Structures algébriques

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 $*$*

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

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

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

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

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

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

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

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

Remarque 2. — 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 appeléle 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

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

6. Si x est un élément de G, alors $\left(x^{-1}\right)^{-1} = x$. 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.

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

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 $S(E)$ des bijections de E dans E muni de la loi $\circ$ est un groupe, appelégroupe des permutations de E. En particulier, pour tout $n \in \mathbf{N}^*$, l'ensemble S_n des bijections de $[\![1,n]\!]$ dans lui-même muni de la loi $\circ$ est un groupe.

Exemple 10. — Soit un entier $n \geqslant 2$. 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 :

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

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 $(S(E),\circ)$ 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 :*

(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

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

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

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

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

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

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

$$A_n := \{\sigma \in S_n \ : \ \varepsilon(\sigma) = 1\} \qquad \text{[groupe alterné d'indice } n\text{]}$$

est un sous-groupe de $(S_n, \circ)$.

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

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

est un sous-groupe de $(S(E), \circ)$.

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

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

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

Exercice 23. — Démontrer que

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

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 :

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

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 $f : G \longrightarrow H$ est un morphisme de groupes si*

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

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

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

3.2. Exemples de morphismes de groupes

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

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

est un morphisme de groupes.

Exemple 28. — L'application

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

est un morphisme de groupes.

Exemple 29. — Soit $n \in \mathbf{N}^*$. Pour tout $\sigma \in S_n$, on pose

$$I(\sigma) := \operatorname{card}\left(\left\{(i,j) \in [\![1,n]\!]^2 \ : \ i<j \text{ et } \sigma(i)>\sigma(j)\right\}\right) \qquad \text{[nombre d'inversions de } \sigma\text{]}$$

La signature

$$\varepsilon \left| \begin{array}{ccc} (S_n,\circ) & \longrightarrow & (\{-1,1\},\times) \\ \sigma & \longmapsto & \varepsilon(\sigma)=(-1)^{I(\sigma)} \end{array} \right.$$

est un morphisme de groupes.

Exemple 30. — Soit n^*. L'application

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

est un morphisme de groupes.

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

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

est-elle un morphisme de groupes ?

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

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

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.*

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

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

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

2. *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.*

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

Proposition 35. — *structures du noyau et de l'image d'un morphisme de groupes Soient $(G,*)$, $(H,\cdot)$ deux groupes et $f\colon G \longrightarrow H$ un morphisme de groupes.*
1. $\mathrm{Ker}\,(f)$ *est un sous-groupe de G.*
2. $\mathrm{Im}\,(f)$ *est un sous-groupe de H.*

Exemple 36. — Soit un entier $n \geqslant 2$. L'application
$$\left|\begin{array}{ccc} (\mathrm{O}_n(\mathbf{R}),\times) & \longrightarrow & (\mathbf{R}^*,\times) \\ M & \longmapsto & \det(M) \end{array}\right.$$
est un morphisme de groupes. Son noyau est noté $\mathrm{SO}_n(\mathbf{R})$, i.e.
$$\mathrm{SO}_n(\mathbf{R}) := \{M \in \mathrm{O}_n(\mathbf{R}) \ : \ \det(M) = 1\} \qquad \text{[groupe spécial orthogonal]}$$

Exercice 37. — On considère l'application
$$\rho \left|\begin{array}{ccc} (\mathbf{R},+) & \longrightarrow & (\mathrm{SO}_2(\mathbf{R}),\times) \\ \theta & \longmapsto & \rho(\theta) := \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \end{array}\right.$$
1. Démontrer que l'application ρ est bien définie et surjective.
2. Démontrer que l'application ρ est un morphisme de groupes et préciser son noyau.

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

Proposition 38. — *Soient $(G,*)$, $(H,\cdot)$ deux groupes et $f\colon G \longrightarrow H$ un morphisme de groupes.*
1. *L'application f est injective si et seulement si* $\mathrm{Ker}\,(f) = \{e_G\}$*, où e_G désigne le neutre de $(G,*)$.*
2. *L'application f est surjective si et seulement si* $\mathrm{Im}\,(f) = H$.

3.6. Composition de morphismes de groupes

Théorème 39. — *Soient $(G_1,*_1)$, $(G_2,*_2)$, $(G_3,*_3)$ trois groupes. Soient $f\colon (G_1,*_1) \longrightarrow (G_2,*_2)$ et $g\colon (G_2,*_2) \longrightarrow (G_3,*_3)$ deux morphismes de groupes. Alors*
$$g \circ f \left|\begin{array}{ccc} (G_1,*_1) & \longrightarrow & (G_3,*_3) \\ x_1 & \longmapsto & g(f(x_1)) \end{array}\right.$$
est un morphisme de groupes.

3.7. Isomorphisme de groupes

Définition 40. — *Soient $(G_1,*_1)$, $(G_2,*_2)$ et $f\colon (G_1,*_1) \longrightarrow (G_2,*_2)$ une application. On dit que f est un isomorphisme de groupes si*
1. *f est un morphisme de groupes ;*
2. *f est bijectif.*

Remarque 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 $\left(\mathbf{R}_+^*,\times\right)$ sont-ils isomorphes ?

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

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

est un morphisme de groupes.

4. Sous-groupes additifs de Z

Rappel 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 :

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

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

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

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

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

Théorème 47. — *Soit H un sous-groupe de $(\mathbf{Z},+)$. Il existe un unique $a\in\mathbf{N}$ tel que*

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

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

5. Sous-groupe engendré par une partie

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.*

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

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

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

5.3. Description du sous-groupe engendré par une partie

Théorème 55. — *Soient $(G,*)$ un groupe et $A \subset G$ une partie non vide de G. Notons A^{-1} l'ensemble des inverses des éléments de A*

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

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

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

5.4. Sous-groupe engendré par un élément

Définition 56. — *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*

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

Proposition 57. — *Soient $(G,*)$ un groupe et $(x, n, m) \in G \times \mathbf{Z} \times \mathbf{Z}$.*

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

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 58. — *Soient $(G,*)$ un groupe et $a \in G$.*

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

5.5. Parties génératrices d'un groupe

Définition 59. — *Soit $(G,*)$ un groupe. Une partie A de G est une partie génératrice si le sous-groupe engendré par A est le groupe G tout entier, i.e. si $G =< A >$.*

Exemple 60. — Le groupe $(\mathbf{Z}, +)$ des entiers relatifs est engendré par l'élément 1.

