19. Algèbre générale

§ 1 Groupes

§ 1.1 Définition d'un groupe

C19.1. Définition (Groupe) Soit G un ensemble et soit une loi de composition interne notée $*$:

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

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

1. **la loi $*$ est associative**, i.e. :
$$\forall (x,y,z)\in G^3,\quad (x*y)*z = x*(y*z)$$
2. **la loi $*$ possède un élément neutre**, i.e. :
$$\exists e\in G,\quad \forall x\in G,\quad e*x = x = x*e$$
3. **tout élément de G admet un inverse pour la loi $*$**, i.e. :
$$\forall x\in G,\quad \exists y\in G,\quad x*y = e = y*x.$$

C19.2. Remarque Soit $(G,*)$ un groupe.

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

C19.3. Définition (Groupe commutatif ou abélien) Soit $(G,*)$ un groupe. Si la loi $*$ vérifie la propriété additionnelle suivante :
$$\forall (x,y)\in G^2,\quad x*y = y*x$$
alors on dit que le groupe $(G,*)$ est commutatif ou abélien, ou que **la loi $*$ est commutative**.

C19.4. Remarque Lorsque le groupe G est abélien, sa loi est souvent notée $+$. Dans ce cas, le neutre est parfois noté 0. Quant à l'inverse d'un élément x de G, il est alors appelé opposé de x et est noté $-x$ (et non x^{-1}).

§ 1.2 Exemples de groupes

C19.5. Exemple Les ensembles de nombres livrent les groupes commutatifs suivants.

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

C19.6. Exercice Justifier que ni $(\mathbb{N},+)$, ni $(\mathbb{Z},\times)$ ne sont des groupes.

C19.7. Exemple (Le groupe abélien $(\mathbb{K}[X],+)$) Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Si $A\in\mathbb{K}[X]$ et $B\in\mathbb{K}[X]$, on définit le polynôme $A+B$ est défini par :
$$A+B := \sum_{k=0}^{+\infty} \left([A]_k +_{\mathbb{K}} [B]_k\right) X^k \in \mathbb{K}[X].$$

On définit ainsi une loi de composition interne + sur $\mathbb{K}[X]$ et on vérifie que $(\mathbb{K}[X],+)$ est un groupe abélien.
Le neutre de ce groupe est le polynôme $0_{\mathbb{K}[X]}$ dont tous les coefficients égalent $0_{\mathbb{K}}$ et l'opposé d'un polynôme $A\in\mathbb{K}[X]$ est

$$-A:=\sum_{k=0}^{+\infty}(-[A]_k)\,X^k\,.$$

C19.8. Exemple (Le groupe abélien $\left(\mathcal{M}_{p,n}(\mathbb{K}),+\right)$) Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Soit $(p,n)\in\mathbb{N}^*\times\mathbb{N}^*$. Pour tout $(A,B)\in\mathcal{M}_{p,n}(\mathbb{K})$, on définit la matrice $A+B\in\mathcal{M}_{p,n}(\mathbb{K})$, par :

$$\forall\,(i,j)\in[\![1,p]\!]\times[\![1,n]\!],\quad [A+B]_{i,j}:=[A]_{i,j}+_{\mathbb{K}}[B]_{i,j}\quad .$$

On définit ainsi une loi de composition interne sur $\mathcal{M}_{p,n}(\mathbb{K})$ et on vérifie que $\left(\mathcal{M}_{p,n}(\mathbb{K}),+\right)$ est un groupe abélien. Le neutre de ce groupe est la matrice de format $p\times n$ dont tous les coefficients sont égaux à $0_{\mathbb{K}}$ et l'opposé $-A$ d'un élément A de $\mathcal{M}_{p,n}(\mathbb{K})$ est définit par :

$$\forall\,(i,j)\in[\![1,p]\!]\times[\![1,n]\!],\quad [-A]_{i,j}=-[A]_{i,j}\quad .$$

C19.9. Exercice Soit E un ensemble non vide. On note $\mathfrak{S}(E)$ l'ensemble des bijections de E dans lui-même.

1. Soit $(f,g)\in\mathfrak{S}(E)^2$. Démontrer que $f\circ g\in\mathfrak{S}(E)$.
2. Soit $(f,g,h)\in\mathfrak{S}(E)^3$. Vérifier : $\left(f\circ g\right)\circ h=f\circ\left(g\circ h\right)$.
3. Déterminer $e\in\mathfrak{S}(E)$ telle que :
$$\forall\,f\in\mathfrak{S}(E),\quad e\circ f=f=f\circ e.$$
4. Soit $f\in\mathfrak{S}(E)$. Déterminer $g\in\mathfrak{S}(E)$ telle que : $f\circ g=e=g\circ f$.
5. En vertu de la question 1, la composition des applications induit une loi de composition interne sur $\mathfrak{S}(E)$. Que peut-on dire de $(\mathfrak{S}(E),\circ)$?
6. Si $(f,g)\in\mathfrak{S}(E)^2$, que peut-on dire de $\left(f\circ g\right)^{-1}$?
7. Le groupe $(\mathfrak{S}(E),\circ)$ est-il abélien ?

C19.10. Exemple (Le groupe symétrique $(\mathfrak{S}_n,\circ)$) Soit $n\in\mathbb{N}_{\geqslant 2}$. L'ensemble des bijections de $[\![1,n]\!]$ dans lui-même est noté $\mathfrak{S}_n$, i.e. $\mathfrak{S}_n:=\mathfrak{S}\left([\![1,n]\!]\right)$. Son cardinal est $n!$. D'après l'exercice C19.9, $\mathfrak{S}_n$ muni de la loi de composition interne donnée par la composition des applications est un groupe. Il est appelé groupe symétrique.

C19.11. Exercice (Table du groupe $(\mathfrak{S}_3,\circ)$) L'ensemble $\mathfrak{S}_3$ possède 6 éléments :

- l'application identité :
$$\mathrm{id}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\quad ;$$
- trois transpositions :
$$(1\,2):=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\quad ;\quad (1\,3):=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\quad ;\quad (2\,3):=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$
- deux cycles de longueur 3 :
$$(1\,2\,3):=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad ;\quad (1\,3\,2):=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\quad .$$

1. Dresser la table du groupe $(\mathfrak{S}_3,\circ)$.

$f\circ g$	$f=\mathrm{id}$	$f=(1\,2)$	$f=(1\,3)$	$f=(2\,3)$	$f=(1\,2\,3)$	$f=(1\,3\,2)$
$g=\mathrm{id}$						
$g=(1\,2)$						
$g=(1\,3)$						
$g=(2\,3)$						
$g=(1\,2\,3)$						
$g=(1\,3\,2)$						

2. En déduire l'inverse de chacun des éléments du groupe $(\mathfrak{S}_3, \circ)$.
3. Le groupe $(\mathfrak{S}_3, \circ)$ est-il abélien ?

C19.12. Exemple (Le groupe $(GL_n(\mathbb{K}), \times)$) Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Soit $n \in \mathbb{N}_{\geqslant 2}$. Pour tout $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$, on définit la matrice $A \times B$ de $\mathcal{M}_n(\mathbb{K})$ par :

$$\forall (i,j) \in [\![1,n]\!]^2, \quad [A \times B]_{i,j} := \sum_{k=1}^{n} [A]_{i,k} \times_{\mathbb{K}} [B]_{k,j} \quad .$$

1. Démontrer que pour tout $(A, B, C) \in \mathcal{M}_n(\mathbb{K})^3$: $(A \times B) \times C = A \times (B \times C)$.
2. Déterminer une matrice $E \in \mathcal{M}_n(\mathbb{K})$ tel que :

$$\forall A \in \mathcal{M}_n(\mathbb{K}), \quad E \times A = A = A \times E \quad .$$

3. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On rappelle que A est inversible s'il existe une matrice $B \in \mathcal{M}_n(\mathbb{K})$ telle que : $A \times B = E = B \times A$.
   (a) Démontrer que si A est inversible, alors la matrice B telle que $A \times B = E = B \times A$ est unique. Elle est appelée matrice inverse de A et est notée A^{-1}.
   (b) On suppose que A est inversible à gauche, i.e. qu'il existe $B \in \mathcal{M}_n(\mathbb{K})$ telle que : $B \times A = E$. Justifier qu'alors A est inversible et que $B = A^{-1}$.
   (c) On suppose que A est inversible à droite, i.e. qu'il existe $C \in \mathcal{M}_n(\mathbb{K})$ telle que : $A \times C = E$. Justifier qu'alors A est inversible et que $C = A^{-1}$.
4. L'ensemble des matrices de $\mathcal{M}_n(\mathbb{K})$ qui sont inversibles est noté $\mathrm{GL}_n(\mathbb{K})$.
   (a) Soit $(A, B) \in \mathrm{GL}_n(\mathbb{K})^2$. Démontrer que $A \times B \in \mathrm{GL}_n(\mathbb{K})$ et exprimer $(A \times B)^{-1}$ en fonction de A^{-1} et de B^{-1}.
   (b) Démontrer que $E \in \mathrm{GL}_n(\mathbb{K})$.
   (c) Soit $A \in \mathrm{GL}_n(\mathbb{K})$. Démontrer que $A^{-1} \in \mathrm{GL}_n(\mathbb{K})$ et que $\left(A^{-1}\right)^{-1} = A$.
5. En vertu de la question 4.(a), la multiplication matricielle induit une loi de composition interne sur $\mathrm{GL}_n(\mathbb{K})$. Que peut-on dire de $(\mathrm{GL}_n(\mathbb{K}), \times)$?
6. Le groupe $(\mathrm{GL}_n(\mathbb{K}), \times)$ est-il abélien ?

§ 1.3 Produit d'un nombre fini de groupes

C19.13. Théorème (Produit de deux groupes) Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. La loi $*$ définie sur l'ensemble $G_1 \times G_2$ par :

$$\forall ((x_1,x_2),(y_1,y_2)) \in (G_1 \times G_2)^2, \qquad (x_1,x_2) * (y_1,y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$$

est une loi de composition interne sur $G_1 \times G_2$ et $(G_1 \times G_2, *)$ est un groupe, appelé groupe produit de G_1 et G_2.

C19.14. Exercice On note conserve les notations du Théorème précédent. Soit e_1 (resp. e_2) le neutre de $(G_1, *_1)$ (resp. de $(G_2, *_2)$)

1. Préciser le neutre du groupe $(G_1 \times G_2, *)$.
2. Soit $x_1 \in G_1$, dont le neutre pour la loi $*_1$ est noté x_1^{-1}. Soit $x_2 \in G_2$, dont le neutre pour la loi $*_2$ est noté x_2^{-1}. Quel est le neutre de $(x_1, x_2) \in G_1 \times G_2$ pour la loi $*$?

C19.15. Remarque (Produit d'un nombre fini de groupes) On peut de la même façon définir le produit d'un nombre fini de groupes. Si $(G_1, *_1), \ldots, (G_n, *_n)$ sont des groupes, alors la loi $*$ définie sur $G := G_1 \times \ldots \times G_n$ par :

$$\forall (x_1,\ldots,x_n) \in G, \quad \forall (y_1,\ldots,y_n) \in G, \quad (x_1,\ldots,x_n) * (y_1,\ldots,y_n) = \left(x_1 *_1 y_1, \ldots, x_n *_n y_n\right)$$

est une loi de composition interne sur G et $(G, \times)$ est un groupe, appelé groupe produit de $(G_1, *_1), \ldots, (G_n, *_n)$.

C19.16. Exemple Soit $n \in \mathbb{N}_{\geqslant 2}$.

1. Le produit du groupe $(\mathbb{Z}, +)$ n fois avec lui-même coïncide avec $\mathbb{Z}^n$ muni de la loi + usuelle. Il s'agit d'un groupe abélien.
2. Le produit du groupe $(\mathbb{R}, +)$ n fois avec lui-même coïncide avec $\mathbb{R}^n$ muni de la loi + usuelle. Il s'agit d'un groupe abélien.

§ 2 Sous-groupes

§ 2.1 Définition d'un sous-groupe

C19.17. Définition (Sous-groupe d'un groupe) Soit $(G,*)$ un groupe, dont le neutre est noté e. Soit $H \subset G$. On dit que H est un sous-groupe de $(G,*)$ si :

1. H **contient l'élément neutre**, i.e. : $e \in H$.
2. H **est stable pour la loi** $*$, i.e. :
$$\forall (x,y) \in H^2, \quad x * y \in H ;$$
3. H **est stable pour le passage à l'inverse**, i.e. :
$$\forall x \in H, \quad x^{-1} \in H .$$

C19.18. Exemple Si $(G,*)$ est un groupe, dont le neutre est noté e, alors $\{e\}$ et G sont des sous-groupes de G.

§ 2.2 Un sous-groupe possède une structure naturelle de groupe

C19.19. Proposition (Un sous-groupe d'un groupe possède une structure naturelle de groupe) Soit $(G,*)$ un groupe. Soit $H \subset G$ un sous-groupe de $(G,*)$. Alors la restriction de la loi $*$ à H (notée abusivement également $*$) définit une loi de composition interne sur H et $(H,*)$ est un groupe.

C19.20. Remarque D'après la proposition C19.19, pour montrer qu'un ensemble G muni d'une loi interne $*$ est un groupe, il suffit de montrer que G est un sous-groupe d'un groupe plus gros G', où la loi $*$ sur G est induite par celle de G'.

§ 2.3 Caractérisation des sous-groupes

C19.21. Proposition (Caractérisation des sous-groupes) Soit $(G,*)$ un groupe. Soit H une partie de G. Alors H est un sous-groupe de $(G,*)$ si et seulement si les deux propriétés suivantes sont vérifiées.

1. H **est non vide**, i.e. : $H \neq \emptyset$.
2. H **est stable par produit tordu**, i.e. :
$$\forall (x,y) \in H^2, \quad x * y^{-1} \in H .$$

C19.22. Remarque (Caractérisation des sous-groupes d'un groupe abélien) Soit $(G,+)$ un groupe abélien. En écrivant la proposition C19.21, il vient qu'une partie H de G est un sous-groupe de $(G,+)$ si et seulement si les deux propriétés suivantes sont vérifiées.

1. H **est non vide**, i.e. : $H \neq \emptyset$.
2. H **est stable par somme tordue** :
$$\forall (x,y) \in H^2, \quad x - y \in H .$$

§ 2.4 Exemples de sous-groupes

C19.23. Exemple (Le groupe $(\mathbb{U},\times)$ et ses sous-groupes $(\mathbb{U}_n,\times)$)

1. L'ensemble des nombres complexes de module 1 est noté $\mathbb{U}$. Démontrer que $\mathbb{U}$ est un sous-groupe de $(\mathbb{C},\times)$.
2. Soit $n \in \mathbb{N}_{\geqslant 2}$. L'ensemble des racines n-ièmes de l'unité est l'ensemble noté $\mathbb{U}_n$ qui est défini par :
$$\mathbb{U}_n := \left\{ z \in \mathbb{C} \, : \, z^n = 1 \right\} .$$
Démontrer que $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{U},\times)$.

