_A \left| \begin{array}{l} A \times A \longrightarrow A \\ (x, y) \longmapsto x \times_A y \end{array} \right.$$

- d'une loi de composition externe à domaine d'opérateurs dans \mathbf{K}

$$\cdot \left| \begin{array}{l} \mathbf{K} \times A \longrightarrow A \\ (\lambda, x) \longmapsto \lambda \cdot x \end{array} \right.$$

On dit que $(A, +_A, \times_A, \cdot)$ 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, \cdot et $\times_{\mathbf{K}}$ vérifient la propriété de compatibilité suivante.

$$\forall (\lambda, \mu, x, y) \in \mathbf{K} \times \mathbf{K} \times A \times A, \quad (\lambda \cdot x) \times_A (\mu \cdot y) = (\lambda \times_{\mathbf{K}} \mu) \cdot (x \times_A y)$$

17.2. Exemples de \mathbf{K} -algèbres

Exemple 201. — Le corps \mathbf{K} est naturellement une \mathbf{K} -algèbre. En effet, $(\mathbf{K}, +_{\mathbf{K}}, \times_{\mathbf{K}}, \cdot_{\mathbf{K}})$ est une \mathbf{K} -algèbre.

Exemple 202. — Soit un entier $n \geq 2$. Soit $n \in \mathbf{N}_{\geq 2}$. Sur $\mathcal{M}_n(\mathbf{K})$, nous disposons d'une addition et d'une multiplications internes et nous avons déjà observé que $(\mathcal{M}_n(\mathbf{K}), +, \times)$ est un anneau. Si l'on définit l'opération \cdot par :

$$\cdot \left| \begin{array}{l} \mathbf{K} \times \mathcal{M}_n(\mathbf{K}) \longrightarrow \mathcal{M}_n(\mathbf{K}) \\ (\lambda, M) \longmapsto \lambda \cdot M := (\lambda \times_{\mathbf{K}} [M]_{i,j})_{1 \leq i,j \leq n} \end{array} \right.$$

alors $(\mathcal{M}_n(\mathbf{K}), +, \cdot)$ est un \mathbf{K} -espace vectoriel, de dimension finie n^2 . On vérifie que $(\mathcal{M}_n(\mathbf{K}), +, \times, \cdot)$ est une \mathbf{K} -algèbre.

Exemple 203. — Soit E un \mathbf{K} espace vectoriel. Sur $\mathcal{L}(E)$, nous disposons d'une addition et d'une multiplications internes et nous avons déjà observé que $(\mathcal{L}(E), +, \circ)$ est un anneau. Si l'on définit l'opération \cdot par :

$$\cdot \left| \begin{array}{l} \mathbf{K} \times \mathcal{L}(E) \longrightarrow \mathcal{L}(E) \\ (\lambda, f) \longmapsto \lambda \cdot f \end{array} \right| \begin{array}{l} E \longrightarrow E \\ x \longmapsto \lambda \cdot f(x) \end{array}$$

alors $(\mathcal{L}(E), +, \cdot)$ est un \mathbf{K} -espace vectoriel. On vérifie que $(\mathcal{L}(E), +, \circ, \cdot)$ est une \mathbf{K} -algèbre.

Exemple 204. — Sur $\mathbf{K}[X]$, 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 :

$$\cdot \left| \begin{array}{l} \mathbf{K} \times \mathbf{K}[X] \longrightarrow \mathbf{K}[X] \\ (\lambda, P) \longmapsto \lambda \cdot P := \sum_{k=0}^{+\infty} \lambda \times_{\mathbf{K}} [P]_k X^k \end{array} \right.$$

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

17.3. Sous-algèbres

Définition 206. — 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 207. — Soit un entier $n \geq 2$. On note $\mathcal{T}_n(\mathbf{K})$ l'ensemble des matrices triangulaires supérieures de $\mathcal{M}_n(\mathbf{K})$. Démontrer que $\mathcal{T}_n(\mathbf{K})$ est une sous-algèbre de $\mathcal{M}_n(\mathbf{K})$.

Exercice 208. — Soit x un nombre réel. Démontrer que $\text{Vect}_{\mathbf{Q}}((x^n)_{n \in \mathbf{N}})$ est une sous- \mathbf{Q} -algèbre de \mathbf{R} .

Proposition 209. — Soit $(A, +, \times, \cdot)$ une \mathbf{K} -algèbre et soit B une sous- \mathbf{K} -algèbre de $(A, +, \times, \cdot)$. Alors les applications induites :

$$+_B \left| \begin{array}{l} B \longrightarrow B \\ (x, y) \longmapsto x + y \end{array} \right. \quad \times_B \left| \begin{array}{l} B^2 \longrightarrow B \\ (x, y) \longmapsto x \times y \end{array} \right. \quad \cdot_B \left| \begin{array}{l} \mathbf{K} \times B \longrightarrow B \\ (\lambda, x) \longmapsto \lambda \cdot x \end{array} \right.$$

sont bien définies et $(B, +_B, \times_B, \cdot_B)$ est une \mathbf{K} -algèbre.

17.4. Morphisme d'algèbres

Définition 210. — *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.

- (a) f est une application \mathbf{K} -linéaire de $(A_1, +_1, \cdot_1)$ vers $(A_2, +_2, \cdot_2)$.
- (b) f est un morphisme d'anneaux de $(A_1, +_1, \times_1)$ et $(A_2, +_2, \times_2)$.

Exemple 211. — Soient $n \in \mathbf{N}_{\geq 2}$ et $M \in \mathcal{M}_n(\mathbf{R})$. On considère de nouveau l'application :

$$\varphi \left\{ \begin{array}{l} (\mathbf{K}[X], +, \circ, \cdot) \longrightarrow (\mathcal{M}_n(\mathbf{R}), +, \times, \cdot) \\ P = \sum_{k=0}^{+\infty} a_k X^k \longmapsto P(M) := \sum_{k=0}^{+\infty} a_k M^k \end{array} \right.$$

L'application φ est un morphisme de \mathbf{R} -algèbres.

Proposition 212. — Soient $(A_1, +_1, \times_1, \cdot_1)$, $(A_2, +_2, \times_2, \cdot_2)$, $(A_3, +_3, \times_3, \cdot_3)$ trois \mathbf{K} -algèbres et

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

deux morphismes de \mathbf{K} -algèbres. Alors l'application :

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

est un morphisme de \mathbf{K} -algèbres.

Définition 213. — Un morphisme de \mathbf{K} -algèbre qui est bijectif est appelé isomorphisme de \mathbf{K} -algèbres.

Exemple 214. — Soit E un \mathbf{R} -espace vectoriel de dimension finie $n \geq 2$, muni d'une base \mathcal{B} . On considère de nouveau l'application :

$$\text{Mat}_{\mathcal{B}}(\cdot) \left\{ \begin{array}{l} (\mathcal{L}(E), +, \circ, \cdot) \longrightarrow (\mathcal{M}_n(\mathbf{R}), +, \times, \cdot) \\ f \longmapsto \text{Mat}_{\mathcal{B}}(f) \end{array} \right.$$

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

Proposition 215. — Soit \mathbf{K} un corps, soient $(A, +_A, \times_A, \cdot_A)$ et $(B, +_B, \times_B, \cdot_B)$ deux \mathbf{K} -algèbres et $f : (A, +_A, \times_A, \cdot_A) \longrightarrow (B, +_B, \times_B, \cdot_B)$ un isomorphisme d'anneaux. Alors la bijection réciproque :

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

est un isomorphisme de \mathbf{K} -algèbres.