Exemple 61. — Soit un entier $n \geqslant 2$. Le groupe $(\mathbf{Z}^n, +)$ est engendré par

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

Exemple 62. — Soit un entier $n \geqslant 2$. Le groupe $(S_n, \circ)$ est engendré par les transpositions

$$S_n = < \{(i\ j)\ :\ 1 \leqslant i < j \leqslant n\} > \qquad \left[\text{système générateur à } \binom{n}{2} \text{ éléments}\right]$$

Exemple 63. — Soit un entier $n \geqslant 2$. 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

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

Exercice 64. — Soit un entier $n \geqslant 2$.

1. Soient $a_1, \dots, a_p$ des éléments distincts de $[\![1,n]\!]$ et σ une permutation de $[\![1,n]\!]$. 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 $[\![1,n]\!]$ échangeant 1 et 2 et σ le cycle de longueur n défini par $\sigma := (1\,2\,3\,\dots\,n)$. Démontrer que $\{(1\ 2), \sigma\}$ engendre le groupe $(S_n, \circ)$.

Exercice 65. — 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 66. — 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 $n \geqslant 2$, 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 67. — *Soit $(n,a,b) \in \mathbf{N}^* \times \mathbf{Z} \times \mathbf{Z}$. On dit quea est congru à b modulo n, et on écrit $a \equiv b\ [n]$, si $a - b \in n\mathbf{Z}$.*

Proposition 68. — *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 69. — *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 70. — *Soit $(n,a,b,k) \in \mathbf{N}^* \times \mathbf{Z} \times \mathbf{Z} \times \mathbf{N}^*$. Alors :*

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

Exercice 71. — Démontrer que pour tout $n \in \mathbf{N}$, 5 divise $2^{3n+5} + 3^{n+1}$.

Proposition 72. — *Soit $n \in \mathbf{N}^*$. La relation de congruence modulo n est une relation d'équivalence.*

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

Rappel 73. — Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. Pour tout $x \in E$, on note

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

On rappelle trois propriétés fondamentales des classes d'équivalences.

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

Définition 74. — *Soit $(n, a) \in \mathbf{N}^* \times \mathbf{Z}$. Notons*

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

l'ensemble des entiers congrus à a modulo n.

Proposition 75. — *Soit $n \in \mathbf{N}^*$. Il y a exactement n classes d'équivalences distinctes pour la relation de congruence modulo n. Ces n classes sont*

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}$$

Définition 76. — *Soit $n \in \mathbf{N}^*$. On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble des classes déquivalences pour la relation de congruence modulo n. Ainsi*

$$\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

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

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

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

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

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

Théorème 77. — *Soit $n \in \mathbf{N}^*$. Posons*

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

Alors

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

Exemple 78. — La table du groupe $(\mathbf{Z}/6\mathbf{Z}, +)$ est la suivante.

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

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

6.4. Générateurs du groupe $(\mathbf{Z}/n\mathbf{Z})$

Proposition 79. — *Soient $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}$. L'élément $\overline{a}$ de $\mathbf{Z}/n\mathbf{Z}$ engendre le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ si et seulement si a est premier avec n, i.e.*

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

Exemple 80. — Les seuls éléments qui engendrent le groupe $(\mathbf{Z}/12\mathbf{Z}, +)$ sont $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$.

7. Classification des groupes monogènes

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

Définition 81. — *Soit $(G, *)$ un groupe.*

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

Remarque 82. — Tout groupe monogène est abélien.

7.2. Exemples de groupes monogènes, de groupes cycliques

Exemple 83. — Le groupe $(\mathbf{Z}, +)$ est engendré par l'élément 1. Il est donc est monogène

Exemple 84. — Pour tout $n \in \mathbf{N}^*$, le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ est fini et engendré par l'élément $\overline{1}$. Il est donc cyclique.

Exemple 85. — Pour tout $n \in \mathbf{N}^*$, le groupe multiplicatif

$$\mathbf{U}_n := \{z \in \mathbf{C} \,:\, z^n = 1\} = \left\{e^{i\frac{2k\pi}{n}} \,:\, k \in [\![0, n-1]\!]\right\}$$

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

Exercice 86. — Démontrer que le groupe $\left(\mathbf{Z}^2, +\right)$ n'est pas monogène. En déduire que les groupes $(\mathbf{Z}, +)$ et $\left(\mathbf{Z}^2, +\right)$ ne sont pas isomorphes.

Exercice 87. — Les groupes $(\mathbf{Z}, +)$ et $(\mathbf{Q}, +)$ sont-ils isomorphes ?

7.3. Les groupes $(\mathbf{Z}/n\mathbf{Z}, +)$ et $(\mathbf{U}_n, \times)$ sont isomorphes

Proposition 88. — *Soit $n \in \mathbf{N}^*$. L'application*

$$\varphi \left| \begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z}, +) & \longrightarrow & (\mathbf{U}_n, \times) \\ \overline{a} & \longmapsto & e^{i\frac{2a\pi}{n}} \end{array} \right.$$

est bien définie et est un isomorphisme de groupes.

7.4. Théorème de classification des groupes monogènes

Théorème 89. — *Soit $(G, *)$ un groupe monogène.*

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

8. Théorème de Lagrange (HP)

Théorème 90. — *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
    $$y * x^{-1} = \left(x * y^{-1}\right)^{-1} \in H$$
    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 $\mathcal{P}(G)$ des parties de G est fini et donc il n'y a qu'un nombre fini de classes d'équivalence, disons p. Notons $\overline{x_1}, \ldots, \overline{x_p}$ la liste exhaustive, sans répétition, des différentes classes d'équivalence. Alors
  $$G = \bigsqcup_{i=1}^{p} \overline{x_i}$$
  En conséquence
  $$(\star) \qquad \operatorname{card}(G) = \sum_{i=1}^{p} \operatorname{card}\left(\overline{x_i}\right)$$