C19.24. Exercice (Le groupe $(\mathrm{O}_n(\mathbb{R}),\times)$) On note $\mathrm{O}_n(\mathbb{R})$ l'ensemble défini par :
$$\mathrm{O}_n(\mathbb{R}) := \left\{ M \in \mathcal{M}_n(\mathbb{R}) \, : \, M^\top \times M = I_n = M \times M^\top \right\} .$$
Démontrer que $\mathrm{O}_n(\mathbb{R})$ est un sous-groupe de $(\mathrm{GL}_n(\mathbb{R}),\times)$. Il est appelé groupe orthogonal.

C19.25. Exercice (Le groupe $(\mathrm{GL}(E),\circ)$) Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Soit E un $\mathbb{K}$-espace vectoriel. On note $\mathrm{GL}(E)$ l'ensemble des automorphismes de E. Alors $\mathrm{GL}(E)$ est un sous-groupe de $(\mathfrak{S}(E),\circ)$.

C19.26. Exercice (Le groupe $(\mathrm{O}(E),\circ)$) Soit $(E,\langle\cdot,\cdot\rangle)$ un espace euclidien. Un endomorphisme f de E est une isométrie de E si :
$$\forall x \in E, \qquad \left|\left| f(x) \right|\right| = ||x||$$

où $||\cdot||$ est la norme associée au produit scalaire $\langle\cdot,\cdot\rangle$. L'ensemble des isométries de E est noté $\mathrm{O}(E)$. Démontrer que $\mathrm{O}(E)$ est un sous-groupe de $(\mathrm{GL}(E),\circ)$.

C19.27. Exercice (Le groupe des isométries d'un triangle équilatéral) On considère le plan euclidien usuel, noté $\mathscr{P}$. Soit ABC un triangle équilatéral, dont le centre de gravité est noté O. Une isométrie du plan $\mathscr{P}$ est une application de $\mathscr{P}$ dans $\mathscr{P}$, qui préserve les longueurs, i.e. telle que :

$$\forall\,(P,Q)\in\mathscr{P}^2,\quad f(P)f(Q)=PQ.$$

On peut démontrer, mais on admet ici, qu'une isométrie du plan $\mathscr{P}$ est nécessairement bijective. L'injectivité d'une isométrie du plan $\mathscr{P}$ est aisée à établir, mais la surjectivité est plus délicate à démontrer.

1. On note $\mathrm{Is}(\mathscr{P})$ l'ensemble des isométries de $\mathrm{Is}(\mathscr{P})$. Démontrer que $\mathrm{Is}(\mathscr{P})$ est un sous-groupe de $(\mathfrak{S}(\mathscr{P}),\circ)$.
2. L'ensemble des isométries de $\mathscr{P}$ préservant le triangle ABC est :

   $$\mathrm{Is}(ABC)=\left\{f\in\mathrm{Is}(\mathscr{P})\ :\ f(\{A,B,C\})=\{A,B,C\}\right\}.$$

   Démontrer que $\mathrm{Is}(ABC)$ est un sous-groupe de $\mathrm{Is}(\mathscr{P})$.
3. Soit $f\in\mathrm{Is}(ABC)$. Démontrer $f(O)=O$.
4. On rappelle (et nous redémontrerons plus tard dans l'année) qu'une isométrie de $\mathscr{P}$ qui fixe le point O est :
   - soit une rotation de centre O ;
   - soit une réléxion, i.e. une symétrie orthogonale par rapport à une droite.

   En déduire que $\mathrm{Is}(ABC)$ possède 6 éléments, que l'on explicitera.
5. Dresser la table du groupe $\mathrm{Is}(ABC)$ et la comparer à la table du groupe $(\mathfrak{S}_3,\circ)$ (cf. Exercice C19.11).

§ 2.5 Sous-groupes de $(\mathbb{Z},+)$

C19.28. Proposition (Exemple fondamental de sous-groupe de $(\mathbb{Z},+)$) Soit $a\in\mathbb{Z}$. Alors l'ensemble des multiples entiers de a, noté $a\mathbb{Z}$, défini par :

$$a\mathbb{Z}:=\{an\ :\ n\in\mathbb{Z}\}$$

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

C19.29. Rappel (Division euclidienne sur $\mathbb{Z}$) En utilisant la propriété du bon ordre dans $\mathbb{N}$ (toute partie non vide de $\mathbb{N}$ possède un plus petit élément), on démontre qu'il existe une division euclidienne sur $\mathbb{Z}$. Précisément, si $b\in\mathbb{N}^*$, alors pour tout $a\in\mathbb{Z}$, il existe un unique couple $(q,r)\in\mathbb{Z}^2$ 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.

C19.30. Théorème (Structure des sous-groupes de $(\mathbb{Z},+)$) Soit H un sous-groupe de $(\mathbb{Z},+)$. Il existe un unique $a\in\mathbb{N}$ tel que :

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

C19.31. Remarque La proposition et le théorème qui précèdent nous livrent le résultat suivant. Les parties de $\mathbb{Z}$ de la forme $a\mathbb{Z}$ (avec $a\in\mathbb{Z}$) sont les seuls sous-groupes de $(\mathbb{Z},+)$.

§ 2.6 Intersection de sous-groupes

C19.32. Théorème (Intersection de sous-groupes) Soit $(G,*)$ un groupe. Soit $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors leur intersection :

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

est un sous-groupe de G.

C19.33. Exercice

1. Déterminer le sous-groupe $H:=51\mathbb{Z}\cap 85\mathbb{Z}$ de $(\mathbb{Z},+)$. Cf. Théorème de structure des sous-groupes de $(\mathbb{Z},+)$.
2. Plus généralement, soient a et b des entiers naturels non nuls. Déterminer le sous-groupe $H:=a\mathbb{Z}\cap b\mathbb{Z}$ de $(\mathbb{Z},+)$.

C19.34. Exercice 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.

§ 3 Morphismes de groupes

§ 3.1 Définition d'un morphisme de groupes

C19.35. Définition (Morphisme de groupes) Soient $(G,*)$ et $(H,\cdot)$ deux groupes. Une application $f : G \longrightarrow H$ est un morphisme de groupes si :

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

C19.36. Proposition (Propriétés d'un morphisme de groupes) Soient $(G,*)$ et $(H,\cdot)$ deux groupes, Soit $f : G \longrightarrow H$ un morphisme de groupes. Notons respectivement e_G et e_H les éléments neutres de G et H. Alors :

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

§ 3.2 Exemples de morphismes de groupes

C19.37. Exemple Si $a \in \mathbb{Z}$, l'application

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

est un morphisme de groupes.

C19.38. Exemple L'application

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

est un morphisme de groupes.

C19.39. Exemple Soit $n \in \mathbb{N}_{\geqslant 2}$. La signature

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

est un morphisme de groupes.

C19.40. Exemple Soit $n \in \mathbb{N}_{\geqslant 2}$. Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. L'application

$$\left| \begin{array}{ccc} (\mathrm{GL}_n(\mathbb{K}),\times) & \longrightarrow & (\mathbb{K}^*,\times) \\ M & \longmapsto & \mathrm{Det}(M) \end{array} \right.$$

est un morphisme de groupes.

C19.41. Exercice Soit $n \in \mathbb{N}_{\geqslant 2}$. Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. L'application

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

est-elle un morphisme de groupes ?

C19.42. Exercice (Description des morphismes de groupes de $(\mathbb{Z},+)$ dans lui-même) Soit f un morphisme de groupes de $(\mathbb{Z},+)$ dans lui-même. Démontrer qu'il existe $a \in \mathbb{Z}$ tel que $f = \varphi_a$, où φ_a le morphisme introduit dans l'Exemple C19.37.

C19.43. Exercice Soit $(G,*)$ un groupe. On note $\mathrm{Hom}(Z,G)$ l'ensemble des morphismes de groupes de $(\mathbb{Z},+)$ dans $(G,*)$. Démontrer que l'application :

$$\chi \left| \begin{array}{ccc} \mathrm{Hom}(Z,G) & \longrightarrow & G \\ f & \longmapsto & f(1) \end{array} \right.$$

est bijective.

§ 3.3 Morphismes de groupes et sous-groupes

C19.44. Proposition (Image et image réciproque d'un sous-groupe par un morphisme de groupes) Soient $(G,*)$ et $(H,\cdot)$ deux groupes. Soit $f : G \longrightarrow H$ un morphisme de groupes.

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

C19.45. Définition (Noyau et image d'un morphisme de groupes) Soient $(G,*)$ et $(H,\cdot)$ deux groupes. Soit $f : G \longrightarrow H$ un morphisme de groupes. Notons respectivement e_G et e_H les éléments neutres de G et H.

1. L'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.

C19.46. Proposition (Structures du noyau et de l'image d'un morphisme de groupes) Soient $(G,*)$ et $(H,\cdot)$ deux groupes. Soit $f : G \longrightarrow H$ un morphisme de groupes. Alors :

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

C19.47. Remarque (Critère d'injectivité et de surjectivité pour un morphisme de groupes) Soient $(G,*)$ et $(H,\cdot)$ deux groupes. Soit $f : G \longrightarrow H$ un morphisme de groupes.

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

C19.48. Exemple (Groupe spécial linéaire) Soit $n \in \mathbb{N}_{\geqslant 2}$. Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. L'application
$$\left| \begin{array}{ccc} (\mathrm{GL}_n(\mathbb{K}),\times) & \longrightarrow & (\mathbb{K}^*,\times) \\ M & \longmapsto & \mathrm{Det}(M) \end{array} \right.$$
est un morphisme de groupes. Son noyau est noté $\mathrm{SL}_n(\mathbb{K})$. Ainsi :
$$\mathrm{SL}_n(\mathbb{K}) := \{M \in GL_n(\mathbb{K}) \ : \ \mathrm{Det}(M) = 1\}$$
est un sous-groupe de $(GL_n(\mathbb{K}),\times)$, appelé **groupe spécial linéaire**.

C19.49. Exemple (Groupe spécial orthogonal) Soit $n \in \mathbb{N}_{\geqslant 2}$. L'application
$$\left| \begin{array}{ccc} (\mathrm{O}_n(\mathbb{R}),\times) & \longrightarrow & (\mathbb{R}^*,\times) \\ M & \longmapsto & \mathrm{Det}(M) \end{array} \right.$$
est un morphisme de groupes. Son noyau est noté $\mathrm{SO}_n(\mathbb{R})$. Ainsi :
$$\mathrm{SO}_n(\mathbb{R}) := \{M \in \mathrm{O}_n(\mathbb{R}) \ : \ \mathrm{Det}(M) = 1\}$$
est un sous-groupe de $(\mathrm{O}_n(\mathbb{R}),\times)$, appelé **groupe spécial orthogonal**.

C19.50. Exercice On considère l'application
$$\rho \left| \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathrm{SO}_2(\mathbb{R}),\times) \\ \theta & \longmapsto & \rho(\theta) := \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}. \end{array} \right.$$

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.

C19.51. Exemple (Groupe alterné) Soit $n \in \mathbb{N}_{\geqslant 2}$. Le noyau de la signature

$$\varepsilon : (\mathfrak{S}_n, \circ) \longrightarrow (\{-1,1\}, \times)$$

est l'ensemble des permutations de signature 1. Son noyau, noté $\mathscr{A}_n$, est un sous-groupe de $(\mathfrak{S}_n, \circ)$. On l'appelle **groupe alterné**.

§ 3.4 Propriétés des morphismes de groupes

C19.52. Théorème (Composition de morphismes de groupes) Soient $(G_1, *_1)$, $(G_2, *_2)$, $(G_3, *_3)$ trois groupes. Soient $f : (G_1, *_1) \longrightarrow (G_2, *_2)$ et $g : (G_2, *_2) \longrightarrow (G_3, *_3)$ deux morphismes de groupes. Alors

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

est un morphisme de groupes.

C19.53. Définition (Isomorphisme de groupes) Soient $(G_1, *_1)$, $(G_2, *_2)$ et $f : (G_1, *_1) \longrightarrow (G_2, *_2)$ une application. On dit que f est un isomorphisme de groupes si :

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

C19.54. Définition (Inverse d'un isomorphisme de groupes) Soit $f : (G_1, *_1) \longrightarrow (G_2, *_2)$ un isomorphisme de groupes. Sa bijection réciproque

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

est un morphisme de groupes.

C19.55. Terminologie Deux groupes sont dits isomorphes s'il existe un isomorphisme de groupes de l'un vers l'autre.

C19.56. Exercice Déterminer tous les isomorphismes de groupes de $(\mathbb{Z}, +)$ dans lui-même.

C19.57. Exercice Les groupes $(\mathbb{R}^*, \times)$ et $\left(\mathbb{R}^{+*}, \times\right)$ sont-ils isomophes ?

§ 4 Sous-groupe engendré par une partie

§ 4.1 Definition du sous-groupe engendré par une partie

C19.58. Proposition-Définition (Sous-groupe engendré par une partie) Soit $(G,*)$ un groupe. Soit 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 $< A > \subset H$.
3. Le sous-groupe engendré par A est l'intersection de tous les sous-groupes de G contenant A :

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

C19.59. Exercice

1. Déterminer le sous-groupe $< 6, 10 >$ de $(\mathbb{Z}, +)$ engendré par 6 et 10.
2. Plus généralement, si a et b sont des entiers naturels non nuls, déterminer le sous-groupe $< a, b >$ de $(\mathbb{Z}, +)$ engendré par a et b.

§ 4.2 Description du sous-groupe engendré par une partie

C19.60. Théorème (Description du sous-groupe engendré par une partie) Soient $(G,\cdot)$ un groupe et $A \subset G$ une partie non vide de G. Notons A^{-1} l'ensemble des inverses des éléments de A :

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

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

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

§ 4.3 Notation puissance dans un groupe

C19.61. Définition (Notation puissance dans un groupe) Soit $(G,*)$ un groupe, dont le neutre est noté e. Soit $x \in G$ et soit $n \in \mathbb{Z}$. La puissance n-ième de x est l'élément de G, noté x^n, défini par :

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

C19.62. Proposition (Propriétés de la notation puissance) Soit $(G,*)$ un groupe, dont le neutre est noté e. Soit $x \in G$.

1. Pour tout $(n, m) \in \mathbb{Z}^2$, $x^n * x^m = x^{n+m}$.
2. Pour tout $(n, m) \in \mathbb{Z}^2$, $(x^n)^m = x^{nm}$.

C19.63. Attention Soit $(G,*)$ un groupe. Si $(x, y) \in G^2$ et $n \in \mathbb{Z}$, alors 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 $*$.

§ 4.4 Partie génératrice d'un groupe

C19.64. Définition (Partie génératrice d'un groupe) Soient $(G,*)$ un groupe et A une partie non vide de G. On dit que A est une partie génératrice de G (ou que A engendre G) si $< A >= G$.

C19.65. **Exemple** Le groupe $(\mathbb{Z},+)$ des entiers relatifs est engendré par l'élément 1.

C19.66. **Exemple** Soit $n\in\mathbb{N}_{\geqslant 2}$. Le groupe $(\mathbb{Z}^n,+)$ est engendré par :

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

C19.67. **Exemple** Soit $n\in\mathbb{N}_{\geqslant 2}$. Le groupe $(\mathfrak{S}_n,\circ)$ des permutations de l'ensemble $[\![1,n]\!]$ est engendré par les transpositions.

C19.68. **Exercice (Sous-groupe engendré par un élément)** Soit $(G,*)$ un groupe et soit $a\in G$.

1. Démontrer :
$$<a>=\{a^n\ :\ n\in\mathbb{Z}\}.$$
2. L'ensemble $<a>$ est-il nécessairement infini ?

C19.69. **Exercice (Une partie génératrice de $(\mathrm{GL}_n(\mathbb{K}),\times)$)** Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Soit $n\in\mathbb{N}_{\geqslant 2}$. On note $\left(E_{i,j}\right)_{1\leqslant i,j\leqslant n}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$.

- Soit $i\in[\![1,n]\!]$ et soit $\lambda\in\mathbb{K}^*$. La matrice $D_i(\lambda)\in\mathcal{M}_n(\mathbb{K})$ est définie par :
$$D_i(\lambda):=\lambda.E_{i,i}+\sum_{j\in[\![1,n]\!]\setminus\{i\}}E_{j,j}\ .$$
Une telle matrice est appelée **matrice de dilatation**.
- On pose $\Delta:=\{(i,i)\ :\ i\in[\![1,n]\!]\}$. Soit $(i,j)\in[\![1,n]\!]^2\setminus\Delta$. Soit $\lambda\in\mathbb{K}$. La matrice $T_{i,j}(\lambda)\in\mathcal{M}_n(\mathbb{K})$ est définie par :
$$T_{i,j}(\lambda):=I_n+\lambda.E_{i,j}\ .$$
Une telle matrice est appelée **matrice de transvection**.

En analysant matriciellement l'algorithme du pivot de *Gauß*, démontrer que l'ensemble :

$$\left\{D_i(\lambda)\ :\ i\in[\![1,n]\!]\text{ et }\lambda\in\mathbb{K}^*\right\}\cup\left\{T_{i,j}(\lambda)\ :\ (i,j)\in[\![1,n]\!]^2\setminus\Delta\text{ et }\lambda\in\mathbb{K}\right\}$$

est une partie génératrice du groupe $(\mathrm{GL}_n(\mathbb{K}),\times)$.

§ 4.5 Groupes de type fini

C19.70. **Définition (Groupe de type fini)** Un groupe est dit de type fini s'il est engendré par une partie finie.

C19.71. **Exemple (Groupes finis versus groupes de type fini)**

1. Un groupe fini est nécessairement de type fini. En particulier les groupes de symétrie sont de type fini.
2. D'après les exemples C19.65 et C19.66 les groupes $(\mathbb{Z},+)$ et $(\mathbb{Z}^n,+)$ sont de type fini. Un groupe de type fini n'est donc pas nécessairement fini.

C19.72. **Exercice** Soit $n\in\mathbb{N}_{\geqslant 2}$. Notons $(1\,2)$ 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 $(\mathfrak{S}_n,\circ)$.

C19.73. **Exercice** Soient $(a,b)\in\mathbb{Z}^2$. Donner une condition nécessaire et suffisante pour que la partie $\{a,b\}$ engendre le groupe $(\mathbb{Z},+)$.

C19.74. **Exercice** Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Soit $n\in\mathbb{N}_{\geqslant 2}$.

1. Démontrer que $(\mathbb{K}^*,\times)$ n'est pas de type fini.
2. En déduire que pour tout $n\in\mathbb{N}_{\geqslant 2}$, le groupe $(\mathrm{GL}_n(\mathbb{K}),\times)$ n'est pas de type fini.

C19.75. **Exercice** Le groupe $(\mathbb{Q},+)$ est-il de type fini ?

§ 4.6 Groupes monogènes et groupes cycliques

C19.76. Définition (Groupe monogène, groupe cyclique)

1. Un groupe engendré par un élément est appelé **gropue monogène**.
2. Un groupe monogène et fini est appelé **groupe cyclique**.

C19.77. Exercice Justifier qu'un groupe monogène est abélien.

C19.78. Exemple $(\mathbb{Z},+)$ est monogène.

C19.79. Exemple Le groupe $\left(\mathbb{Z}^2,+\right)$ n'est pas monogène.

C19.80. Exemple Soit $n\in\mathbb{N}_{\geqslant 2}$. Le groupe $(\mathbb{U}_n,\times)$ des racines n-ièmes de l'unité est cyclique, engendré par $e^{\frac{2i\pi}{n}}$.

C19.81. Exercice Les groupes $(\mathbb{Z},+)$ et $\left(\mathbb{Z}^2,+\right)$ sont-ils isomorphes ?

C19.82. Exercice Les groupes $(\mathbb{Z},+)$ et $(\mathbb{Q},+)$ sont-ils isomorphes ?

§ 5 Groupes finis

§ 5.1 Théorème de Lagrange

C19.83. Rappel (Relation d'équivalence et classes d'équivalence) Soit X un ensemble non vide. Soit $\sim$ une relation sur X.
On dit que cette relation est une relation d'équivalence si :
- $\sim$ est réflexive, i.e. : $\forall\, x \in X,\ x \sim x$;
- $\sim$ est symétrique, i.e. : $\forall\, (x_1, x_2) \in X^2,\ x_1 \sim x_2 \Longrightarrow x_2 \sim x_1$;
- $\sim$ est transitive, i.e. : $\forall\, (x_1, x_2, x_3) \in X^3,\ (x_1 \sim x_2 \text{ et } x_2 \sim x_3) \Longrightarrow x_1 \sim x_3$.

Soit $x \in X$. La classe d'équivalence de x, notée $\overline{x}$, est la partie de X définie par :

$$\overline{x} := \{y \in X \,:\, y \sim x\}.$$

Si $(x_1, x_2) \in X^2$, alors $\overline{x_1} = \overline{x_2}$ si et seulement si $x_1 \sim x_2$.
Considérons la famille des classes d'équivalence $\left(\overline{x_i}\right)_{i\in I}$. On peut la considérer comme la « liste » exhaustive, sans répétition, des différentes classes d'équivalence. Alors $\left(\overline{x_i}\right)_{i\in I}$ forme une partition de X, i.e. :
- $\forall\, (i,j) \in I^2, \quad i \neq j \Longrightarrow \overline{x_i} \cap \overline{x_j} = \emptyset$;
- $\bigcup\limits_{i\in I} \overline{x_i} = X$.

C19.84. Théorème (Théorème de Lagrange) Soit $(G, *)$ un groupe fini. Soit 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 $x \sim y$ si et seulement si $x * y^{-1} \in H$. Établissons que $\sim$ est une relation d'équivalence sur G.
  — *La relation $\sim$ est réflexive.* Soit $x \in G$. Comme $x * x^{-1} = e_G \in H$, $x \sim x$.
  — *La relation $\sim$ est symétrique.* Soient $(x, y) \in G^2$ tels que $x \sim y$. 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 $y \sim x$.
  — *La relation $\sim$ est transitive.* Soient $(x, y, z) \in G^3$ tels que $x \sim y$ et $y \sim z$. Alors $x * y^{-1} \in H$ et $y * z^{-1} \in H$. Comme H est stable pour la loi $*$, $x * z^{-1} = x * y^{-1} * y * z^{-1} \in H$.
- Comme G est fini, l'ensemble $\mathscr{P}(G)$ des parties de G sest 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. D'après le rappel précédent :

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

le symbole $\sqcup$ étant utilisé à la place de $\bigcup$ pour indiquer que la réunion est formée d'ensembles deux-à-deux disjoints. En conséquence :

$$(\star) \qquad \operatorname{Card}(G) = \sum_{i=1}^{p} \operatorname{Card}\left(\overline{x_i}\right).$$

- Soit $i \in [\![1, p]\!]$. Démontrons $\operatorname{Card}\left(\overline{x_i}\right) = \operatorname{Card}(H)$, 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 $\sim$). L'application

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

est bien définie. En effet :

$$\begin{array}{rcl} z \in H & \Rightarrow & x_i * x_i^{-1} * z \in H \\ & \Rightarrow & x_i * \left(z^{-1} * x_i\right)^{-1} \in H \\ & \Rightarrow & x_i * \psi(z)^{-1} \in H \\ & \Rightarrow & x_i \sim \psi(z) \\ & \Rightarrow & \psi(z) \in \overline{x_i}. \end{array}$$

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

C19.85. **Exemple** 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.

C19.86. **Exemple** Soit G un groupe d'ordre 32. Alors G ne possède aucun sous-groupe de cardinal 5.

§ 5.2 Ordre d'un élément

C19.87. **Définition (Ordre d'un élément)** Soit $(G,*)$ un groupe, dont le neutre est noté e. Soit $x \in G$. On dit que x est d'ordre fini s'il existe un entier $n \in \mathbb{N}^*$ tel que $x^n = e$. Si tel est le cas, on appelle ordre de x et on note $o(x)$ le plus petit $n \in \mathbb{N}^*$ tel que $x^n = e$:

$$o(x) := \min\left\{n \in \mathbb{N}^* \ : \ x^n = e\right\}.$$

C19.88. **Exemple** Dans le groupe $(\{-1,1\},\times)$, 1 est d'ordre 1 et -1 est d'ordre 2.

C19.89. **Exemple** Dans le groupe $(\mathbb{U}_n,\times)$, $e^{\frac{2i\pi}{n}}$ est d'ordre n.

C19.90. **Exemple** Dans le groupe $(\mathbb{Z},+)$, le seul élément d'ordre fini est 0.

C19.91. **Exemple** Dans le groupe $(\mathfrak{S}_n,\circ)$, le cycle $(1\,2\,3\,\ldots\,n)$ est d'ordre n et une transposition est d'ordre 2.

C19.92. **Proposition (Propriété de divisibilité de l'ordre d'un élément)** Soit $(G,*)$ un groupe, dont le neutre est noté e. Soit $x \in G$ un élément d'ordre d. Alors pour tout $n \in \mathbb{N}$, on a :

$$x^n = e \iff d \mid n.$$

Démonstration

$\boxed{\Longrightarrow}$ Soit $n \in \mathbb{N}$ tel que $x^n = e$. Écrivons la division euclidienne de n par d :

$$n = qd + r$$

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

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

Si $r \neq 0$, alors r vérifie $1 \leqslant r \leqslant d-1$ et $x^r = e$, ce qui contredit la minimalité de d. Donc $r = 0$ et d divise n.

$\boxed{\Longleftarrow}$ Soit $n \in \mathbb{N}$ tel que d divise n. Alors il existe $q \in \mathbb{N}$ tel que $n = qd$. Donc :

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

C19.93. **Théorème (Ordre d'un élément dans un groupe fini)** Soit $(G,*)$ un groupe **fini**. Soit $x \in G$. Alors :

1. x est d'ordre fini ;
2. $o(x)$ est le cardinal du groupe $< x >$ engendré par x ;
3. $o(x)$ divise Card (G).

Démonstration

1. Considérons l'application :

$$\left|\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & G \\ & & i & \longmapsto & x^i \end{array}\right.$$

Comme $\mathbb{Z}$ est infini et G est fini, cette application ne peut être injective. Donc il existe i_1, i_2 dans $\mathbb{Z}$ tels que $i_1 \neq i_2$ et $\varphi(i_1) = \varphi(i_2)$. Quite à échanger i_1 et i_2, on peut supposer que $i_1 > i_2$. De $\varphi(i_1) = \varphi(i_2)$, on déduit : $x^{i_1 - i_2} = e$. Comme $i_1 - i_2 \in \mathbb{N}^*$, x est d'ordre fini.

2. Posons $n := o(x)$. Nous démontrons que l'application

$$\left|\begin{array}{ccccc} \psi & : & [\![0,n-1]\!] & \longrightarrow & <x>=\{x^k \,:\, k\in\mathbb{N}\} \\ & & i & \longmapsto & x^i \end{array}\right.$$

est une bijection, ce qui livrera le résultat.
   - *L'application ψ est injective*
     Soient $i_1, i_2 \in [\![0,n-1]\!]$ tels que $\psi(i_1)=\psi(i_2)$. Quitte à échanger i_1 et i_2, on peut supposer $i_1 \geqslant i_2$, d'où $0 \leqslant i_1 - i_2 \leqslant n-1$. De $\psi(i_1)=\psi(i_2)$, on déduit $x^{i_1-i_2}=e$. Si $i_1-i_2\neq 0$, alors $1\leqslant i_1-i_2\leqslant n-1$ et la minimalité de $n=o(x)$ est contredite. Donc $i_1=i_2$.
     Ainsi ψ est injective.
   - *L'application ψ est injective*
     Soit $k\in\mathbb{N}$. La division euclidienne de k par n s'écrit :
     $$k = qn+r$$
     où $q\in\mathbb{N}$ et $r\in[\![0,n-1]\!]$. Alors :
     $$x^k = x^{qn+r} = \left(x^n\right)^q * x^r = e^q * x^r = e * x^r = x^r = \varphi(r).$$
     Donc ψ est surjective.
3. Par le théorème de Lagrange, le cardinal de $< x >$ divise le cardinal de G. Or le cardinal de $< x >$ est $o(x)$ par 2. Donc $o(x)$ divise le cardinal de G.

C19.94. **EXERCICE** Soit $n\in\mathbb{N}_{\geqslant 2}$, soit $\sigma\in\mathfrak{S}_n$, notons $\sigma = c_1\circ\ldots\circ c_r$ sa décomposition en produit de cycles à supports disjoints. Démontrer que l'ordre de σ est le ppcm des longueurs des cycles $c_1,\ldots,c_r$.

C19.95. **EXERCICE**

1. Démontrer que l'ensemble
$$\mathbb{U}_\infty := \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n = \left\{z\in\mathbb{U} \,:\, \exists n\in\mathbb{N}^*,\, z^n=1\right\}$$
est un sous-groupe de $(\mathbb{U},\times)$.
2. Démontrer que $\mathbb{U}_\infty$ est infini et que tout élément de $\mathbb{U}_\infty$ est d'ordre fini.