- Soit $i \in [\![1,p]\!]$. Démontrons $\text{card}\,(\overline{x_i}) = \text{card}\,(H)$, ce qui grâce à l'identité $(\star)$ nous permettra de conclure. L'application
$$\varphi \left| \begin{array}{ccc} \overline{x_i} & \longrightarrow & H \\ y & \longmapsto & x_i * y^{-1} \end{array} \right.$$
est bien définie (cf. définition de $\mathcal{R}$). L'application
$$\psi \left| \begin{array}{ccc} H & \longrightarrow & \overline{x_i} \\ z & \longmapsto & z^{-1} * x_i \end{array} \right.$$
est également bien définie. En effet
$$\begin{array}{rcl} z \in H & \Rightarrow & x_i * x_i^{-1} * z \in H \\ & \Rightarrow & x_i * \left(z^{-1} * x_i\right)^{-1} \in H \\ & \Rightarrow & x_i * \psi(z)^{-1} \in H \\ & \Rightarrow & x_i \,\mathcal{R}\, \psi(z) \\ & \Rightarrow & \psi(z) \in \overline{x_i}. \end{array}$$
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 91. — 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 92. — *Soient $(G,*)$ un groupe, de neutre noté e, et $x \in G$.*

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

Exercice 93. — 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 94. — 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 $< g >$ qu'il engendre

Proposition 95. — *Soient $(G,*)$ un groupe et $x \in G$. Alors*

1. *x est d'ordre fini si et seulement si $< x >$ est un ensemble fini ;*
2. *si x est d'ordre fini, alors $\text{card}\,(< x >) = \text{ord}\,(x)$.*

Démonstration.

1. $\Longrightarrow$ Supposons x d'ordre fini et posons $n := \text{ord}\,(x) \geqslant 1$. Nous démontrons que l'application
$$f \left| \begin{array}{ccc} [\![0,n-1]\!] & \longrightarrow & < x > \\ k & \longmapsto & x^k \end{array} \right.$$
est bijective, pour obtenir que $< x >$ est un ensemble fini, de cardinal $n = \text{ord}\,(x)$.

- Soit $g \in < x >$. Nous savons qu'il existe un entier $m \in \mathbf{Z}$ tel que $g = x^m$. La division euclidienne de m par n livre l'existence (et l'unicité) de $q \in \mathbf{Z}$ et $r \in [\![0, n-1]\!]$ tels que
$$m = qn + r$$
Alors, comme $x^n = e_G$
$$g = x^m = (x^n)^q * x^r = x^r = f(r)$$
L'application f est donc surjective.
- Soient $k, \ell \in [\![0, n-1]\!]$ tels que $f(k) = f(\ell)$. Sans perte de généralité, on peut supposer $k \leqslant \ell$. De
$$x^k = x^\ell$$
on déduit, en multipliant par $\left(x^{-1}\right)^k$ par la gauche, que
$$x^{\ell-k} = e_G$$
Comme $0 \leqslant \ell - k \leqslant n-1$, si $\ell - k$ n'était pas nul, nous aurions une contradiction avec la minimalité de l'ordre n de x. Aussi k et ℓ sont-ils égaux. L'application f est injective.

1. $\Longleftarrow$ Supposons que l'ensemble $< x >$ est fini. Alors l'application
$$g \left| \begin{array}{ccc} \mathbf{N} & \longrightarrow & < x > \\ k & \longmapsto & x^k \end{array} \right.$$
n'est pas injective. Il existe donc $k, \ell \in \mathbf{N}^*$ distincts tels que $g(k) = g(\ell)$. Sans perte de généralité, on peut supposer $k < \ell$. De
$$x^k = x^\ell$$
on déduit, en multipliant par $\left(x^{-1}\right)^k$ par la gauche, que
$$x^{\ell-k} = e_G$$
Comme $\ell - k \in \mathbf{N}^*$, x est d'ordre fini.

2. L'identité a été établie lors de la démonstration de l'implication directe de l'équivalence de l'assertion 1.

□

De cette démonstration, nous déduisons que si x est un élément d'ordre fini d'un groupe G, alors
$$e_G \ , \ x \ \ x^2 \ , \ \ldots \ , \ x^{\mathrm{ord}(x)-1}$$
est une liste exhaustive et sans répétition des éléments du sous-groupe $< x >$ de G engendré par x.

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

Proposition 96. — *Dans un groupe fini, tout élément est d'ordre fini.*

Remarque 97. — On vérifie que
$$\mathbf{U}_\infty := \bigcup_{n=1}^{+\infty} \mathbf{U}_n$$
est un sous-groupe de $(\mathbf{C}^*, \times)$. Ainsi, $\mathbf{U}_\infty$ est-il naturellement muni d'une structure de groupe multiplicatif. Tous les éléments du groupe $(\mathbf{U}_\infty, \times)$ sont d'ordre fini, mais l'ensemble $\mathbf{U}_\infty$ est infini.

Exemple 98. — Dans le groupe $(\mathbf{Z}, +)$, le seul élément d'ordre fini est 0.

Exemple 99. — Dans le groupe $(\{-1, 1\}, \times)$, 1 est d'ordre 1 et -1 est d'ordre 2.

Exemple 100. — Soit un entier $n \geqslant 2$. L'élément $e^{i\frac{2\pi}{n}}$ est d'ordre n dans le groupe $(\mathbf{U}_n, \times)$.

Exemple 101. — Soient un entier $n \geqslant 2$ et $p \in [\![2, n]\!]$. Dans le groupe $(S_n, \circ)$, tout p-cycle est d'ordre p.

Exercice 102. — Soit E un $\mathbf{R}$-espace vectoriel non réduit à $\{0_E\}$. Que dire d'un élément d'ordre 2 du groupe $(\mathbf{GL}(E), \circ)$? On s'efforcera d'être aussi exhaustif que possible.

9.4. Puissances d'un éléments d'ordre fini

Proposition 103. — *Soient $(G,*)$ un groupe dont le neutre est noté e et x un élément de G d'ordre fini.*

$$\forall n \in \mathbf{Z} \quad x^n = e \iff \text{ord}\,(x) \mid n$$

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

Théorème 104. — *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 $< x >$ de G étant une partie de G, il est fini. D'après la proposition 95, x est d'ordre fini.
2. D'après la proposition 95
$$\text{ord}\,(x) = \text{card}\,(< x >)$$
D'après le théorème de Lagrange (théorème 90)
$$\text{card}\,(< x >) \mid \text{card}\,(G)$$
Ainsi $\text{ord}\,(x) \mid \text{card}\,(G)$.
3. Comme $\text{ord}\,(x) \mid \text{card}\,(G)$, la proposition 103 livre $x^{\text{card}(G)} = e_G$.

□

9.6. Une sélection d'exercices sur les groupes

Exercice 105. — Soient $(G,*)$ un groupe cyclique de cardinal noté n et d un diviseur positif de n.

1. Démontrer que
$$H_d = \left\{x \in G \ : \ x^d = e_G\right\}$$
est un sous-groupe de $(G,*)$, cyclique, de cardinal d.
2. Démontrer que H_d est l'unique sous-groupe de cardinal d de $(G,*)$.