§ 6 Anneaux

§ 6.1 Définition d'un anneau

C19.96. Définition (Anneau) Soit A un ensemble non vide muni de deux lois de compositions internes $+$ et $\times$. On suppose que les conditions suivantes sont vérifiées :

1. $(A,+)$ **est un groupe commutatif, d'élément neutre noté** 0_A.
2. La loi $\times$ **est associative**, i.e. :
$$\forall (x,y,z) \in A^3, \quad (x \times y) \times z = x \times (y \times z)\,.$$
3. La loi $\times$ **possède un élément neutre** 1_A, i.e. :
$$\exists 1_A \in A, \quad \forall x \in A, \quad x \times 1_A = x = 1_A \times x\,.$$
4. La loi $\times$ **est distributive par rapport à la loi** $+$, i.e. :
$$\forall (x,y,z) \in A^3, \quad x \times (y+z) = (x \times y) + (x \times z)$$
$$\forall (x,y,z) \in A^3, \quad (y+z) \times x = (y \times x) + (z \times x)\,.$$

On dit alors que $(A,+,\times)$ est un anneau. Si de plus la loi $\times$ est commutative, i.e. :
$$\forall (x,y) \in A^2, \quad x \times y = y \times x$$
on dit que $(A,+,\times)$ est un anneau commutatif.

C19.97. Remarque Soit $(A,+,\times)$ un anneau.

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

§ 6.2 Exemples d'anneaux

C19.98. Exemple (Anneaux construits à l'aide d'ensembles de nombres) $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs.

C19.99. Exemple (L'anneau $(\mathscr{L}(E),+,\circ)$) Le symbole $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Soit E un $\mathbb{K}$-espace vectoriel. Alors $(\mathscr{L}(E),+,\circ)$ est un anneau, qui est non commutatif si E n'est pas de dimension 0 ou 1. Son élément neutre pour la multiplication $\circ$ est id_E.

C19.100. Exemple (L'anneau $(\mathscr{M}_n(\mathbb{K}),+,\times)$) Soit $n \in \mathbb{N}_{\geqslant 2}$. Alors $(\mathscr{M}_n(\mathbb{K}),+,\times)$ est un anneau non commutatif. Son élément neutre pour la multiplication $\times$ est la matrice I_n.

C19.101. Exemple (L'anneau $(\mathbb{K}[X],+,\times)$) $(\mathbb{K}[X],+,\times)$ est un anneau commutatif. Son élément neutre est le polynôme constant 1.

§ 7 Sous-anneau

§ 7.1 Définition d'un sous-anneau

C19.102. Définition (Sous-anneau) Soit $(A,+,\times)$ un anneau. Une partie B de A est appelée sous-anneau de $(A,+,\times)$ si les propriétés suivantes sont vérifiées.

1. B **contient** 0_A **et** 1_A, i.e. $0_A \in B$ et $1_A \in B$.
2. B **est stable pour les lois** $+$ **et** $\times$:
$$\forall (x,y) \in B^2, \quad x+y \in B \quad \text{et} \quad x \times y \in B\,.$$
3. B **est stable par passage à l'opposé**, i.e.
$$\forall x \in B, \quad -x \in B\,.$$

§ 7.2 Un sous-anneau possède une structure naturelle d'anneau

C19.103. Proposition (Un sous-anneau possède une structure naturelle d'anneau) Soit $(A,+,\times)$ un anneau et soit B un sous-anneau de $(A,+,\times)$. Alors les applications induites :
$$+_B \left| \begin{array}{ccc} B^2 & \longrightarrow & B \\ (x,y) & \longmapsto & x+y \end{array} \right. \qquad \times_B \left| \begin{array}{ccc} B^2 & \longrightarrow & B \\ (x,y) & \longmapsto & x \times y \end{array} \right.$$
sont biens définies et $(B,+_B,\times_B)$ est un anneau.

§ 7.3 Caractérisation des sous-anneaux

C19.104. Proposition (Critère pour être un sous-anneau) Soit $(A,+,\times)$ un anneau. Une partie B de A est un sous-anneau de $(A,+,\times)$ si et seulement si les propriétés suivantes sont vérifiées.

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

C19.105. Exercice Soit $n \in \mathbb{N}_{\geqslant 2}$. On pose $\zeta := e^{i\frac{2\pi}{n}}$. On définit l'ensemble $\mathbb{Z}[\zeta]$ par
$$\mathbb{Z}[\zeta] := \left\{ \sum_{k=0}^{n-1} a_k \zeta^k \,:\, (a_0,a_1,\dots,a_{n-1}) \in \mathbb{Z}^n \right\}.$$
Démontrer que $\mathbb{Z}[\zeta]$ est un sous-anneau de $(\mathbb{C},+,\times)$.

§ 8 Élément inversible dans un anneau

§ 8.1 Définition d'un élément inversible d'un anneau et de l'inverse d'un tel

C19.106. Définition (Élement inversible d'un anneau et inverse d'un tel) Soit $(A,+,\times)$ un anneau.

1. Un élément x de A est dit **inversible** si
$$\exists\, y\in A,\quad x\times y = 1_A = y\times x.$$
2. Si x est un élément inversible de A, alors l'élément y de A tel que $x\times y = 1_A = y\times x$ est unique. On l'appelle **inverse de x** et on le note x^{-1}. D'après la définition même de x^{-1} :
$$x\times x^{-1} = 1_A = x^{-1}\times x\,.$$

§ 8.2 Groupe des élements inversibles d'un anneau

C19.107. Proposition-Définition (Groupe des élements inversibles d'un anneau) Soit $(A,+,\times)$ un anneau. L'ensemble des éléments inversibles de A est noté $U(A)$.

1. L'élément 1_A appartient à $U(A)$ et $1_A^{-1} = 1_A$.
2. Si $(x,y)\in U(A)^2$, alors $x\times y\in U(A)$ et $(x\times y)^{-1} = y^{-1}\times x^{-1}$.
3. Si $x\in U(A)$, alors $x^{-1}\in U(A)$ et $\left(x^{-1}\right)^{-1} = x$.
4. D'après les propriétés précédentes, loi $\times$ induit une loi de composition interne sur $U(A)$, que l'on note encore (abusivement) $\times$, et $(U(A),\times)$ est un groupe. On l'appelle groupe des éléments inversibles de l'anneau $(A,+,\times)$.

C19.108. Exemple Le groupe des éléments inversibles de l'anneau $(\mathbb{Z},+,\times)$ est $(\{-1,1\},\times)$.

C19.109. Exemple Le groupe des éléments inversibles de l'anneau $(\mathbb{Q},+,\times)$ est $(\mathbb{Q}^*,\times)$.

C19.110. Exemple Soit $n\in\mathbb{N}_{\geqslant 2}$. Le groupe des éléments inversible de l'anneau $(\mathcal{M}_n(\mathbb{C}),+,\times)$ est le groupe $(\mathrm{GL}_n(\mathbb{C}),\times)$.

§ 9 Morphisme d'anneaux

§ 9.1 Définition d'un morphisme d'anneaux

C19.111. Définition (Morphisme d'anneaux) 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.
$$f(1_A)=1_B$$
où 1_A et 1_B désignent les éléments unités respectifs de $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$;
2. f **respecte les additions**, i.e.
$$\forall (x,y)\in A^2,\quad f\left(x+_A y\right)=f(x)+_B f(y)$$
3. f **respecte les multiplications**, i.e.
$$\forall (x,y)\in A^2,\quad f\left(x\times_A y\right)=f(x)\times_B f(y)\,.$$

§ 9.2 Exemples de morphismes d'anneaux

C19.112. Exemple L'identité $\mathrm{id}_{\mathbb{Z}}$ est l'unique morphisme d'anneaux de $(\mathbb{Z},+,\times)$ dans $(\mathbb{Z},+,\times)$.

C19.113. Exemple Soit E un $\mathbb{R}$-espace vectoriel de dimension finie $n\geqslant 2$. Soit $\mathscr{B}$ une base de E. L'application :

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

est un isomorphisme d'anneaux.

C19.114. Exemple Soit $n\in\mathbb{N}_{\geqslant 2}$ et $M\in\mathscr{M}_n(\mathbb{R})$. L'application :

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

est un morphisme d'anneaux.

C19.115. Exercice L'application transposée

$$T\ \left|\begin{array}{ccc}\mathscr{M}_n(\mathbb{R}) & \longrightarrow & \mathscr{M}_n(\mathbb{R})\\ M & \longmapsto & M^\top\end{array}\right.$$

est-elle un isomorphisme de l'anneau $(\mathscr{M}_n(\mathbb{R}),+,\times)$ dans lui-même ?

§ 9.3 Propriétés des morphismes d'anneaux

C19.116. Proposition (Composition de morphismes d'anneaux) Soient $(A_1,+_1,\times_1)$, $(A_2,+_2,\times_2)$, $(A_3,+_3,\times_3)$ trois anneaux et

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

deux morphismes d'anneaux. Alors l'application :

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

est un morphisme d'anneaux.

C19.117. Définition (Isomorphisme d'anneaux) Un morphisme d'anneaux qui est bijectif est appelé isomorphisme d'anneaux.

C19.118. Proposition (Inverse d'un isomorphisme d'anneaux) 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

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

est un isomorphisme d'anneaux.

Démonstration

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

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

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

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

C19.119. Exercice Soient $(A,+_A,\times_A)$, $(B,+_B,\times_B)$ deux anneaux. et $f\colon(A,+_A,\times_A)\longrightarrow(B,+_B,\times_B)$ un morphisme d'anneaux.

1. Soit $x\in U(A)$. Démontrer que $f(x)\in U(B)$.
2. Que dire de l'application suivante ?

$$\widetilde{f}\left|\begin{array}{ccc}(U(A),\times_A) & \longrightarrow & (U(B),\times_B)\\ x & \longmapsto & f(x)\end{array}\right.$$

§ 9.4 Morphismes d'anneaux et sous-anneaux

C19.120. Définition (Noyau et image d'un morphisme d'anneaux) Soient $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ deux anneaux et $f\colon(A,+_A,\times_A)\longrightarrow(B,+_B,\times_B)$ un morphisme d'anneaux.

1. On appelle noyau de f le sous-ensemble $\mathrm{Ker}(f)$ de A défini par :

$$\mathrm{Ker}(f):=\{x\in A\,:\,f(x)=0_B\}=f^{-1}(\{0_B\}).$$

2. On appelle image de f le sous-ensemble $\mathrm{Im}(f)$ de B défini par :

$$\mathrm{Im}(f):=\{f(x)\,:\,x\in A\}=f(A).$$

C19.121. Remarque (Critère d'injectivité et de surjectivité pour un morphisme d'anneaux) Soient $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ deux anneaux et $f\colon(A,+_A,\times_A)\longrightarrow(B,+_B,\times_B)$ un morphisme d'anneaux.

1. f est injectif si et seulement si $\mathrm{Ker}(f)=\{0_A\}$.
2. f est surjectif si et seulement si $\mathrm{Im}(f)=B$.

C19.122. Proposition (Structure de l'image d'un morphisme d'anneaux) Soient $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ deux anneaux et $f\colon(A,+_A,\times_A)\longrightarrow(B,+_B,\times_B)$ un morphisme d'anneaux. Alors $\mathrm{Im}(f)$ est un sous-anneau de $(B,+_B,\times_B)$.

C19.123. Remarque On conserve les notations de la proposition précédente. $\mathrm{Ker}(f)$ n'est pas un sous-anneau de $(A,+_A,\times_A)$, sauf si $1_B=0_B$, ce qui équivaut à $B=\{0_B\}$. La partie $\mathrm{Ker}(f)$ de A est un idéal (bilatère) de de A. Cf. Partie suivante.

§ 10 Idéaux d'un anneau commutatif

§ 10.1 Définition d'un idéal

C19.124. Définition (Idéal d'un anneau commutatif) Soit $(A,+,\times)$ un anneau commutatif. Soit $I \subset A$. 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. :

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

C19.125. Exercice Soit $(A,+,\times)$ un anneau commutatif.

1. Que dire d'un idéal I de $(A,+,\times)$ tel que $1_A \in I$?
2. Que dire d'un idéal I de $(A,+,\times)$ tel que $I \cap U(A) \neq \emptyset$?

§ 10.2 Critère pour être un idéal

C19.126. Proposition (Critère pour être un idéal) Pour montrer que I est un idéal d'un anneau $(A,+,\times)$, il suffit de vérifier les trois propriétés suivantes :

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

§ 10.3 Exemples d'idéaux

C19.127. Exemple Si $(A,+,\times)$ est un anneau commutatif, alors $\{0_A\}$ et A sont des idéaux de A.

C19.128. Exercice On considère l'anneau commutatif $\left(\mathscr{C}^0(\mathbb{R},\mathbb{R}),+,\times\right)$. Démontrer que :

$$I := \left\{ f \in \mathscr{C}^0(\mathbb{R},\mathbb{R}) \,:\, f(1) = 0 \right\}$$

est un idéal de $\left(\mathscr{C}^0(\mathbb{R},\mathbb{R}),+,\times\right)$.

C19.129. Exercice On considère l'anneau commutatif $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$. Démontrer que :

$$I := \left\{ (u_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}} \,:\, \exists N \in \mathbb{N},\ \forall\, n \geqslant N,\ u_n = 0 \right\}$$

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

§ 10.4 Idéaux de $(\mathbb{Z},+,\times)$

C19.130. Lemme (Sous-groupes de $(\mathbb{Z},+)$ versus idéaux de $(\mathbb{Z},+,\times)$) Soit I une partie de $\mathbb{Z}$. Alors :

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

C19.131. Théorème (Idéaux de $(\mathbb{Z},+,\times)$)

1. Soit $a \in \mathbb{Z}$. L'ensemble
$$a\mathbb{Z} := \{an \,:\, n \in \mathbb{Z}\}$$
des multiples de a est un idéal de $(\mathbb{Z},+,\times)$.
2. Soit I un idéal de l'anneau $(\mathbb{Z},+,\times)$. Alors il existe $a \in \mathbb{Z}$ tel que $I = a\mathbb{Z}$.

§ 10.5 Idéaux de $(\mathbb{K}[X],+,\times)$

C19.132. Théorème (Idéaux de $(\mathbb{K}[X],+,\times)$)

1. Soit $A\in\mathbb{K}[X]$. L'ensemble
$$A\mathbb{K}[X]:=\{AP\,:\,P\in\mathbb{K}[X]\}$$
des multiples de A est un idéal de $(\mathbb{K}[X],+,\times)$.
2. Soit I un idéal de l'anneau $(\mathbb{K}[X],+,\times)$. Alors il existe $A\in\mathbb{K}[X]$ tel que $I=A\mathbb{K}[X]$.

§ 10.6 Morphismes d'anneaux et idéaux

C19.133. Proposition (Structure du noyau d'un morphisme d'anneaux) Soient $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ deux anneaux commutatifs et $f:(A,+_A,\times_A)\longrightarrow(B,+_B,\times_B)$ un morphisme d'anneaux. Alors le noyau de f est un idéal de A.

Démonstration

- Comme f est un morphisme de groupes de $(A,+)$ vers $(B,+)$, $f(0_A)=0_B$. Donc $0_A\in\mathrm{Ker}(f)$. Le noyau de f est donc non vide.
- Soit $x_1,x_2\in\mathrm{Ker}(f)$.
$$f(x_1+_A x_2)\underset{(\star)}{=}f(x_1)+_B f(x_2)=0_B+0_B=0_B$$
où $(\star)$ provient du fait que f est un morphisme d'anneaux. Donc $x_1+_A x_2\in\mathrm{Ker}(f)$.
- Soit $x\in\mathrm{Ker}(f)$ et soit $a\in A$.
$$f(a\times_A x)\underset{(\star)}{=}f(a)\times_B f(x)=f(a)\times_B 0_B\underset{(\star\star)}{=}0_B$$
où $(\star)$ provient du fait que f est un morphisme d'anneaux, et $(\star\star)$ découle du caractère absorbant de 0_B. Donc $a\times_A x\in\mathrm{Ker}(f)$.

C19.134. Exercice Soit $n\in\mathbb{N}_{\geqslant 2}$ et $M\in\mathcal{M}_n(\mathbb{R})$. On considère de nouveau l'application :
$$\left|\begin{array}{ccc}(\mathbb{K}[X],+,\circ) & \longrightarrow & (\mathcal{M}_n(\mathbb{R}),+,\times)\\ P=\sum_{k=0}^{+\infty}a_kX^k & \longmapsto & P(M):=\sum_{k=0}^{+\infty}a_kM^k\end{array}\right.$$
qui est un morphisme d'anneaux, cf. Exemple C19.114. Donner le maximum de propriétés de son noyau $\mathrm{Ker}(f)$.

§ 10.7 Opérations sur les idéaux

C19.135. Proposition (Une intersection d'idéaux est un idéal) Soit $(A,+,\times)$ un anneau commutatif. Soit $(I_j)_{j\in J}$ une famille d'idéaux de A. Alors leur intersection :
$$\bigcap_{j\in J}I_j:=\{x\in A\,:\,\forall\, j\in J,\ x\in I_j\}$$
est un idéal de A.

Démonstration

On sait déjà que $I=\bigcap_{j\in J}I_j$ est un sous-groupe de $(A,+)$, donc stable par $+$. Démontrons que I est absorbant.
Soit $x\in I$, soit $a\in A$. Pour tout $j\in J$, $x\in I_j$, donc $a\times x\in I_j$ puisque I_j est absorbant. Donc $a\times x\in I$, d'où le caractère absorbant de I.

C19.136. Exercice Soit $(A,+,\times)$ un anneau commutatif. Soient I,J deux idéaux de A. Posons :
$$IJ:=\left\{x\in A\,:\,\exists\, n\in\mathbb{N}^*,\ \exists\,(a_1,\dots,a_n)\in I^n,\ \exists\,(b_1,\dots,b_n)\in J^n \text{ tels que } x=a_1\times b_1+\dots+a_n\times b_n\right\}.$$

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

§ 10.8 Idéaux engendrés par un seul élément

C19.137. Proposition-Définition (Idéal engendré par un élément) Soit $(A,+,\times)$ un anneau commutatif. Soit a un élément de A.

1. Parmi les idéaux de A qui contiennent l'élément a, il en existe un plus petit (pour l'inclusion), appelé idéal engendré par a et noté $I(a)$.
2. En d'autres termes, $I(a)$ est caractérisé par les deux propriétés suivantes :
   - $I(a)$ est un idéal de A tel que $a \in I(a)$;
   - si J est un idéal de A tel que $a \in J$, alors $I(a) \subset J$.
3. L'idéal engendré par a est l'intersection de tous les idéaux de A contenant a :

$$I(a) = \bigcap_{\substack{J \text{ idéal de } A \\ a \in J}} J.$$

C19.138. Proposition (Description de l'idéal engendré par un élément) Soient $(A,+,\times)$ un anneau commutatif et $a \in A$. Alors :

$$I(a) = \{a \times x \,:\, x \in A\}.$$

On note encore aA l'idéal engendré par a.

Démonstration

Posons

$$J = \left\{y \in A \,:\, \exists a \in A \text{ tel que } y = x \times a\right\}.$$

Montrons que J est un idéal de A contenant x, puis que tout idéal de A contenant x contient aussi J.

- *J contient x*
  Comme $x = x \times 1_A$, alors $x \in J$.
- *J est un idéal*
  — Montrons d'abord que J est stable par $+$.
  Soit $y, z \in J$. Il existe donc y', z' tels que $y = x \times y'$ et $z = x \times z'$. Alors :

$$y + z = x \times y' + x \times z' = x \times (y' + z').$$

  Comme $y' + z' \in A$, il vient $y + z \in J$.
  — Montrons que J est absorbant.
  Soit $y \in J$, soit $a \in A$. il existe $y' \in A$ tel que $y = x \times y'$. Alors

$$y \times a = (x \times y') \times a = x \times (y' \times a)$$

  par associativité de la multiplication, donc $y \times a \in J$.
- *J est le plus petit idéal contenant x*
  Soit I un idéal de A contenant x. Soit $y \in J$, il existe $y' \in A$ tel que $y = x \times y'$. Comme I est absorbant, $x \times y' \in I$, donc $y \in I$. Donc $J \subset I$.

Bilan : J est un idéal de A contenant x, donc $I(x) \subset J$. De plus, pour tout idéal I de A contenant x, $J \subset I$, donc $J \subset I(x)$. Ainsi $J = I(x)$.

C19.139. Remarque D'après les Théorèmes C19.131 et C19.132, nous savons que les idéaux de $(\mathbb{Z},+,\times)$ et les idéaux de $(\mathbb{K}[X],+,\times)$ sont engendrés par un élément.

§ 10.9 Divisibilité dans un anneau intègre

C19.140. Définition (Anneau intègre) Soit $(A,+,\times)$ un anneau. On dit que l'anneau A est intègre si :

$$\forall (x,y) \in A^2, \quad x \times y = 0_A \Longrightarrow (x = 0_A \text{ ou } y = 0_A).$$

C19.141. Exemple Les anneaux $(\mathbb{Z},+,\times)$ et $(\mathbb{K}[X],+,\times)$ sont des anneaux intègres.

C19.142. Exemple Soit $n \in \mathbb{N}_{\geqslant 2}$. Les anneaux $(\mathcal{M}_n(\mathbb{R}),+,\times)$, $\left(\mathscr{C}^0(\mathbb{R},\mathbb{R}),+,\times\right)$ et $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ ne sont pas des anneaux intègres.

C19.143. Remarque Un anneau $(A,+,\times)$ intègre est **régulier à droite et à gauche**, i.e. :

$$\forall\, a \in A \setminus \{0\}, \quad \forall\, (b,c) \in A^2, \quad b \times a = c \times a \Longrightarrow b = c$$

$$\forall\, a \in A \setminus \{0\}\,, \quad \forall\, (b,c) \in A^2, \quad a \times b = a \times c \implies b = c\,.$$

C19.144. Définition (Divisibilité dans un anneau commutatif intègre) Soit $(A,+,\times)$ un anneau commutatif intègre. Soient $(a,b) \in A^2$. On dit que a divise b, et on note $a \div b$, si :

$$\exists c \in A \text{ tel que } b = a \times c.$$

C19.145. Proposition (Caractérisation de la divisibilité en termes d'idéaux) Soit $(A,+,\times)$ un anneau commutatif intègre et soient $(a,b) \in A^2$. Alors :

$$a \div b \iff bA \subset aA.$$

Démonstration

$\boxed{\implies}$ Supposons $a \div b$. Alors il existe $c \in A$ tel que $b = a \times c$. Soit alors $x \in bA$. Il existe $x' \in A$ tel que $x = b \times x'$, d'où

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

donc $x \in aA$. D'où $bA \subset aA$.

$\boxed{\impliedby}$ Supposons $bA \subset aA$. Comme $b = b \times 1_A \in bA$, $b \in aA$. Donc il existe $x \in A$ tel que $b = a \times x$, donc $a \div b$.

§ 11 Corps

§ 11.1 Définition d'un corps

C19.146. Définition (Corps) Soit $(A,+,\times)$ un anneau commutatif. On dit que $(A,+,\times)$ est un corps si :

1. $0_A \neq 1_A$;
2. **tout élément non nul de A est inversible pour la loi $\times$**, i.e. :

$$\forall x \in A\setminus\{0_A\},\quad \exists y \in A,\quad x\times y = 1_A.$$

C19.147. Proposition (Inverse d'un élément non nul dans un corps) Soit $(K,+,\times)$ un corps. Soit $x \in \mathbb{K}\setminus\{0_K\}$. Alors l'élément $y \in K$ tel que $x\times y = 1_A$ est unique. On l'appelle inverse de x et on le note x^{-1}.

C19.148. Remarque Un corps est un anneau commutatif intègre.

C19.149. Exercice Quels sont les idéaux d'un corps ?

C19.150. Exercice Soit $(A,+,\times)$ un anneau commutatif, tel que $0_A \neq 1_A$, dont le nombre des idéaux est de 2. Démontrer que $(A,+,\times)$ est un corps.

C19.151. Exercice Soit $(A,+,\times)$ un anneau commutatif tel que $0_A \neq 1_A$. On suppose que A est intègre et fini. Démontrer que $(A,+,\times)$ est un corps.

§ 11.2 Exemples de corps

C19.152. Exemple $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps.

C19.153. Exemple $(\mathbb{Z},+,\times)$ et $(\mathbb{R}[X],+,\times)$ ne sont pas des corps.

§ 11.3 Définition d'un sous-corps

C19.154. Définition (Sous-corps) Soit $(K,+,\times)$ un corps. Une partie L de K est appelée sous-corps de $(K,+,\times)$ si les propriétés suivantes sont vérifiées.

1. **L contient 0_K et 1_K**, i.e.
$$0_A \in L \quad \text{et} \quad 1_A \in L.$$
2. **L est stable pour les lois $+$ et $\times$**, i.e. :
$$\forall (x,y) \in L^2,\quad x+y \in L \quad \text{et} \quad x\times y \in L.$$
3. **L est stable par passage à l'opposé et à l'inverse**, i.e. :
$$\forall x \in L,\quad -x \in L \qquad \text{et} \qquad \forall x \in L\setminus\{0_K\},\quad x^{-1} \in L.$$

§ 11.4 Un sous-corps possède une structure naturelle de corps

C19.155. Proposition (Un sous-corps possède une structure naturelle de corps) Soit $(K,+,\times)$ un corps et soit L un sous-corps de $(K,+,\times)$. Alors les applications induites :

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

sont biens définies et $(L,+_L,\times_L)$ est un corps.

§ 11.5 Critère pour être un sous-corps

C19.156. Proposition (Critère pour être un sous-corps) Soit $(K,+,\times)$ un corps. Une partie L de K est un sous-corps de $(K,+,\times)$ si et seulement si les propriétés suivantes sont vérifiées.

1. L **est un sous-anneau de** $(K,+,\times)$.
2. L **est stable par passage à l'inverse**, i.e.
$$\forall\, x \in L\setminus\{0_K\},\quad x^{-1}\in L\,.$$

§ 11.6 Exemples de sous-corps

C19.157. Exemple $(\mathbb{Q},+,\times)$ est un sous-corps de $(\mathbb{R},+,\times)$ et $(\mathbb{R},+,\times)$ est un sous-corps de $(\mathbb{C},+,\times)$.

C19.158. Exercice On pose
$$\mathbb{Q}(i) := \left\{a+bi\,:\,(a,b)\in\mathbb{Q}^2\right\}\subset\mathbb{C}\,.$$
Démontrer que $\mathbb{Q}(i)$ est un sous-corps de $(\mathbb{C},+,\times)$.

C19.159. Exercice (Corps engendré par un nombre algébrique) Soit α un nombre complexe. On suppose que α est algébrique sur $\mathbb{Q}$, i.e. qu'il existe $P\in\mathbb{Q}[X]\setminus\{0\}$ tel que $P(\alpha)=0$. Démontrer que :
$$\mathbb{Q}[\alpha] := \mathrm{Vect}_{\mathbb{Q}}\left(\left(\alpha^k\right)_{k\in\mathbb{N}}\right)$$
est un sous-corps de $\mathbb{C}$.

§ 12 L'ANNEAU $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

§ 12.1 CONSTRUCTION DE L'ANNEAU $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

C19.160. DÉFINITION (RELATION DE CONGRUENCE) Soit $n \in \mathbb{N}^*$, soient $(a,b) \in \mathbb{Z}^2$. On dit que a est congru à b modulo n, et on écrit $a \equiv b\ [n]$, si $a - b \in n\mathbb{Z}$.

C19.161. PROPOSITION (CARACTÉRISATION DE LA RELATION DE CONGRUENCE PAR LES RESTES) Soit $n \in \mathbb{N}^*$, soient $(a,b) \in \mathbb{Z}^2$. Alors $a \equiv b\ [n]$ si et seulement si a et b ont même reste dans la division euclidienne par n.

Démonstration

Soient $p, q \in \mathbb{Z}$, écrivons la division euclidienne de p et q par n :

$$\exists!(u,v,r,s) \in \mathbb{Z}^4 \text{ tel que } \begin{cases} p = un + r, & \text{avec } 0 \leqslant r < n \\ q = vn + s, & \text{avec } 0 \leqslant s < n \end{cases}$$

Alors :

$$p \equiv q\ [n] \iff n|(p-q) \iff n|(u-v)n + (r-s) \iff n|(r-s).$$

Or, $-n < r - s < n$ donc n divise $r - s$ si et seulement si $r - s = 0$.

C19.162. EXEMPLE

1. $6 \equiv 4\ [2]$.
2. Soit $a \in \mathbb{Z}$. Si a est pair, $a \equiv 0\ [2]$ et si a est impair, $a \equiv 1\ [2]$.
3. Soit $a \in \mathbb{Z}$. Une et une seule des assertions suivantes est vraie :
$$a \equiv 0\ [3], \qquad p \equiv 1\ [3], \qquad p \equiv 2\ [3].$$
4. Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Alors :
$$a \equiv 0\ [n] \iff n \mid a.$$

C19.163. PROPOSITION (COMPATIBILITÉ AVEC LA SOMME ET LE PRODUIT) Soient $n \in \mathbb{N}^*$ et $(a,b,c,d) \in \mathbb{Z}^4$. Alors :

$$\begin{cases} a \equiv c\ [n] \\ b \equiv d\ [n] \end{cases} \Longrightarrow \begin{cases} a + b \equiv c + d\ [n] \\ ab \equiv cd\ [n] \end{cases}.$$

Démonstration

Supposons que n divise $(p-q)$ et $(r-s)$. Alors il existe $(u,v) \in \mathbb{Z}^2$ tel que $p - q = nu$ et $r - s = nv$. Alors $(p+r) - (q+s) = n(u+v)$ donc n divise $(p+r) - (q+s)$. De plus, $pr - qs = (p-q)r + q(r-s) = n(ur+qv)$ donc n divise $pr - qs$.

C19.164. COROLLAIRE (COMPATIBILITÉ AVEC LES PUISSANCES) Soient $n \in \mathbb{N}^*$, $(a,b) \in \mathbb{Z}^2$ et $k \in \mathbb{N}^*$. Alors :

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

Démonstration

Récurrence immédiate sur k en utilisant la compatibilité de la congruence et du produit.