Exercice 106. — Soient un entier $n \geqslant 2$ et $\sigma \in S_n$. Considérons « la » décomposition de σ en produit de cycles à supports disjoints

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

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

Exercice 107. — 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 108. — 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 109. — *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 110. — 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 ajourant $-x$ à chaque membre, il vient $(-1_A) \times x = -x$.

10.2. Définition d'un anneau commutatif

Définition 111. — *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 112. — Les ensembles de nombres livrent les anneaux commutatifs suivants.

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

Exemple 113. — 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 114. — Si n est un entier tel que $n \geqslant 2$, 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 115. — 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 116. — *Soit $(A,+,\times)$ un anneau. Une partie B de A est appelée sous-anneau de $(A,+,\times)$ si les propriétés suivantes sont vérifiées.*

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

(A2) *B est stable pour les lois $+$ et $\times$*

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

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

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

Proposition 117. — *Soit $(A,+,\times)$ un anneau et soit B un sous-anneau de $(A,+,\times)$. Alors les applications induites*

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

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

11.2. Caractérisation des sous-anneaux

Proposition 118. — *Soit $(A,+,\times)$ un anneau. Une partie B de A est un sous-anneau de $(A,+,\times)$ si et seulement si les propriétés suivantes sont vérifiées.*

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

Exercice 119. — Soient un entier $\geqslant 2$ et $\zeta := e^{i\frac{2\pi}{n}}$. On définit l'ensemble $\mathbf{Z}[\zeta]$ par

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

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

12. Rappels sur les morphismes d'anneaux

12.1. Définition d'un morphisme d'anneaux

Définition 120. — *Soient $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ deux anneaux. Une application*

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

est un morphisme d'anneaux si

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

12.2. Exemples de morphismes d'anneaux

Exemple 121. — L'identité $\mathrm{id}_{\mathbf{Z}}$ est l'unique morphisme d'anneaux de $(\mathbf{Z},+,\times)$ dans $(\mathbf{Z},+,\times)$.

Exemple 122. — Soient $n\in\mathbf{N}^*$ et $M\in\mathcal{M}_n(\mathbf{R})$. L'application

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

est un morphisme d'anneaux.

Exercice 123. — L'application transposée

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

est-elle un automorphisme d'anneau ?

12.3. Composition de morphismes d'anneaux

Proposition 124. — *Soient $(A_1,+_1,\times_1)$, $(A_2,+_2,\times_2)$, $(A_3,+_3,\times_3)$ trois anneaux et*

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

deux morphismes d'anneaux. Alors l'application

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

est un morphisme d'anneaux.

12.4. Isomorphisme d'anneaux

Définition 125. — *Un morphisme d'anneaux qui est bijectif est appelé isomorphisme d'anneaux.*

Exemple 126. — Soient E un $\mathbf{R}$-espace vectoriel de dimension finie $n\geqslant 2$, muni d'une base $\mathcal{B}$. L'application

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

est un isomorphisme d'anneaux.

Proposition 127. — *Soient $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ deux anneaux et $f\colon A\longrightarrow B$ un isomorphisme d'anneaux. Alors la bijection réciproque*

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

est un isomorphisme d'anneaux.

Démonstration.

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

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

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

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

□

13. Compléments sur les anneaux

13.1. Produit d'un nombre fini d'anneaux

Proposition 128. — *Soient un entier $n \geqslant 2$ et $(A_1, +_1, \times_1), \dots, (A_n, +_n, \times_n)$ des anneaux. On définit deux opérations sur*

$$\prod_{k=1}^{n} A_k = \{(a_1, \dots, a_n) \ : \ a_1 \in A_1, \dots, a_n \in A_n\}$$

en posant

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

et

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

Alors $\left(\prod_{k=1}^{n} A_k, +, \times\right)$ est un anneau. Son neutre pour la loi $+$ est $(0_{A_1}, \dots, 0_{A_n})$ et son neutre pour la loi $\times$ est $(1_{A_1}, \dots, 1_{A_n})$.

Éléments de démonstration.

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

□

Rappel 129. — Un anneau commutatif $(A, +, \times)$ estintègre 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 130. — 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 131. — *Soient $(A, +, \times)$ un anneau commutatif et I une partie de A. On dit que I est un idéal de A si :*

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

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

Exemple 132. — Si $(A, +, \times)$ est un anneau commutatif, alors $\{0_A\}$ et A sont des idéaux de A, appelés idéaux triviaux.

Exercice 133. — 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 134. — *Pour montrer que I est un idéal d'un anneau commutatif $(A,+,\times)$, il suffit de vérifier les trois propriétés suivantes :*

1. *I est non vide ;*
2. *I est stable par addition tordue, i.e.*
$$\forall\,(x,y)\in I^2 \quad x-y\in I$$
3. *I est absorbant, i.e.*
$$\forall\,x\in I \quad \forall a\in A \quad a\times x\in I$$

13.4. Exemples d'idéaux

Exemple 135. — L'ensemble
$$I:=\left\{f\in\mathcal{C}^0(\mathbf{R},\mathbf{R})\ :\ f(1)=0\right\}$$
est un idéal de l'anneau $\left(\mathcal{C}^0(\mathbf{R},\mathbf{R}),+,\times\right)$.

Exemple 136. — L'ensemble
$$I:=\left\{(u_n)_{n\in\mathbf{N}}\in\mathbf{R}^{\mathbf{N}}\ :\ \exists\,N\in\mathbf{N},\ \forall\,n\geqslant N,\ u_n=0\right\}$$
est un idéal de $\left(\mathbf{R}^{\mathbf{N}},+,\times\right)$.

Exercice 137. — operations sur les idéaux Soit $(A,+,\times)$ un anneau commutatif.

1. Soit $(I_j)_{j\in J}$ une famille d'idéaux de A. Démontrer que leur intersection
$$\bigcap_{j\in J} I_j:=\{x\in A\ :\ \forall\,j\in J,\ x\in I_j\}$$
est un idéal de A.
2. Soient un entier $r\geqslant 2$ et $I_1,I_2,\ldots,I_r$ des idéaux de A. Démontrer que leur somme
$$I_1+I_2+\ldots+I_r:=\left\{x_1+x_2+\ldots+x_r\ :\ (x_1,x_2,\ldots,x_r)\in\prod_{j=1}^{r}I_j\right\}$$
est un idéal de A.
3. Soient I,J deux idéaux de A. Posons
$$IJ:=\left\{\sum_{i=1}^{n}a_i\times b_i\ :\ n\in\mathbf{N}\text{ et }(a_1,\ldots,a_n)\in I^n\ ,\ (b_1,\ldots,b_n)\in J^n\right\}$$
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 138. — *Soit $f\colon(A,+_A,\times_A)\longrightarrow(B,+_B,\times_B)$ un morphisme d'anneaux commutatifs. Alors*
$$\mathrm{Ker}\,(f):=\{x\in A\ :\ f(x)=0_B\}$$
est un idéal de A.