C19.165. PROPOSITION (LA RELATION DE CONGRUENCE EST UNE RELATION D'ÉQUIVALENCE) Soit $n \in \mathbb{N}^*$. La relation de congruence modulo n est une relation d'équivalence.

Démonstration

Montrons que la relation de congruence modulo n est réflexive, symétrique et transitive.

- *Réflexivité*
  Soit $p \in \mathbb{Z}$, comme n divise $p - p = 0$, alors $p \equiv q\ [n]$.
- *Symétrie*
  Soit $(p,q) \in \mathbb{Z}^2$ tel que $p \equiv q\ [n]$. Alors n divise $(p-q)$, donc n divise $(q-p)$, donc $q \equiv p\ [n]$.
- *Transitivité*
  Soit $(p,q,r) \in \mathbb{Z}^2$ tel que $p \equiv q\ [n]$ et $q \equiv r\ [n]$. Alors par compatibilité de la congruence et de la somme, on obtient $p + q \equiv q + r\ [n]$, puis en soustrayant q (ce qui est possible, car $-q \equiv -q\ [n]$) en utilisant la compatibilité de la somme et de la congruence, on obtient $p \equiv r\ [n]$.

C19.166. **Exercice** Démontrer que pour tout $n \in \mathbb{N}$, 5 divise $2^{3n+5} + 3^{n+1}$.

C19.167. **Exercice** Quel est le reste de la division euclidienne de $16^{2^{1000}}$ par 7 ?

C19.168. **Exercice** Soit $n \in \mathbb{N}^*$ un nombre ayant $\overline{a_m a_{m-1} \dots a_0}$ pour écriture en base 10. Démontrer les assertions suivantes.

1. $n \equiv a_0 + \dots + a_m$ [3]
2. $n \equiv a_0 + \dots + a_m$ [9]
3. $n \equiv a_0 - a_1 + a_2 - a_3 + a_4 - \dots + (-1)^m a_m$ [11]

C19.169. **Définition (Classe d'équivalence)** Soit $n \in \mathbb{N}^*$. Soit $a \in \mathbb{Z}$. Notons :

$$\overline{a} := \{b \in \mathbb{Z} \ : \ a \equiv b \ [n]\}$$

l'ensemble des entiers congrus à a modulo n.

1. On dit que $\overline{a}$ est la classe d'équivalence de a modulo n.
2. Un élément de $\overline{a}$ est appelé un représentant de $\overline{a}$.

C19.170. **Remarque** Soit $(a, b) \in \mathbb{Z}^2$. Alors :

$$b \text{ est un représentant de } \overline{a} \iff \overline{b} = \overline{a}.$$

C19.171. **Proposition (Nombre de classes d'équivalence)** Soit $n \in \mathbb{N}^*$. Il y a exactement n classes d'équivalences distinctes pour le relation de congruence modulo n. Ces classes sont $\overline{0}, \overline{1}, \dots, \overline{n-1}$.

C19.172. **Définition (L'ensemble $\mathbb{Z}/n\mathbb{Z}$)** Soit $n \in \mathbb{N}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes déquivalences pour la relation de congruence modulo n.

C19.173. **Théorème (Structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$)** Soit $n \in \mathbb{N}^*$. Soient $\overline{a}$, $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$. Posons :

$$\begin{cases} \overline{a} + \overline{b} := \overline{a+b} \\ \overline{a} \times \overline{b} := \overline{a \times b}. \end{cases}$$

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

C19.174. **Remarque** Soit $n \in \mathbb{N}^*$. Soit $(a, b) \in \mathbb{Z}^2$. Alors $\overline{b \times a} = b \times \overline{a}$.

§ 12.2 Étude du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

C19.175. **Proposition (Caractère cyclique de $(\mathbb{Z}/n\mathbb{Z}, +)$)** Soit $n \in \mathbb{N}^*$. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique engendré par $\overline{1}$.

Démonstration

Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est fini de cardinal n. Il suffit de montrer qu'il est monogène. Pour cela, on remarque que pour tout $p \in [\![0, n-1]\!]$,

$$\overline{p} = \underbrace{\overline{1 + \dots + 1}}_{p \text{ fois}} = \underbrace{\overline{1} + \dots + \overline{1}}_{p \text{ fois}} = p\overline{1}.$$

C19.176. Théorème (Générateurs de $\mathbb{Z}/n\mathbb{Z}$) Soit $n \in \mathbb{N}^*$. Soit $a \in \mathbb{Z}$. Alors :

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

Démonstration

Procédons par double implication.

$\boxed{\Longrightarrow}$ Soit $p \in \mathbb{Z}$ tel que $< \overline{p} >= \mathbb{Z}/n\mathbb{Z}$. Alors il existe $u \in \mathbb{Z}$ tel que $u\overline{p} = \overline{1}$, donc $\overline{up} = \overline{1}$, donc n divise $up - 1$, d'où l'existence d'un entier $v \in \mathbb{Z}$ tel que $up - 1 = vn$, soit encore $up - vn = 1$. D'après le théorème de Bezout, $p \wedge n = 1$.

$\boxed{\Longleftarrow}$ Soit $p \in \mathbb{Z}$ tel que $p \wedge n = 1$. D'après le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $up + vn = 1$, donc en passant aux classes d'équivalence : $\overline{up} = \overline{1}$ (puisque $\overline{n} = \overline{0}$). Or $\overline{up} = u\overline{p}$, donc $u\overline{p} = \overline{1}$. Soit alors $q \in \mathbb{Z}$, $\overline{q} = uq\overline{p}$, donc $\overline{q} \in < \overline{p} >$. Ainsi, $\overline{p}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$.

C19.177. Exemple Pour $n = 4$, remarquons que $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}\}$. En revanche, on a bien $\langle \overline{3} \rangle = \mathbb{Z}/4\mathbb{Z}$.

C19.178. Exemple Si n est premier, tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

C19.179. Proposition (Isomorphisme entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{U}_n, \times)$) Soit $n \in \mathbb{N}^*$. Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{U}_n, \times)$ sont isomorphes. Plus précisément, l'application :

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

est bien définie et est un isomorphisme de groupes.

Démonstration

- Commençons par montrer que l'application φ est bien définie : soit $(p, q) \in \mathbb{Z}^2$ tel que $\overline{p} = \overline{q}$. Alors il existe $u \in \mathbb{Z}$ tel que $q = p + un$. Alors $\dfrac{2iq\pi}{n} = \dfrac{2ip\pi}{n} + 2iu$, donc $e^{\frac{2iq\pi}{n}} = e^{\frac{2ip\pi}{n}}$. Donc φ est bien définie.
- Montrons que φ un morphisme de groupes : soit $(\overline{p}, \overline{q}) \in (\mathbb{Z}/n\mathbb{Z})^2$, on a :

$$\begin{aligned} \varphi(\overline{p} + \overline{q}) &= \varphi(\overline{p + q}) \\ &= e^{\frac{2i(p+q)\pi}{n}} \\ &= e^{\frac{2ip\pi}{n}}.e^{\frac{2iq\pi}{n}} \\ &= \varphi(\overline{p}).\varphi(\overline{q}) \end{aligned}$$

- Montrons enfin que φ est bijective. Comme $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ sont finis de même cardinal, il suffit de montrer que φ est injective. Soit alors $\overline{p} \in \mathrm{Ker}(()\varphi)$: alors $e^{\frac{2ip\pi}{n}} = 1$, donc il existe $u \in \mathbb{Z}$ tel que $\dfrac{2ip\pi}{n} = 2iu\pi$, donc $p = un$, donc $\overline{p} = \overline{0}$. Donc φ est bien injective, donc bijective.
  Ainsi, φ est bien un isomorphisme.

C19.180. Proposition (Morphisme canonique de $(\mathbb{Z}, +)$ dans un groupe G associé à un élément de G) Soit $(G, *)$ un groupe, soit $a \in G$.

1. L'application :
$$\varphi_a \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & a^k \end{array} \right.$$
est un morphisme de groupes, appelé morphisme canonique associé à a.
2. Son image $\mathrm{Im}(\varphi_a)$ est le sous-groupe de G engendré par a.

Démonstration

1. Soit $k_1, k_2 \in \mathbb{Z}$.
$$\varphi_a(k_1 + k_2) = a^{k_1+k_2} = a^{k_1}.a^{k_2} = \varphi_a(k_1).\varphi_a(k_2).$$
2. $\mathrm{Im}(\varphi_a) := \{\varphi_a(k) \ : \ k \in \mathbb{Z}\} = \{a^k \ : \ k \in \mathbb{Z}\} =< a >$ (cf. exemple 5).

C19.181. Théorème (Classification des groupes monogènes) Soit $(G,*)$ un groupe monogène et soit a un générateur de $(G,*)$. Le noyau du morphisme canonique φ_a est un sous-groupe de $\mathbb{Z}$. Il est donc de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

1. Si $\mathrm{Ker}(\varphi_a) = \{0\}$, $(G,*)$ est isomorphe à $(\mathbb{Z},+)$.
2. Si $\mathrm{Ker}(\varphi_a) = n\mathbb{Z}$, avec $n \geqslant 1$, $(G,*)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

Démonstration

Étudions séparément les deux cas possibles, suivant le noyau du morphisme de groupes

$$\varphi_a \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & a^k . \end{array} \right.$$

- Supposons que $\mathrm{Ker}(\varphi_a) = \{0\}$.
  Alors φ_a est injective. Comme a est un générateur de G, φ_a est surjective. Donc φ_a est un isomorphisme.
- Supposons que $\mathrm{Ker}(\varphi_a) = n\mathbb{Z}$, avec $n \geqslant 1$. Posons alors :

$$\overline{\varphi_a} \left| \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z},+) & \longrightarrow & (G,*) \\ \overline{p} & \longmapsto & a^p . \end{array} \right.$$

  Nous allons démontrer que $\overline{\varphi_a}$ est un isomorphisme de groupes.
  — *$\overline{\varphi_a}$ est bien définie*
  Soient $(p,q) \in \mathbb{Z}^2$ tels que $\overline{p} = \overline{q}$. Il existe donc $u \in \mathbb{Z}$ tel que $q = p + un$. Ainsi :

$$a^q = a^{p+un} = a^p * a^{nu} = a^p * e_G = a^p$$

  puisque $nu \in n\mathbb{Z} = \mathrm{Ker}(\varphi_a)$. Donc $a^p = a^q$. L'application $\overline{\varphi_a}$ est donc bien définie.
  — *$\overline{\varphi_a}$ est un morphisme de groupes*
  Soit $(\overline{p},\overline{q}) \in (\mathbb{Z}/n\mathbb{Z})^2$, alors :

$$\overline{\varphi_a}(\overline{p}+\overline{q}) = \overline{\varphi_a}(\overline{p+q}) = a^{p+q} = a^p * a^q = \overline{\varphi_a}(\overline{p}) * \overline{\varphi_a}(\overline{q}).$$

  — *$\overline{\varphi_a}$ est bijective*
  Commençons par établir l'injectivité. Soit $\overline{p} \in \mathrm{Ker}(\overline{\varphi_a})$. Alors $a^p = e_G$, donc $p \in \mathrm{Ker}(\varphi_a) = n\mathbb{Z}$, donc il existe $u \in \mathbb{Z}$ tel que $p = nu$. Ainsi $\overline{p} = \overline{0}$. Nous en déduisons que $\mathrm{Ker}(\overline{\varphi_a}) = \{\overline{0}\}$. L'application $\overline{\varphi_a}$ est donc injective.
  La surjectivité de $\overline{\varphi_a}$ provient du caractère générateur de a. En effet soit $g \in G$, il existe $p \in \mathbb{Z}$ tel que $g = a^p = \overline{\varphi_a}(\overline{p})$.
  Ainsi, $\overline{\varphi_a}$ est bien un isomorphisme de groupes.

§ 12.3 Étude de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$

C19.182. Théorème (Éléments inversibles de $(\mathbb{Z}/n\mathbb{Z},+,\times)$) Soit $n \in \mathbb{N}^*$. Notons $U(\mathbb{Z}/n\mathbb{Z})$ le groupe des éléments inversibles de $(\mathbb{Z}/n\mathbb{Z},+,\times)$. Alors :

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

Démonstration

Procédons par double inclusion :

⊂ Soit $\overline{p} \in U(\mathbb{Z}/n\mathbb{Z})$. Alors il existe $\overline{q} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{p}.\overline{q} = \overline{1}$, donc $\overline{pq-1} = \overline{0}$, donc il existe $u \in \mathbb{Z}$ tel que $pq - 1 = un$, donc $qp - un = 1$, et le théorème de Bezout assure que $p \wedge n = 1$.

⊃ Soit $p \in \mathbb{Z}$ tel que $p \wedge n = 1$. D'après le théorème de Bezout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $up + vn = 1$, donc en passant aux classes d'équivalence : $\overline{up} + \overline{vn} = \overline{1}$, d'où $\overline{u}\,\overline{p} = \overline{1}$, donc $\overline{p}$ est inversible et son inverse vaut $\overline{u}$.

C19.183. Remarque Soit $n \in \mathbb{N}^*$. Soit $a \in \mathbb{Z}$.

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

C19.184. Corollaire (Critère pour que $(\mathbb{Z}/n\mathbb{Z},+,\times)$ soit un corps) Soit $n\in\mathbb{N}^*$. L'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un corps si et seulement si n est premier.

Démonstration

$$\begin{aligned}\text{l'anneau } \mathbb{Z}/n\mathbb{Z} \text{ est un corps} &\iff \text{pour tout } r\in[\![1,n-1]\!],\ \overline{r} \text{ est inversible}\\ &\iff \text{pour tout } r\in[\![1,n-1]\!],\ r\wedge n=1 \text{ (cf. Thm 10)}\\ &\iff n \text{ n'a pas d'autre diviseur positif que 1 et } n\\ &\iff n \text{ est premier}\end{aligned}$$

C19.185. Exercice Quel est l'inverse de $\overline{4}$ dans $\mathbb{Z}/5\mathbb{Z}$?

C19.186. Exercice Quel est l'inverse de $\overline{16}$ dans $\mathbb{Z}/17\mathbb{Z}$?

C19.187. Exercice Soit $n\in\mathbb{N}^*$.

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

§ 12.4 Théorème des restes chinois

C19.188. Proposition (Produit d'un nombre fini d'anneaux) Soit $(A_1,+_1,\times_1),\dots,(A_p,+_p,\times_p)$ des anneaux. Sur le produit cartésien d'ensembles $A_1\times\dots\times A_p$, on définit deux lois + et × par :

$$\forall (x_1,\dots,x_p),(y_1,\dots,y_p)\in(A_1\times\dots\times A_p)^2,\quad (x_1,\dots,x_p)+(y_1,\dots,y_p):=(x_1+_1y_1,\dots,x_p+_py_p).$$

$$\forall (x_1,\dots,x_p),(y_1,\dots,y_p)\in(A_1\times\dots\times A_p)^2,\quad (x_1,\dots,x_p)\times(y_1,\dots,y_p):=(x_1\times_1y_1,\dots,x_p\times_py_p).$$

Alors $(A,+,\times)$ est un anneau.

Esquisse de démonstration

- On vérifie que le neutre de $A_1\times\dots\times A_p$ pour la loi + est $(0_{A_1},\dots,0_{A_p})$.
- On vérifie que l'élément $(x_1,\dots,x_p)\in A_1\times\dots\times A_p$ a pour opposé $(-x_1,\dots,-x_p)$.
- On vérifie que le neutre de $A_1\times\dots\times A_p$ pour la loi . est $(1_{A_1},\dots,1_{A_p})$.
- Enfin, l'associativité de +, l'associativité de . et la distributivité de + par rapport à . résulte essentiellement des propriétés correspondantes pour les lois $+_1,\cdot_1,\dots,+_p,\cdot_p$.

C19.189. Remarque Soit $(A_1,+_1,\times_1)$, $(A_2,+_2,\times_2)$ des anneaux, non réduits au zéro, i.e. tels que $0_{A_1}\neq 1_{A_1}$ et $0_{A_2}\neq 1_{A_2}$. Alors $(A_1\times A_2,+,\times)$ **n'est pas** intègre.

C19.190. Proposition (Groupe des inversibles d'un produit d'anneaux) Soit $(A_1,+_1,\times_1),\dots,(A_p,+_p,\times_p)$ des anneaux. Soit $(A_1\times\dots\times A_p,+,\times)$ l'anneau produit. Alors les groupes

$$U(A_1\times\dots\times A_p)\quad\text{et}\quad U(A_1)\times\dots\times U(A_p)$$

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

Démonstration

Soit l'application

$$\left|\begin{array}{rccc}\varphi & : & U(A_1)\times\dots\times U(A_p) & \longrightarrow & U(A_1\times\dots\times A_p)\\ & & (x_1,\dots,x_p) & \longmapsto & (x_1,\dots,x_p)\end{array}\right.$$

- *L'application φ est bien définie*
  Soit $(x_1,\dots,x_p)\in U(A_1)\times\dots\times U(A_p)$.
  Soit $i\in[\![1,p]\!]$. Puisque x_i est inversible dans A_i, il existe $y_i\in A_i$ tel que $x_i\cdot_i y_i=y_i\cdot_i x_i=1_{A_i}$. Alors :

  $$(x_1,\dots,x_p).(y_1,\dots,y_p)=(y_1,\dots,y_p).(x_1,\dots,x_p)=(1_{A_1},\dots,1_{A_p})=1_A.$$

  Donc $(x_1,\dots,x_p)$ est inversible dans $A_1\times\dots\times A_p$, i.e. appartient à $U(A_1\times\dots\times A_p)$.
- *L'application φ est clairement un morphisme de groupes injectif.*

whiteDémonstratio

- *L'application φ est surjective.*
  Soit $(x_1,\dots,x_p)\in U(A_1\times\dots\times A_p)$. Alors, il existe $(y_1,\dots,y_p)\in(A_1\times\dots\times A_p)$ tel que :
  $$(x_1,\dots,x_p).(y_1,\dots,y_p)=(y_1,\dots,y_p).(x_1,\dots,x_p)=1_A=(1_{A_1},\dots,1_{A_p}).$$
  Par définition de la multiplication dans A, et de l'égalité de deux éléments d'un produit cartésien, il vient :
  $$\forall i\in[\![1,p]\!],\quad x_i.y_i=y_i.x_i=1_{A_i}.$$
  Ainsi $x_i\in U(A_i)$ pour tout $i\in[\![1,p]\!]$. Donc $(x_1,\dots,x_n)$ peut être vu comme un élément de $U(A_1)\times\dots\times U(A_p)$ et $\varphi(x_1,\dots,x_n)=(x_1,\dots,x_n)$.

Puisque l'application φ est un isomorphisme de groupes (multiplicatifs), les groupes $U(A_1\times\dots\times A_p)$ et $U(A_1)\times\dots\times U(A_p)$ sont isomorphes.

C19.191. Théorème (Théorème des restes chinois) Soit n,m des entiers supérieurs ou égaux à 2, **premiers entre eux**. Alors les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})$ sont isomorphes. Précisément, l'application :
$$f\ \left|\begin{array}{ccc}\mathbb{Z}/nm\mathbb{Z}&\longrightarrow&(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})\\ \overline{a}\bmod nm&\longmapsto&(\overline{a}\bmod n,\overline{a}\bmod m)\end{array}\right.$$
qui est bien définie, est un isomorphisme d'anneaux.

C19.192. Exercice Résoudre le système $\begin{cases}x=3\bmod 5\\ x=2\bmod 7\end{cases}$ d'inconnue $x\in\mathbb{Z}$.

§ 12.5 Théorème d'Euler

C19.193. Définition (Indicatrice d'Euler) L'application :
$$\varphi\ \left|\begin{array}{ccc}\mathbb{N}^*&\longrightarrow&\mathbb{N}^*\\ n&\longmapsto&\#U(\mathbb{Z}/n\mathbb{Z})=\#\{a\in[\![1,n]\!]\ :\ a\wedge n=1\}\end{array}\right.$$
est appelée indicatrice d'Euler.

C19.194. Théorème (Théorème d'Euler) Soit $n\in\mathbb{N}^*$. Soit $a\in\mathbb{Z}$ tel que $a\wedge n=1$. Alors :
$$a^{\varphi(n)}=1\text{ mod n.}$$

Démonstration

Soit $a\in\mathbb{Z}$ tel que $a\wedge n=1$. D'après le théorème 10, $\overline{a}\in U(\mathbb{Z}/n\mathbb{Z})$. Or $U(\mathbb{Z}/n\mathbb{Z})$ est un groupe (multiplicatif) qui est fini, de cardinal $\varphi(n)$ par définition de l'indicatrice d'Euler. Alors, d'après le théorème 6 :
$$\overline{a}^{\varphi(n)}=\overline{1}$$
d'où $a^{\varphi(n)}=1$ mod n.

C19.195. Remarque Si $n=p$ est un nombre premier, le théorème d'Euler se spécialise en le petit théorème de fermat :
$$\forall a\in[\![1,p-1]\!],\quad a^{p-1}=1\bmod p.$$

C19.196. Théorème (Calcul de l'indicatrice d'Euler)

1. Soit n,m des entiers supérieurs ou égaux à 2, premiers entre eux. Alors $\varphi(nm)=\varphi(n)\,\varphi(m)$.
2. Soit p un nombre premier, soit $k\in\mathbb{N}^*$. Alors $\varphi\left(p^k\right)=(p-1)p^{k-1}$.
3. Soit $n\in\mathbb{N}^*$. Notons $p_1,\dots,p_r$ les diviseurs premiers de n. Alors $\varphi(n)=n\prod_{k=1}^{r}\left(1-\frac{1}{p_k}\right)$.

Démonstration

1. Par le théorème des restes chinois $\mathbb{Z}/nm\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})$ sont des anneaux isomorphes. Par suite, les groupes des éléments inversibles $U(\mathbb{Z}/nm\mathbb{Z})$ et $U((\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z}))$ sont isomorphes. En particulier, ils ont le même cardinal :
$$\varphi(nm) = \#U(\mathbb{Z}/nm\mathbb{Z}) = \#U((\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})).$$
D'après la proposition 19, les groupes $U((\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z}))$ et $U(\mathbb{Z}/n\mathbb{Z})\times U(\mathbb{Z}/m\mathbb{Z})$ sont isomorphes. En particulier, ils ont le même cardinal :
$$\#U((\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})) = \#\left(U(\mathbb{Z}/n\mathbb{Z})\times U(\mathbb{Z}/m\mathbb{Z})\right) = \#U(\mathbb{Z}/n\mathbb{Z})\,\#U(\mathbb{Z}/m\mathbb{Z}) = \varphi(n)\,\varphi(m).$$
Ainsi $\varphi(nm) = \varphi(n)\varphi(m)$.
2. Soit p un nombre premier, soit $k\in\mathbb{N}^*$. $\varphi\left(p^k\right)$ est le nombre d'entiers $n\in[\![0,p^k-1]\!]$ tels que $p^k\wedge n = 1$. Soit $n\in[\![0,p^k-1]\!]$. Comme, p étant premier, $p^k\wedge n = 1$ équivaut à p ne divise pas n. Donc :
$$\begin{array}{rcl}\varphi\left(p^k\right) &=& \#\left([\![0,p^k-1]\!]\setminus\{n\in[\![0,p^k-1]\!] \,:\, n \text{ est multiple de } p\}\right)\\ &=& \#\left([\![0,p^k-1]\!]\setminus\{qp \,:\, q\in[\![0,p^{k-1}-1]\!]\}\right)\\ &=& p^k-p^{k-1}\\ &=& (p-1)p^{k-1}.\end{array}$$
3. Écrivons la décomposition de n en produit de nombre premiers :
$$n = p_1^{k_1}\dots p_r^{k_r}$$
où les p_i sont les diviseurs premiers de n et les k_i sont des entiers naturels non nuls. À l'aide de 1 (et d'une récurrence laissée en exercice), il vient :
$$\varphi(n) = \prod_{i=1}^{r}\varphi\left(p_i^{k_i}\right).$$
Utilisant le résultat 2 :
$$\varphi(n) = \prod_{i=1}^{r}\varphi\left(p_i^{k_i}\right) = \prod_{i=1}^{r}(p_i-1)p^{k_i-1} = \prod_{i=1}^{r}p^{k_i}\left(1-\frac{1}{p_i}\right) = \prod_{i=1}^{r}p^{k_i}\times\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right) = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

C19.197. **Exercice** Démontrer que $10^6\equiv 1\ [7]$, puis que $\sum_{k=1}^{12}10^{10^k}\equiv -1\ [7]$.

C19.198. **Exercice** Démontrer que, pour tout $n\in\mathbb{N}$, 121 ne divise pas n^2+3n+5.

C19.199. **Exercice** Soit p un entier premier. Trouver les classes $\overline{a}\in\mathbb{Z}/p\mathbb{Z}$ telles que $\overline{a}^{-1} = \overline{a}$.

C19.200. **Exercice (Théorème de Wilson)** Soit $p\in\mathbb{N}^*$ un entier premier. Démontrer :
$$(p-1)!\equiv -1\ [p].$$

§ 13 Algèbres

§ 13.1 Définition d'une algèbre

C19.201. Définition (𝕂-algèbre) Soit $(\mathbb{K},+_{\mathbb{K}},\times_{\mathbb{K}})$ un corps. 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'un loi de composition externe à domaine d'opérateurs dans $\mathbb{K}$:
$$. \left|\begin{array}{ccc} \mathbb{K}\times A & \longrightarrow & A \\ (\lambda,x) & \longmapsto & \lambda.x \end{array}\right.$$

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

1. $(A,+_A,.)$ est un $\mathbb{K}$-espace vectoriel ;
2. $(A,+_A,\times_A)$ est un anneau ;
3. les trois opérations $\times_A$, . et $\times_{\mathbb{K}}$ vérifient la propriété de compatibilité suivante.

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

§ 13.2 Exemples d'algèbres

C19.202. Exemple (Un corps 𝕂 est naturellement une 𝕂-algèbre) Soit $(\mathbb{K},+_{\mathbb{K}},\times_{\mathbb{K}})$ un corps. Alors $(\mathbb{K},+_{\mathbb{K}},\times_{\mathbb{K}},\times_{\mathbb{K}})$ est une $\mathbb{K}$-algèbre.

C19.203. Exemple Soit $\mathbb{K}$ un corps. Soit $n\in\mathbb{N}_{\geqslant}2$. Sur $\mathcal{M}_n(\mathbb{K})$, nous disposons d'une addition et d'une multiplications internes et nous avons déjà observé que $(\mathcal{M}_n(\mathbb{K}),+,\times)$ est un anneau. Si l'on définit l'opération . par :

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

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

C19.204. Exercice Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$ 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 . par :

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

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

C19.205. Exercice Soit $\mathbb{K}$ un corps. Sur $\mathbb{K}[X]$, muni de nous disposons d'une addition et d'une multiplications internes et nous avons déjà observé que $(\mathbb{K}[X],+,\times)$ est un anneau. Si l'on définit l'opération . par :

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

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

C19.206. Exercice (Structure de 𝕂-algèbre sur $\mathcal{F}(X,\mathbb{K})$) Soit $\mathbb{K}$ un corps. Soit X un ensemble non vide. On note $\mathcal{F}(X,\mathbb{K})$ l'ensemble des applications de X dans $\mathbb{K}$. Munir $\mathcal{F}(X,\mathbb{K})$ d'une structure de $\mathbb{K}$-algèbre naturelle.

§ 13.3 Sous-algèbre

C19.207. Définition (Sous-algèbre) Soit $\mathbb{K}$ un corps et soit $(A,+,\times,.)$ une $\mathbb{K}$-algèbre. Une partie B de A est appelée sous-$\mathbb{K}$-algèbre de $(A,+,\times,.)$ si B est à la fois un sous-$\mathbb{K}$-espace vectoriel de $(A,+,.)$ et un sous-anneau de $(A,+,\times)$.

§ 13.4 Une sous-algèbre possède une structure naturelle d'algèbre

C19.208. Proposition (Une sous-algèbre possède une structure naturelle d'algèbre) Soit $(K,+,\times)$ un corps, soit $(A,+,\times,.)$ une $\mathbb{K}$-algèbre et soit B une sous-$\mathbb{K}$-algèbre de $(A,+,\times,.)$. Alors les applications induites :

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

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

C19.209. Exercice Soit x un nombre réel. Démontrer que $\mathrm{Vect}_{\mathbb{Q}}\left((x^n)_{n\in\mathbb{N}}\right)$ est une sous-$\mathbb{Q}$-algèbre de $\mathbb{R}$.

§ 13.5 Morphisme d'algèbres

C19.210. Définition (Morphismes de $\mathbb{K}$-algèbres) Soit $\mathbb{K}$ un corps. Soient $(A_1,+_1,\times_1,.1)$ et $(A_2,+_2,\times_2,.2)$ deux $\mathbb{K}$-algèbres. Une application $f\colon (A_1,+_1,\times_1,.1)\longrightarrow(A_2,+_2,\times_2,.2)$ est appelé morphisme de $\mathbb{K}$-algèbres si les deux propriétés suivantes sont vérifiées.