13.6. Idéal engendré par un élément

Proposition 139. — *Soit $(A,+,\times)$ un anneau et $x\in A$. Alors*
$$xA:=\{x\times a\ :\ a\in A\}\qquad[\textit{idéal de } A \textit{ engendré par } x]$$
est un idéal de A.

13.7. Divisibilité dans un anneau commutatif intègre

Définition 140. — *Soit $(A,+,\times)$ un anneau commutatif intègre. On dit que $x \in A$ divise $y \in A$, et on note $x \mid y$, si*

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

Proposition 141. — *Soit $(A,+,\times)$ un anneau commutatif intègre et $(x,y) \in A^2$. Alors*

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

14. Idéaux de Z

14.1. Sous-groupes additifs de Z versus idéaux de Z

Lemme 142. — *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 Z

Théorème 143. —

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 144. — *Soient un entier $r \geqslant 2$ et $(a_1,a_2,\ldots,a_r) \in (\mathbf{Z}^*)^r$. Alors*

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

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

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

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

Corollaire 145. — *Soient un entier $r \geqslant 2$ et $(a_1,a_2,\ldots,a_r) \in (\mathbf{Z}^*)^r$. Alors*

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

Exercice 146. — Soient un entier $r \geqslant 2$ et $(a_1,a_2,\ldots,a_r) \in (\mathbf{Z}^*)^r$. Démontrer que $\bigcap_{i=1}^{r} a_i\mathbf{Z}$ est un idéal de $\mathbf{Z}$ et que son générateur est le PPCM $a_1 \wedge a_2 \wedge \ldots \wedge a_r$ des entiers $a_1,a_2,\ldots,a_r$.

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

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

Théorème 147. — *Soit $n \in \mathbf{N}^*$. Posons*

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

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

Exercice 148. — Résoudre l'équation

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

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

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

Rappel 149. — Soit $(A, +, \times)$ un anneau.

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

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

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

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

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

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

$$\overline{a}^{-1} = \overline{u} \qquad \text{[identité dans } \mathbf{Z}/n\mathbf{Z}\text{]}$$

Remarque 151. — Soient $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}$. Alors

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

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

Rappel 152. — 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 153. — *Soit $n \in \mathbf{N}^*$. Alors*

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

Définition 154. — *Pour tout nombre premier p, on note $\mathbf{F}_p$ le corps $(\mathbf{Z}/p\mathbf{Z}, +, \times)$.*

Remarque 155. — 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
$$f \left| \begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{K} \\ a & \longmapsto & a\,1_{\mathbf{K}} \end{array} \right.$$
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 $\mathrm{Ker}\,(f) = n\mathbf{Z}$.
3. On démontre alors que
$$g \left| \begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \longrightarrow & \mathbf{K} \\ \overline{a} & \longmapsto & a\,1_{\mathbf{K}} \end{array} \right.$$
est une application bien définie, qui est un isomorphisme d'anneaux. Nous en déduisons $n = p$.
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 156. — Soit p un nombre premier. Comme le $\mathcal{F}_p$ est un corps, le groupe des unités de $\mathbf{F}_p$ est
$$(U(\mathbf{F}_p), \times) = \left(\mathbf{F}_p \setminus \left\{0_{\mathbf{F}_p}\right\}, \times\right)$$
On peut démontrer que $\left(\mathbf{F}_p \setminus \left\{0_{\mathbf{F}_p}\right\}, \times\right)$ est un groupe cyclique (HP) d'ordre $p-1$, bien qu'il soit « en général » délicat d'en trouver un générateur explicite.

Exercice 157. — Quels sont les inverses de $\overline{4}$ dans $\mathbf{Z}/5\mathbf{Z}$ et de $\overline{16}$ dans $\mathbf{Z}/17\mathbf{Z}$?

Exercice 158. — Soit $n \in \mathbf{N}^*$.
1. Quels sont les éléments inversibles de $\mathbf{Z}/2^n\mathbf{Z}$?
2. Calculer le cardinal de $U(\mathbf{Z}/2^n\mathbf{Z})$.

15.3. Théorème des restes chinois

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

Lemme 159. — *Soient $n_1, \dots, n_r \in \mathbf{N}^*$ deux à deux premiers entre eux et $x \in \mathbf{Z}$.*

1. *Si tous les entiers $n_1, \dots, n_r$ divisent x alors $\prod_{k=1}^{r} n_k$ divise x.*
2. *Pour tout $i \in [\![1, r]\!]$, $n_i \wedge \prod_{\substack{k=1 \\ k\neq i}}^{r} n_k = 1$.*

Éléments de démonstration.

1. On démontre que, pour tout premier p
$$v_p\left(\prod_{k=1}^{r} n_k\right) = \sum_{k=1}^{k} v_p(n_k) \leqslant v_p(x)$$
en distinguant les premiers qui divisent un (donc un seul) des $n_1, \dots, n_r$ et ceux qui n'en divisent aucun.
2. On démontre que, pour tout premier p
$$v_p\left(n_i \wedge \prod_{\substack{k=1 \\ k\neq i}}^{r} n_k\right) = \min\left\{v_p(n_i), \sum_{\substack{k=1 \\ k\neq i}}^{r} v_p(n_k)\right\} = 0$$
en distinguant les premiers qui divisent n_i (donc aucun des entiers $n_1, \dots, n_{i-1}, n_{i+1}, \dots, n_r$) et les autres.

□

Théorème 160. — *Soient un entier $r \geqslant 2$ et des entiers $n_1 \geqslant 1, n_2 \geqslant 1, \dots, n_r \geqslant 1$ deux-à-deux premiers entre eux.*

1. *L'application*
$$\varphi \left| \begin{array}{ccc} \mathbf{Z}/n_1n_2\dots n_r\mathbf{Z} & \longrightarrow & (\mathbf{Z}/n_1\mathbf{Z}) \times (\mathbf{Z}/n_2\mathbf{Z}) \times \dots \times (\mathbf{Z}/n_r\mathbf{Z}) \\ \overline{a}^{[n_1n_2\dots n_r]} & \longmapsto & \left(\overline{a}^{[n_1]}, \overline{a}^{[n_2]}, \dots, \overline{a}^{[n_r]}\right) \end{array} \right.$$
est bien définie et est un isomorphisme d'anneaux.
2. *Soit $(a_1, a_2, \dots, a_r) \in \mathbf{Z}^r$. Le système de congruences simultanées*
$$(S) : \left\{ \begin{array}{rcll} x & \equiv & a_1 & [n_1] \\ x & \equiv & a_2 & [n_2] \\ & \vdots & & \\ x & \equiv & a_r & [n_r] \end{array} \right.$$
d'inconnue $x \in \mathbf{Z}$ admet une unique solution modulo $n_1n_2\dots n_r$.
3. *Si $u_1, \dots u_n$ sont des nombres entiers tels que*
   - *$\overline{u_1}^{[n_1]}$ est l'inverse de $\overline{n_2n_3n_4\dots n_r}^{[n_1]}$ dans $\mathbf{Z}/n_1\mathbf{Z}$*
   - *$\overline{u_2}^{[n_2]}$ est l'inverse de $\overline{n_1n_3n_4\dots n_r}^{[n_2]}$ dans $\mathbf{Z}/n_2\mathbf{Z}$*
   - *$\overline{u_3}^{[n_3]}$ est l'inverse de $\overline{n_1n_2n_4\dots n_r}^{[n_3]}$ dans $\mathbf{Z}/n_3\mathbf{Z}$*
   - *$\dots$*
   - *$\overline{u_r}^{[n_r]}$ est l'inverse de $\overline{n_1n_2n_3\dots n_{r-1}}^{[n_r]}$ dans $\mathbf{Z}/n_r\mathbf{Z}$*

   alors
$$x_0 := \sum_{i=1}^{r} a_i\, u_i \prod_{\substack{j=1 \\ j\neq i}}^{r} n_j = a_1\, u_1\, n_2n_3n_4\dots n_r + a_2\, u_2\, n_1n_3n_4\dots n_r + \dots + a_r\, u_r\, n_1n_2n_3\dots n_{r-1}$$
est une solution particulière de (S). L'ensemble solution de (S) est donc $x_0 + n_1n_2\dots n_r\mathbf{Z}$.

Remarque 161. — L'énoncé suivant figure dans le livre « Sunzi suanjing » (traduction : « classique mathématique de Sunzi ») datant du 3ème siècle.

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

Exercice 162. — congruences simultanees Résoudre le système de congruences simultanées :
$$\left\{ \begin{array}{rcll} x & \equiv & 4 & [5] \\ x & \equiv & 5 & [11] \end{array} \right.$$
d'inconnue $x \in \mathbf{Z}$.

Exercice 163. — congruences simultanees Résoudre le système de congruences simultanées :
$$\left\{ \begin{array}{rcll} x & \equiv & 1 & [5] \\ x & \equiv & 2 & [6] \\ x & \equiv & 3 & [7] \end{array} \right.$$
d'inconnue $x \in \mathbf{Z}$.

15.4. Théorème d'Euler

Définition 164. — *L'application*
$$\varphi \left| \begin{array}{ccc} \mathbf{N}^* & \longrightarrow & \mathbf{N}^* \\ n & \longmapsto & \operatorname{card}\left(U(\mathbf{Z}/n\mathbf{Z})\right) = \operatorname{card}\left(\{a \in [\![1, n]\!] \ : \ a \wedge n = 1\}\right) \end{array} \right.$$
est appelée indicatrice d'Euler.

Théorème 165. — *Soient $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}$ tel que $a \wedge n = 1$. Alors*

$$a^{\varphi(n)} \equiv 1 \quad [n] \qquad [\textit{théorème d'Euler}]$$

Remarque 166. — Si $n = p$ est un nombre premier, le théorème d'Euler se spécialise en le petit théorème de Fermat

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

Proposition 167. — *Soient $(A_1, +_1, \times_1), \ldots, (A_p, +_p, \times_p)$ des anneaux et $\left(\prod_{i=1}^{p} A_i, +, \times\right)$ l'anneau produit. Alors*

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

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

Théorème 168. — *On note $\mathbf{P}$ l'ensemble des nombres premiers.*

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

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

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

Exercice 169. — Calculer $\varphi(4040)$.

Exercice 170. — Justifier que

$$10^6 \equiv 1 \quad [7] \qquad \text{et} \qquad \sum_{k=1}^{12} 10^{10^k} \equiv -1 \quad [7]$$

Exercice 171. — Soit $p \in \mathbf{N}^*$ un entier premier. Démontrer

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

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 172. — *Soit $A \in \mathbf{K}[X]$. L'ensemble*

$$A\,\mathbf{K}[X] := \{AP \ : \ P \in \mathbf{K}[X]\} \qquad [\textit{ensemble des multiples de } A]$$

est un idéal de $\mathbf{K}[X]$.

Théorème 173. — *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 174. — *Soient un entier $r \geqslant 2$ et $(A_1, A_2, \ldots, A_r) \in \left(\mathbf{K}[X] \setminus \{0_{\mathbf{K}[X]}\}\right)^r$. Alors*

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

est un idéal. Son générateur unitaire est le PCGD des polynômes $A_1, A_2, \ldots, A_r$, i.e.

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

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

Corollaire 175. — *Soient un entier $r \geqslant 2$ et $(A_1, A_2, \ldots, A_r) \in (\mathbf{K}[X])^r$. Alors*

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

Exercice 176. — Soient un entier $r \geqslant 2$ et $(A_1, A_2, \ldots, A_r) \in (\mathbf{K}[X])^r$. 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 $P_1 \wedge P_2 \wedge \ldots \wedge P_r$ des polynômes $A_1, A_2, \ldots, A_r$.