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

§ 13.6 Propriétés des morphismes d'algèbres

C19.211. Proposition (Composition de morphismes d'algèbres) Soit $\mathbb{K}$ un corps, soient $(A_1,+_1,\times_1,.1)$, $(A_2,+_2,\times_2,.2)$, $(A_3,+_3,\times_3,.3)$ trois $\mathbb{K}$-algèbres et

$$f\colon (A_1,+_1,\times_1,.1)\longrightarrow(A_2,+_2,\times_2,.2) \qquad g\colon (A_2,+_2,\times_2,.2)\longrightarrow(A_3,+_3,\times_3,.3)$$

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

$$g\circ f \left| \begin{array}{ccc} (A_1,+_1,\times_1,.1) & \longrightarrow & (A_3,+_3,\times_3,.3) \\ x_1 & \longmapsto & g(f(x_1)) \end{array} \right.$$

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

C19.212. Définition (Isomorphisme de $\mathbb{K}$-algèbres) Un morphisme de $\mathbb{K}$-algèbre qui est bijectif est appelé isomorphisme de $\mathbb{K}$-algèbres.

C19.213. Proposition (Inverse d'un isomorphisme de $\mathbb{K}$-algèbres) Soit $\mathbb{K}$ un corps, soient $(A,+_A,\times_A,.A)$ et $(B,+_B,\times_B,.B)$ deux $\mathbb{K}$-algèbres et $f\colon (A,+_A,\times_A,.A)\longrightarrow(B,+_B,\times_B,.B)$ un isomorphisme d'anneaux. Alors la bijection réciproque

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

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

§ 13.7 Exemples de morphismes d'algèbres

C19.214. Exemple Soit E un $\mathbb{R}$-espace vectoriel de dimension finie $n\geqslant 2$. Soit $\mathscr{B}$ une base de E. On considère de nouveau l'application :

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

cf. Exemple C19.113. L'application $\mathrm{Mat}_{\mathscr{B}}(\cdot)$ est un isomorphisme de $\mathbb{R}$-algèbres.

C19.215. Exemple Soit $n\in\mathbb{N}_{\geqslant 2}$ et $M\in\mathscr{M}_n(\mathbb{R})$. On considère de nouveau l'application :

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

cf. Exemple C19.114. L'application φ est un morphisme de $\mathbb{R}$-algèbres.

§ 14 UNE SÉLECTION D'EXERCICES

C19.216. EXERCICE (CCINP) Soit $p \in \mathbb{N}^*$. On considère dans $\mathbb{Z}$ la relation d'équivalence $\mathscr{R}$ définie par

$$\forall (x,y) \in \mathbb{Z}^2, \quad x \mathscr{R} y \iff p \mid (x-y).$$

On note $\mathbb{Z}/p\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation d'équivalence.

1. Quelle est la classe d'équivalence de 0 ? Quelle est celle de p ?
2. Donner soigneusement la définition de l'addition usuelle et de la multiplication usuelle dans $\mathbb{Z}/p\mathbb{Z}$.
3. On admet que muni de ces opérations, $\mathbb{Z}/p\mathbb{Z}$ est un anneau. Démontrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

C19.217. EXERCICE (CCINP) On note $\mathfrak{S}_n$ l'ensemble des permutations sur l'ensemble $[\![1,n]\!]$.

1. Démontrer que $(\mathfrak{S}_n, \circ)$ est un groupe.
2. On note σ l'élément de $\mathfrak{S}_8$ défini de la manière suivante

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 7 & 8 & 6 & 2 & 3 \end{pmatrix}$$

   l'image de chaque terme de la premiére ligne étant écrit juste en-dessous.
   (a) Démontrer que la permutation σ est la composée de deux cycles que l'on précisera.
   (b) On note $\sigma^n = \underbrace{\sigma \circ \ldots \circ \sigma}_{n \text{ fois}}$. Déterminer σ^{12}, σ^{24}, σ^4 et σ^{2016}.

C19.218. EXERCICE (CCINP) Résoudre les équations suivantes

1. $3n+5 \equiv 0 \quad [10]$
2. $n^2 \equiv 1 \quad [8]$
3. $n^2+2n+2 \equiv 0 \quad [5]$

d'inconnue $n \in \mathbb{Z}$.

C19.219. EXERCICE (CCINP)

1. Résoudre le système suivant

$$\begin{cases} n \equiv 1 \quad [6] \\ n \equiv 2 \quad [7] \end{cases}$$

   d'inconnue $n \in \mathbb{Z}$.
2. Résoudre le système suivant

$$\begin{cases} 3n \equiv 2 \quad [5] \\ 5n \equiv 1 \quad [6] \end{cases}$$

   d'inconnue $n \in \mathbb{Z}$.
3. Résoudre le système suivant

$$\begin{cases} n+m \equiv 4 \quad [11] \\ nm \equiv 10 \quad [11] \end{cases}$$

   d'inconnue $(n,m) \in \mathbb{Z}^2$.

C19.220. EXERCICE (CCINP) Démontrer que pour tout $n \in \mathbb{N}^*$

$$12^{12^n} \equiv 1 \quad [7] \qquad \text{et} \qquad 10^{10^n} \equiv 4 \quad [7].$$

C19.221. EXERCICE (CCINP) Soit $(G,\cdot)$ un groupe. Soit $a \in G$. Pour tout $(x,y) \in G^2$, posons

$$x \star y = x \cdot a \cdot y\,.$$

Démontrer que $(G,\star)$ est un groupe.

C19.222. EXERCICE (CCINP) Soit $(A,+,.)$ un anneau commutatif. Soit I un idéal de A.

1. L'ensemble $\{x \in A : x^2 \in I\}$ est-il un idéal de A ?

2. L'ensemble $\left\{x \in A : \exists n \in \mathbb{N},\ x^n \in I\right\}$ est-il un idéal de A?

C19.223. **Exercice (CCINP)** Existe-t-il un couple $(a,b) \in \mathbb{N}^2$ tel que $a^2+b^2 = 2011$?

C19.224. **Exercice (TPE)** Résoudre $x^2+x+1=0$ dans $\mathbb{Z}/7\mathbb{Z}$, puis dans $\mathbb{Z}/6\mathbb{Z}$. Que dire dans $\mathbb{Z}/n\mathbb{Z}$?

C19.225. **Exercice (TPE)** Démontrer que l'ensemble des entiers premier congrus à -1 modulo 4 est infini.
Indication : Raisonner par l'absurde et considérer $N = 4p_1 \dots p_r - 1$, où $p_1, \dots, p_r$ sont des nombres premiers « bien choisis ».

C19.226. **Exercice (TPE)** Soit A un anneau tel que pour tout $x \in A$, $x^3 = x$.

1. Démontrer que pour tout $x \in A$, $6x = 0$.
2. Notons $B = \{x \in A : 2x = 0\}$ et $C = \{x \in A : 3x = 0\}$. Démontrer que $B + C = A$.

C19.227. **Exercice (TPE)** Résoudre dans $\mathbb{Z}^2$ l'équation

$$11(n \wedge m) + n \vee m = 203.$$

C19.228. **Exercice (TPE)**

1. Soit $p \geq 3$ un nombre premier. On considère l'équation

$$(E) \qquad x^2 + ax + b = 0$$

d'inconnue $x \in \mathbb{Z}/p\mathbb{Z}$. Démontrer que (E) posséde une solution si et seulement si $a^2 - 4b$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

2. On suppose qu'il existe $u \in \mathbb{N}^*$ tel que $p = 3u+1$.
   (a) Démontrer qu'il existe $a \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $a^u \neq 1$.
   (b) En déduire que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

C19.229. **Exercice (TPE)** Résoudre dans $\mathbb{Z}/37\mathbb{Z}$ le systéme suivant.

$$\begin{cases} \overline{6}x + \overline{7}y = \overline{30} \\ \overline{3}x - \overline{7}y = \overline{0} \end{cases}$$

C19.230. **Exercice (TPE)** Résoudre dans $\mathbb{N}^* \times \mathbb{N}^*$ le système suivant.

$$\begin{cases} n \wedge m = n - m \\ n \vee m = 300 \end{cases}$$

C19.231. **Exercice (Mines)** Résoudre dans $\mathbb{N}^3$ le système suivant.

$$\begin{cases} x^3 - y^3 - z^3 = 3xyz \\ x^2 = 2y + 2z \end{cases}$$

C19.232. **Exercice (Mines)** Déterminer les couples d'entiers $(p,q) \in \mathbb{Z}^2$ tels que 7 divise $2p+3q$.

C19.233. **Exercice (Mines)** Soit $n \in \mathbb{N}^*$. Déterminer le maximum et le minimum, lorsque σ parcourt l'ensemble $\mathfrak{S}_n$, de $\sum_{k=1}^{n} k\sigma(k)$.

C19.234. **Exercice (Mines)** Posons

$$\mathbb{Q}\left[\sqrt{2}\right] := \left\{a + \sqrt{2}b : (a,b) \in \mathbb{Q}^2\right\}.$$

Démontrer que $\mathbb{Q}\left[\sqrt{2}\right]$ est un corps, et déterminer les morphismes d'anneaux de $\mathbb{Q}\left[\sqrt{2}\right]$ dans $\mathbb{Q}\left[\sqrt{2}\right]$.

C19.235. **Exercice (Mines)** Posons $j = e^{\frac{2i\pi}{3}}$ et

$$\mathbb{Z}[j] := \left\{a + bj : (a,b) \in \mathbb{Z}^2\right\}.$$

1. Démontrer que $\mathbb{Z}\left[j\right]$ est un sous-anneau de $\mathbb{C}$.
2. On note U l'ensemble des inversibles de $\mathbb{Z}\left[j\right]$. Démontrer que pour tout $z \in \mathbb{Z}\left[j\right]$, $z \in U$ si et seulement si $|z| = 1$. Déterminer U.

C19.236. Exercice (Centrale) Notons $\mathbb{Z}[i] := \left\{a + ib \,:\, (a,b)_i n\mathbb{Z}^2\right\}$ et

$$\nu \left| \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{R}_+ \\ z & \longmapsto & |z|^2 \end{array} \right. .$$

1. Déterminer les éléments inversibles de $\mathbb{Z}[i]$ (on pourra utiliser ν).
2. Démontrer que 2 est réductible dans $\mathbb{Z}[i]$.
3. Soit $(z,w) \in \mathbb{Z}[i] \times (\mathbb{Z}[i] \setminus \{0\})$. Démontrer qu'il existe $(q,r) \in \mathbb{Z}[i]^2$ tel que $z = qw + r$, avec $\nu(r) < \nu(w)$. Un tel couple est-il nécessairement unique ?
4. Démontrer que les idéaux de $\mathbb{Z}[i]$ sont principaux, i.e. qu'ils sont engendrés par un élément.

C19.237. Exercice (Centrale) Pour tout $n \in \mathbb{N}^*$, on note D_n l'ensemble des diviseurs positifs de n. Soient n et m premiers entre eux, posons

$$\varphi_{n,m} \left| \begin{array}{ccc} D_n \times D_m & \longrightarrow & D_{nm} \\ (d,d') & \longmapsto & dd' \end{array} \right.$$

et

$$\psi_{n,m} \left| \begin{array}{ccc} D_{nm} & \longrightarrow & D_n \times D_m \\ q & \longmapsto & (n \wedge q, m \wedge q) \end{array} \right. .$$

Démontrer que $\varphi_{n,m}$ et $\psi_{n,m}$ sont des applications inverses l'une de l'autre. Qu'en déduire pour le cardinal de D_{nm} ?

C19.238. Exercice (Centrale) Soit G un groupe fini. Pour $a \in G$, posons

$$\Phi_a \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a.x.a^{-1} \end{array} \right. .$$

1. Démontrer que Φ_a est un automorphisme de groupes de G.
2. Démontrer que l'ensemble $I := \{\Phi_a \,:\, a \in G\}$ est un sous-groupe du groupe des automorphismes de G.
3. Supposons I cyclique. Démontrer que G est commutatif.

C19.239. Exercice (Centrale) Soit G un groupe fini de cardinal n et d'élément neutre e. Soit p un diviseur premier de n. Posons $E = \{(x_1,...,x_p) \in G^p \,:\, x_1...x_p = e\}$.

1. Démontrer que $\#E = n^{p-1}$.
2. Notons $\sigma \in \mathfrak{S}_p$ le p-cyle $(1,\dots,p)$. Pour tout $X = \left(x_1,\dots,x_p\right) \in G^p$ et tout $k \in \mathbb{Z}$, on note

$$\sigma^k X := \left(x_{\sigma^k(1)},\dots,x_{\sigma^k(p)}\right).$$

   Démontrer :

$$\forall X \in E, \quad \forall k \in \mathbb{Z}, \quad \sigma^k X \in E.$$

3. Soit $X \in E$. On pose

$$o(X) := \left\{Y \in E \,:\, \exists k \in \mathbb{Z} \text{ tel que } \sigma^k X = Y\right\}.$$

   Démontrer que $o(Y) = o(X)$ pour tout $Y \in o(X)$.
4. Démontrer qu'il existe une famille $(X_i)_{1 \leq i \leq m}$ telle que $(o(X_i))_{1 \leq i \leq m}$ forme une partition de E.
5. Soit $X \in E$. Démontrer que $o(X)$ contient soit p éléments, soit un unique élément.
6. Démontrer que G posséde un élément d'ordre p.

Ce résultat est connu sous le nom de Lemme de Cauchy.

C19.240. Exercice (ENS) Les groupes $(\mathbb{R},+)$ et $(\mathbb{R}^*,\times)$ sont-ils isomorphes ?

C19.241. Exercice (ENS)

1. Donner une expression du nombre a_n de permutations de $[\![1,2n]\!]$ dont la décomposition en cycles de supports disjoints ne fait apparaître aucun cycle de longueur strictement inférieure à n.
2. Déterminer la limite de la suite de terme général $\dfrac{a_n}{(2n)!}$.

C19.242. **Exercice (X-ENS)** Soit n un nombre entier supérieur ou égal à 2. Pour tout nombre premier p, notons $v_p(n!)$ la valuation p-adique de $n!$, i.e. l'exposant de p dans la décomposition de $n!$ en produit de facteurs premiers. Démontrer que

$$v_p(n!) = \sum_{k=1}^{+\infty} E\left(\frac{n}{p^k}\right).$$

Ce résultat est connu sous le nom de formule de Legendre.

C19.243. **Exercice (X)** Soit p un nombre premier. Déterminer, à isomorphisme près, tous les groupes d'ordre p^2.

C19.244. **Exercice (X-ENS)** Soit G un groupe fini et soit p un nombre premier.

1. Supposons que $\forall x \in G$, $x^p = 1$. Démontrer qu'il existe $n \in \mathbb{N}$ tel que $\#G = p^n$.
   Indications : Dans le cas particulier où G est abélien, on pourra munir G d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel pour conclure. Pour la cas où G est quelconque, on pourra considérer un diviseur premier q de Card(G) et montrer, grâce au lemme de Cauchy, que $q = p$.
2. Soit q un nombre premier, supposons que $\#G = pq$. Démontrer qu'il existe un élement $x \in G$ d'ordre p et un élément $y \in G$ d'ordre q. En déduire que G est cyclique.