16.4. Notion de polynôme irréductible sur un corps

Définition 177. — *Soit $P \in \mathbf{K}[X]$. P est dit irréductible sur $\mathbf{K}$ si*

$$\begin{cases} & \deg P \geqslant 1 \\ \text{et} & \\ & \forall\,(P_1, P_2) \in \mathbf{K}[X]^2 \qquad P = P_1P_2 \Longrightarrow (P_1 \in \mathbf{K}_0[X] \text{ ou } P_2 \in \mathbf{K}_0[X])\,. \end{cases}$$

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 $\mathbf{L}$ un sur-corps de $\mathbf{K}$ qui est un sous-corps de $\mathbf{C}$: $\mathbf{K} \subset \mathbf{L} \subset \mathbf{C}$. Le polynôme P peut être irréductible sur $\mathbf{K}$, mais réductible sur $\mathbf{L}$. 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 178. — Démontrer que tout polynôme de $\mathbf{K}[X]$ de degré 1 est irréductible sur $\mathbf{K}$.

Exercice 179. — 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 180. — Démontrer qu'un polynôme de $\mathbf{R}[X]$, de degré impair supérieur ou égal à 3, n'est pas irréductible sur $\mathbf{R}$.

Exercice 181. — 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 182. — *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 183. — *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 184. — *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 $\deg(D) \geqslant 1$. Comme D divise A, il existe $Q \in \mathbf{K}[X]$ tel que $A = DQ$. Comme A est irréductible et $\deg D \geqslant 1$, 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 185. — *Soit $P \in \mathbf{K}[X]$ tel que $\deg P \geqslant 1$.*

1. *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 :*

$$P = \mathrm{dom}\,(P)\ P_1^{n_1} \dots P_r^{n_r}$$

2. *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 $P = \mathrm{dom}\,(P)\ Q_1^{m_1} \dots Q_s^{m_s}$, alors*
   - *$r = s$*
   - *il existe une bijection $\sigma : [\![1, r]\!] \longrightarrow [\![1, r]\!]$ telle que, pour tout $i \in [\![1, r]\!]$, $Q_i = P_{\sigma(i)}$ et $m_i = n_{\sigma(i)}$.*

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

- *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 $k \in [\![1, d]\!]$. 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 $P = AB$, $\deg A \geqslant 1$ et $\deg B \geqslant 1$. Puisque
    $$\deg A + \deg B = \deg AB = \deg P = d + 1$$
    nous en déduisons $\deg A \in [\![1, d]\!]$ et $\deg B \in [\![1, d]\!]$. 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
    $$A = P_1^{n_1} \dots P_r^{n_r} \qquad \text{et} \qquad B = Q_1^{m_1} \dots Q_s^{m_s}.$$
    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 ($i \in [\![1, r]\!]$, $j \in [\![1, s]\!]$), 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 $n_1 \geqslant 1$), 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 184, $P_1 = Q_1$. D'après le lemme 184 et le lemme 182, $P_1^{n_1}$ est premier avec les polynômes $Q_2^{m_2}, \dots, Q_s^{m_s}$. Grâce au lemme 183, 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 $n_1 \leqslant m_1$. 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, $j \in [\![1, s]\!]$.

□

Exercice 186. — 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. Quels sont les diviseurs unitaires de P ?

16.8. Irréductibles de $\mathbf{C}[X]$ et irréductibles de $\mathbf{R}[X]$

Théorème 187. —

1. *Soit* $P \in \mathbf{C}[X]$.
$$P \text{ est irréductible sur } \mathbf{C} \iff \deg P = 1$$
2. *Soit* $P \in \mathbf{R}[X]$.
$$P \text{ est irréductible sur } \mathbf{R} \iff \begin{cases} \deg P = 1 \\ \text{ou} \\ P \text{ est de degré 2 et de discriminant strictement négatif} \end{cases}$$

16.9. Décomposition en produit d'irréductibles dans $\mathbf{C}[X]$

Corollaire 188. — *Soit* $P \in \mathbf{C}[X]$ *tel que* $\deg P \geqslant 1$. *La décomposition de* P *en produit de facteurs irréductibles dans* $\mathbf{C}[X]$ *est « de la forme »*
$$P = \operatorname{dom}(P) \prod_{k=1}^{r} (X - \alpha_k)^{n_k}$$
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 185 et 187. □

Remarque 189. — 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 $k \in [\![1, r]\!]$, n_k est l'ordre de multiplicité de la racine α_k de P.

Remarque 190. — Soit $P \in \mathbf{C}[X]$ de degré supérieur ou égale 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 $\mathbf{C}(X)$

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

16.10. Décomposition en produit d'irréductibles dans $\mathbf{R}[X]$

Corollaire 191. — *Soit $P \in \mathbf{R}[X]$ tel que $\deg P \geqslant 1$. La décomposition de P en produit de facteurs irréductibles dans $\mathbf{R}[X]$ est « d'une des formes suivantes »*

1. *Cas où P n'a aucune racine dans $\mathbf{R}$*

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

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

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

3. *Cas où P a une racine dans $\mathbf{R}$ et une racine dans $\mathbf{C} \setminus \mathbf{R}$*

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

où

- *r et s sont des entiers non nuls*
- *$n_1, \dots, n_r, m_1, \dots, m_r$ 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 $k \in [\![1, s]\!]$, $a_k^2 < 4b_k$.*

Démonstration. Il s'agit d'une conséquence des théorèmes 185 et 187. □

Exercice 192. — Décomposer le polynôme $P = X^4 + 16$ en produit d'irréductibles dans $\mathbf{C}[X]$, puis dans $\mathbf{R}[X]$.

Exercice 193. — Soit $n \in \mathbf{N}_{\geqslant 2}$. 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 K-algèbre

Définition 194. — *Soit A un ensemble muni*

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

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

- *d'une loi de composition notée* $\times$

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

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

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

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

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

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

(A3) *les trois opérations* $\times_A$, $.$ *et* $\times_{\mathbf{K}}$ *vérifient la propriété de compatibilité suivante.*

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

17.2. Exemples de K-algèbres

Exemple 195. — Le corps $\mathbf{K}$ est naturellement une $\mathbf{K}$-algèbre. En effet, $(\mathbf{K}, +_{\mathbf{K}}, \times_{\mathbf{K}}, \times_{\mathbf{K}})$ est une $\mathbf{K}$-algèbre.

Exemple 196. — Soit un entier $n \geqslant 2$. Soit $n \in \mathbf{N}_{\geqslant} 2$. 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

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

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 197. — Soit E un $\mathbf{K}$ espace vectoriel. Sur $\mathcal{L}(E)$, muni de 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 :

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

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 198. — Sur $\mathbf{K}[X]$, muni de nous disposons d'une addition et d'une multiplications internes et nous avons déjà observé que $(\mathbf{K}[X], +, \times)$ est un anneau. Si l'on définit l'opération $\cdot$ par :

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

alors $(\mathbf{K}[X], +, \cdot)$ est un $\mathbf{K}$-espace vectoriel. On vérifie que $(\mathbf{K}[X], +, \times, \cdot)$ est une $\mathbf{K}$-algèbre.

Exercice 199. — 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 200. — *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 201. — Soit un entier $n \geqslant 2$. 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 202. — Soit x un nombre réel. Démontrer que $\mathrm{Vect}_{\mathbf{Q}}\left((x^n)_{n \in \mathbf{N}}\right)$ est une sous-$\mathbf{Q}$-algèbre de $\mathbf{R}$.

Proposition 203. — *Soit $(A,+,\times,\cdot)$ une $\mathbf{K}$-algèbre et soit B une sous-$\mathbf{K}$-algèbre de $(A,+,\times,\cdot)$. Alors les applications induites :*

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

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

17.4. Morphisme d'algèbres

Définition 204. — *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 $f\colon (A_1,+_1,\times_1,\cdot_1)\longrightarrow(A_2,+_2,\times_2,\cdot_2)$ est appelé morphisme de $\mathbf{K}$-algèbres si les deux propriétés suivantes sont vérifiées.*

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

Exemple 205. — Soient $n\in\mathbf{N}_{\geqslant 2}$ et $M\in\mathcal{M}_n(\mathbf{R})$. On considère de nouveau l'application :

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

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

Proposition 206. — *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*

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

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

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

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

Définition 207. — *Un morphisme de $\mathbf{K}$-algèbre qui est bijectif est appelé isomorphisme de $\mathbf{K}$-algèbres.*

Exemple 208. — Soit E un $\mathbf{R}$-espace vectoriel de dimension finie $n\geqslant 2$, muni d'une base $\mathcal{B}$. On considère de nouveau l'application :

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

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

Proposition 209. — *Soit $\mathbf{K}$ un corps, soient $(A,+_A,\times_A,\cdot_A)$ et $(B,+_B,\times_B,\cdot_B)$ deux $\mathbf{K}$-algèbres et $f\colon (A,+_A,\times_A,\cdot_A)\longrightarrow(B,+_B,\times_B,\cdot_B)$ un isomorphisme d'anneaux. Alors la bijection réciproque :*

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

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

17.5. Propriété universelle de $\mathbf{K}[X]$ (HP)

Proposition 210. — *Pour tout $\mathbf{K}$-algèbre A et tout élément a de A, il existe un unique morphisme de $\mathbf{K}$-algèbres*

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

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

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

- *Unicité.*
  Supposons que le morphisme de $\mathbf{K}$-algèbres $\varphi\colon \mathbf{K}[X] \longrightarrow A$ tel que $\varphi(X) = a$ existe. Comme $\varphi(1) = 1_A$ et φ respecte les multiplications
  $$\forall\, n \in \mathbf{N} \quad \varphi\left(X^n\right) = a^n$$
  Comme φ est de plus $\mathbf{K}$-linéaire
  $$\forall\, P \in \mathbf{K}[X] \quad \varphi(P) = \varphi\left(\sum_{n=0}^{+\infty} [P]_n\, X^n\right) = \sum_{n=0}^{+\infty} [P]_n\, \varphi(X^n) = \sum_{n=0}^{+\infty} [P]_n\, a^n$$
  Ainsi, φ est nécessairement l'application
  $$\left|\begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & A \\ P & \longmapsto & \displaystyle\sum_{n=0}^{+\infty} [P]_n\, a^n \end{array}\right.$$
  ce qui assure son unicité.
- *Existence.*
  Guidés par notre étude de l'unicité, nous considérons l'application :
  $$\varphi \left|\begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & A \\ P & \longmapsto & \displaystyle\sum_{n=0}^{+\infty} [P]_n\, a^n \end{array}\right.$$
  — $\mathbf{K}$-*linéarité de* φ. Soient $(\lambda, \mu) \in \mathbf{K}^2$ et $(P, Q) \in \mathbf{K}[X]^2$.
  $$\begin{aligned} \varphi(\lambda P + \mu Q) &= \sum_{n=0}^{+\infty} [\lambda P + \mu Q]_n\, a^n && \text{[définition de } \varphi\text{]} \\ &= \sum_{n=0}^{+\infty} \left(\lambda [P]_n + \mu [Q]_n\right) a^n && \text{[définition de } + \text{ dans } \mathbf{K}[X]\text{]} \\ &= \lambda \left(\sum_{n=0}^{+\infty} [P]_n\, a^n\right) + \left(\sum_{n=0}^{+\infty} [Q]_n\, a^n\right) && \text{[règles de calcul dans la } \mathbf{K}\text{-algèbre } A\text{]} \\ &= \lambda\, \varphi(P) + \mu\, \varphi(Q) && \text{[définition de } \varphi\text{]} \end{aligned}$$
  — *L'application* φ *respecte les multiplications.* Nous introduisons deux applications
  $$B_1 \left|\begin{array}{ccc} \mathbf{K}[X] \times \mathbf{K}[X] & \longrightarrow & A \\ (P, Q) & \longmapsto & \varphi(PQ) \end{array}\right. \quad \text{et} \quad B_2 \left|\begin{array}{ccc} \mathbf{K}[X] \times \mathbf{K}[X] & \longrightarrow & A \\ (P, Q) & \longmapsto & \varphi(P) \times_A \varphi(Q) \end{array}\right.$$
  En utilisant les règles de calculs dans les $\mathbf{K}$-algèbres $\mathbf{K}[X]$, A et la linéarité de φ nous vérifions que
  $$(\star) \qquad \text{les applications } B_1 \text{ et } B_2 \text{ sont bilinéaires.}$$
  Par ailleurs, pour tout $(n, m) \in \mathbf{N}^2$
  $$B_1\left(X^n, X^m\right) = \varphi\left(X^{n+m}\right) = a^{n+m} \qquad \text{et} \qquad B_2\left(X^n, X^m\right) = \varphi\left(X^n\right) \times_A \varphi\left(X^m\right) = a^n \times_A a^m = a^{n+m}$$
  Ainsi
  $$(\star\star) \qquad \forall\, (n, m) \in \mathbf{N}^2 \quad B_1\left(X^n, X^m\right) = B_2\left(X^n, X^m\right)$$

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

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

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

□

Remarque 211. — La proposition précédente généralise l'exemple 205 et caractérise la $\mathbf{K}$-algèbre $\mathbf{K}[X]$ à unique isomorphime de $\mathbf{K}$-algèbres près.